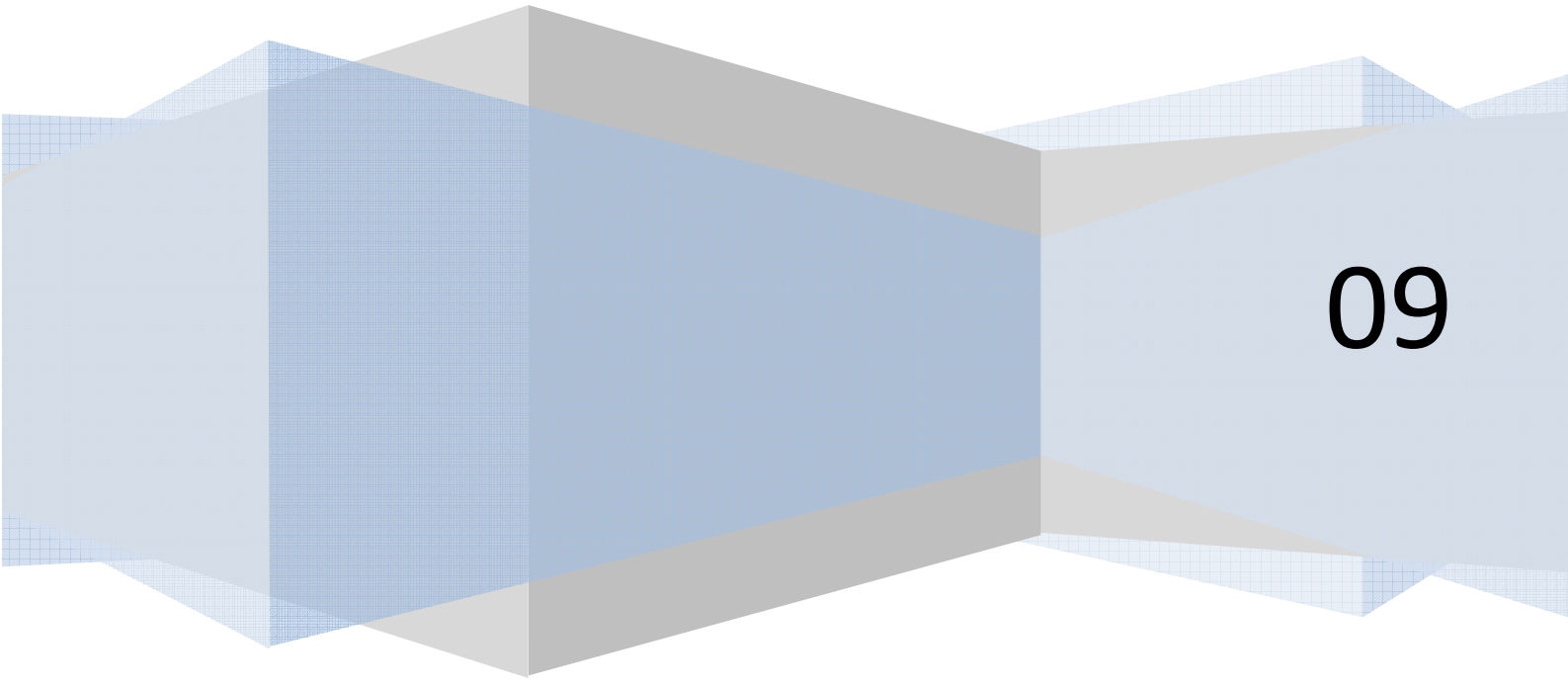
Research In Motion

A60 – How and When to Sign

For BlackBerry SmartPhones

Andre Fabris



09

Contents

A60 – How and When to Sign 3
Introduction 4
BlackBerry Code Signing 5
Obtaining BlackBerry Signing Keys 6
Installing the signing keys 8
Signing your application 10
Certicom Keys 13
Carrier's Keys 14
Links 15

A60 – How and When to Sign

Some applications need to be ‘signed’ before you can deploy them on the device. There are three different signature methods I will cover in this tutorial.

I will talk about BlackBerry signatures, Certicom signatures and Carrier signatures.

I will also show you how to get signature keys and use them to sign your application.

Introduction

Research In Motion (RIM) must track the use of some sensitive application program interfaces (APIs) in the BlackBerry® Java Development Environment (JDE) for security and export control reasons. In the API reference documentation, sensitive classes or methods are indicated by a lock icon or are noted as "signed". If you use these controlled classes or methods in your applications, the application must be signed using a key, or signature, provided by RIM before you can load the application .cod files onto the BlackBerry device.

While the core set of controlled APIs is covered by the RIM API signature, certain cryptography classes related to public/private key cryptography contain technology from Certicom. Use of these classes must be registered and licensed from Certicom directly, and are not covered under RIM's registration process.

Carrier code signing applies to MIDP applications only. When your MIDlet is signed, it is marked as a Trusted MIDlet, and the security prompts will not appear when the user wants to download the application, use file connections, push registry or RMS.

BlackBerry Code Signing

The packages marked as secure and therefore require code signing are listed in Table 1.

Package	Description
net.rim.blackberry.api.browser	This package enables applications to invoke the BlackBerry Browser.
net.rim.blackberry.api.invoke	This package enables applications to invoke BlackBerry applications, such as tasks, messages, MemoPad and phone.
net.rim.blackberry.api.mail	This package enables applications to interact with the BlackBerry messages application to send, receive, and open email messages.
net.rim.blackberry.api.mail.event	This package defines messaging events and listener interfaces to manage mail events.
net.rim.blackberry.api.menuitem	This package enables you to add custom menu items to BlackBerry applications, such as the address book, calendar, and messages.
net.rim.blackberry.api.options	This package enables you to add items to the handheld options.
net.rim.blackberry.api.pdap	This package enables applications to interact with BlackBerry personal information management (PIM) applications, including address book, tasks, and calendar. Most of the same functionality is provided by the MIDP package
javax.microedition.pim	
net.rim.blackberry.api.phone	This package provides access to advanced features of the phone application.
net.rim.blackberry.api.phone.phonelogs	This package provides access to the phone call history.
net.rim.device.api.browser.field	This package enables applications to display a browser field within their user interface.
net.rim.device.api.browser.plugin	This package enables you to add support for additional MIME types to the BlackBerry Browser.
net.rim.device.api.crypto	These packages provide data security capabilities, including data encryption and decryption, digital signatures, data authentication, and certificate management.
net.rim.device.api.io.http	This package enables applications to register with the BlackBerry Browser as provider for one or more URLs.

Table 1

Applications using classes from these packages will work on the simulators, however they will NOT work on the device unless signed.

Obtaining BlackBerry Signing Keys

To get Signing Keys you will need to go to the BlackBerry Developer's web site:

http://na.blackberry.com/eng/developers/javaappdev/codekeys.jsp

and fill in the application form (Figure 1):

https://www.blackberry.com/SignedKeys/

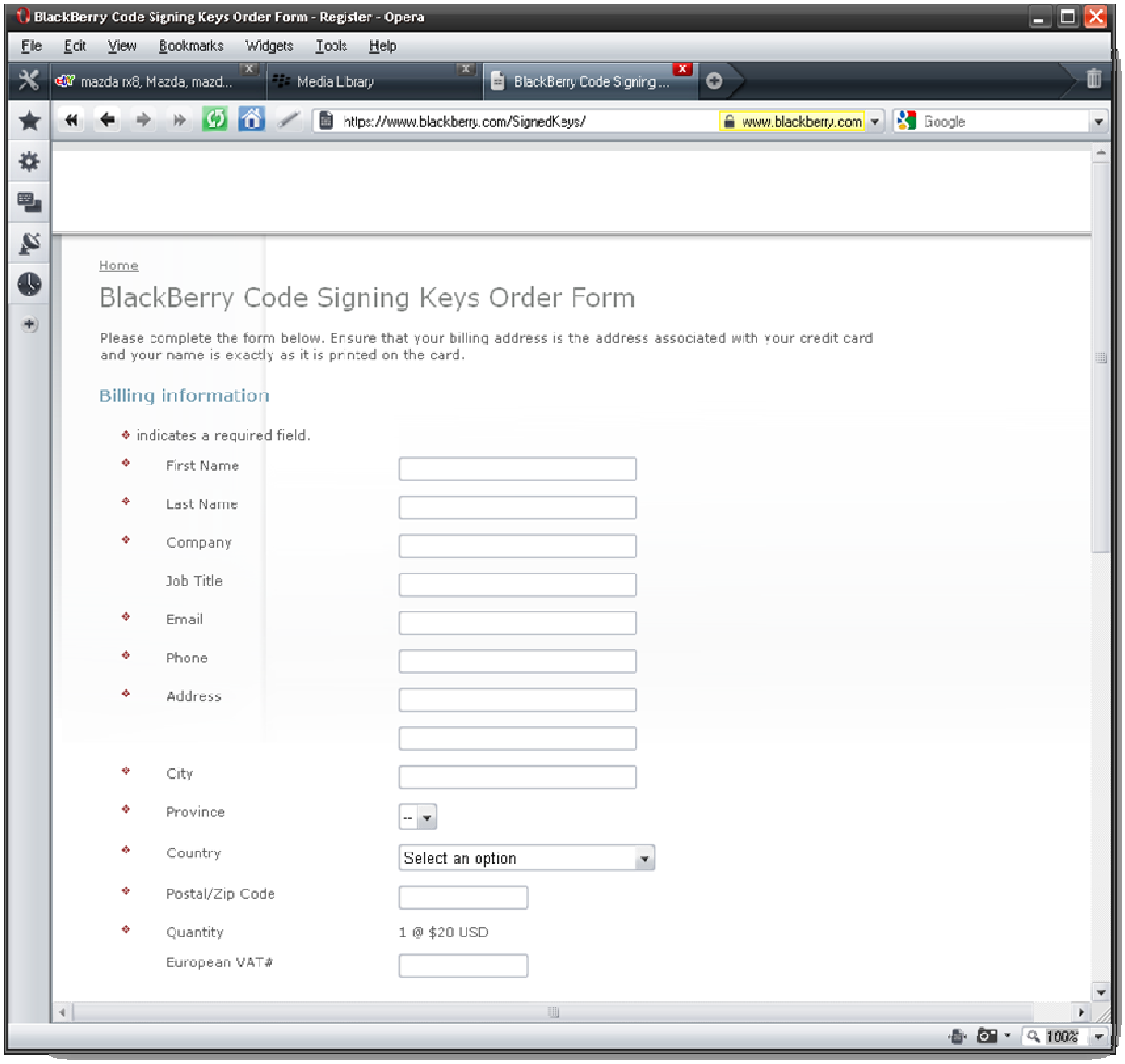


Figure 1

There is an administration fee of $20 (USD) which will be charged to a valid credit card to complete the registration process. The process itself takes up to 48 hours and the keys are sent via e-mail.

Occasionally the process might take up to 10 working days.

Code signing serves one purpose only and that is tracking the usage of APIs. It does not indicate in any way RIM's approval of the application. RIM assumes no liability to you or any other third parties who use your application(s). Please read the licence agreement online for more information.

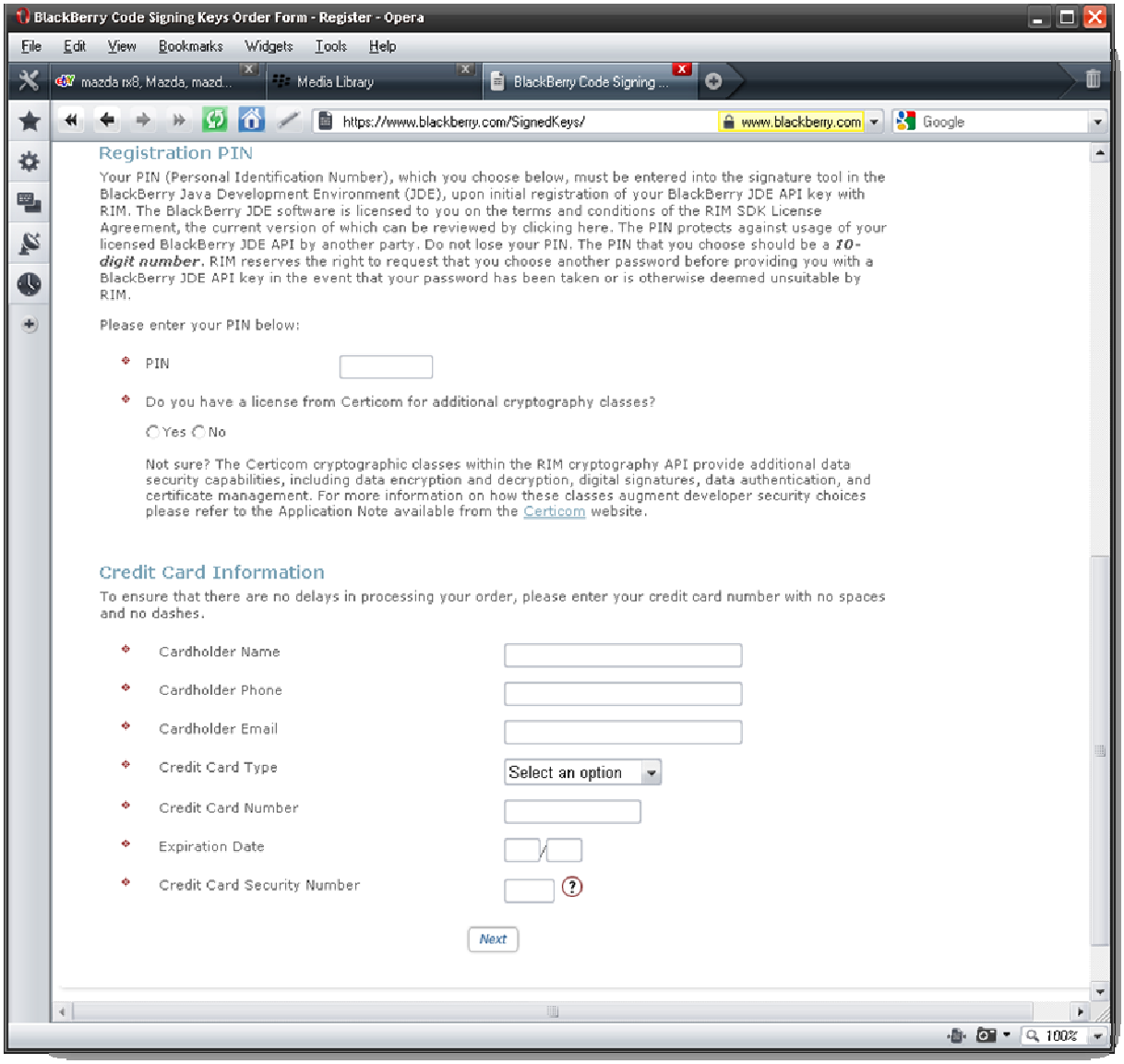


Figure 2

To complete the sign up process, you will need to select a 10 digit pin number used for installing your keys (Figure 2).

After you submit the form and your request is processed, you will receive three e-mails with signing keys and can then proceed with the installation.

Installing the signing keys

You will receive RBB, RRT and RCR keys. To install them you will need to follow this process for each one:

1. Double-click on the attachment (Figure 3).
2. If a dialog box appears that states a private key cannot be found, complete steps 3 through 6 before you continue. Otherwise, proceed to step 7.
3. Click "Yes" to create a new key pair file.
4. Type a password for your private key, and type it again to confirm.
5. Click "Ok"
6. Move your mouse to generate data for a new private key.
7. In the "Registration PIN" field, type the PIN number that you supplied on the signature key request form.
8. In the Private Key password field, type a password of at least 8 characters. This is your private key password, which protects your private key. Please remember this password as you will be prompted for it each time signing is attempted.
9. Click "Register".
10. Click "Exit".

When registering with the signing authority, ensure that you have correctly entered your registration PIN number. If you enter an incorrect PIN 5 times, your keys will be deactivated. The same password must be specified for all keys on the same PC.

All three signing keys have to be installed on the same PC otherwise the signing keys will not work.

If you are having difficulty installing or registering your signature keys please contact devsupport@rim.com.

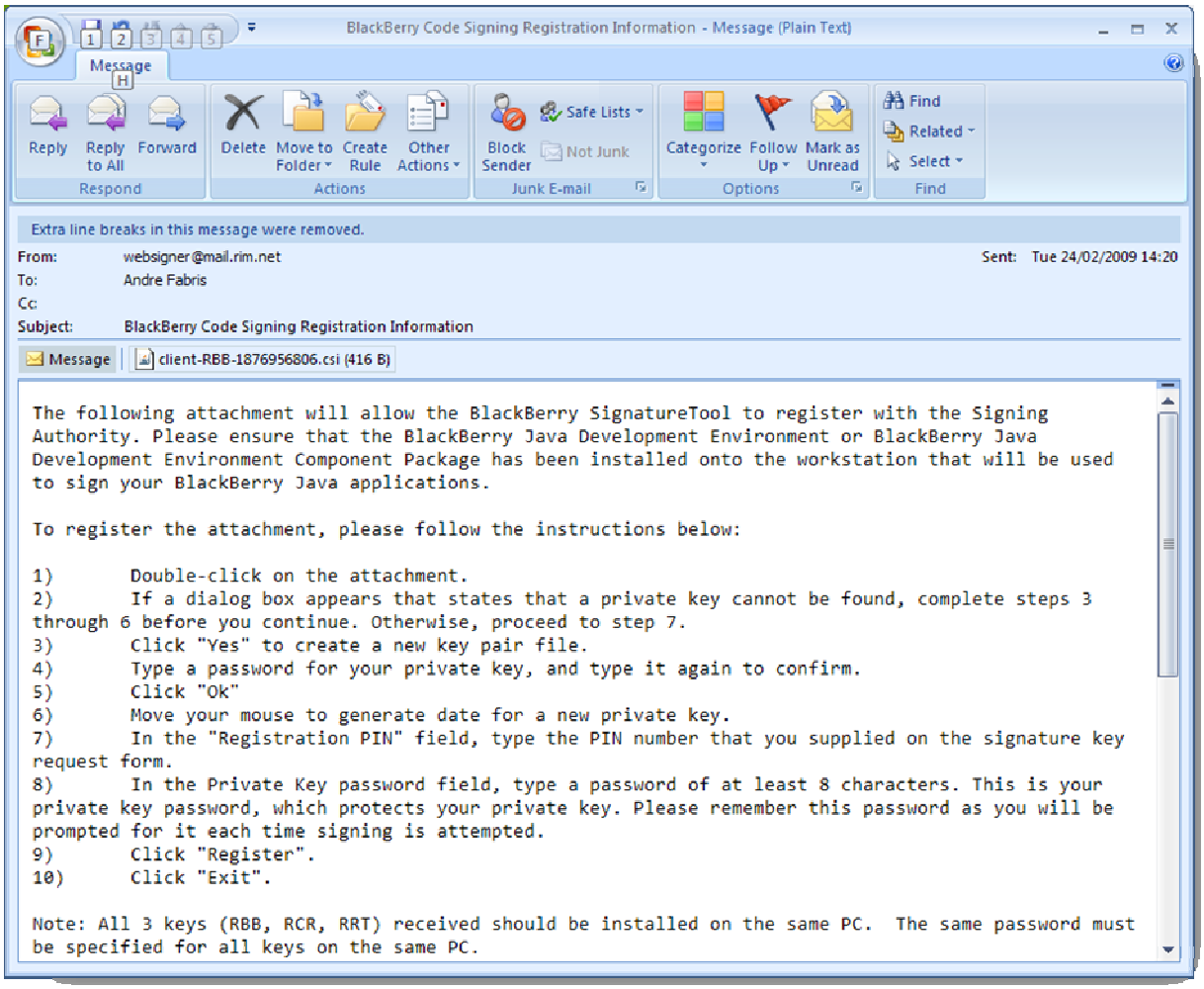

BlackBerry Code Signing Registration Information - Message (Plain Text)
Message
Reply
Reply to All
Forward
Delete
Move to Folder
Create Rule
Other Actions
Block Sender
Safe Lists
Not Junk
Categorize
Follow Up
Mark as Unread
Find
Related
Select
Respond
Actions
Junk E-mail
Options
Find
Extra line breaks in this message were removed.
From: websigner@mail.rim.net
Sent: Tue 24/02/2009 14:20
To: Andre Fabris
Cc:
Subject: BlackBerry Code Signing Registration Information
Message
client-RBB-1876956806.csi (416 B)
The following attachment will allow the BlackBerry SignatureTool to register with the Signing Authority. Please ensure that the BlackBerry Java Development Environment or BlackBerry Java Development Environment Component Package has been installed onto the workstation that will be used to sign your BlackBerry Java applications.
To register the attachment, please follow the instructions below:
1) Double-click on the attachment.
2) If a dialog box appears that states that a private key cannot be found, complete steps 3 through 6 before you continue. Otherwise, proceed to step 7.
3) Click "Yes" to create a new key pair file.
4) Type a password for your private key, and type it again to confirm.
5) Click "Ok"
6) Move your mouse to generate date for a new private key.
7) In the "Registration PIN" field, type the PIN number that you supplied on the signature key request form.
8) In the Private Key password field, type a password of at least 8 characters. This is your private key password, which protects your private key. Please remember this password as you will be prompted for it each time signing is attempted.
9) Click "Register".
10) Click "Exit".
Note: All 3 keys (RBB, RCR, RRT) received should be installed on the same PC. The same password must be specified for all keys on the same PC.

Figure 3

Signing your application

To be able to sign your application, your PC must have an Internet connection to connect to the signing servers. I will show you two ways to sign your application.

To sign your application within Eclipse just click on BlackBerry / Request Signatures..(Figure 4)

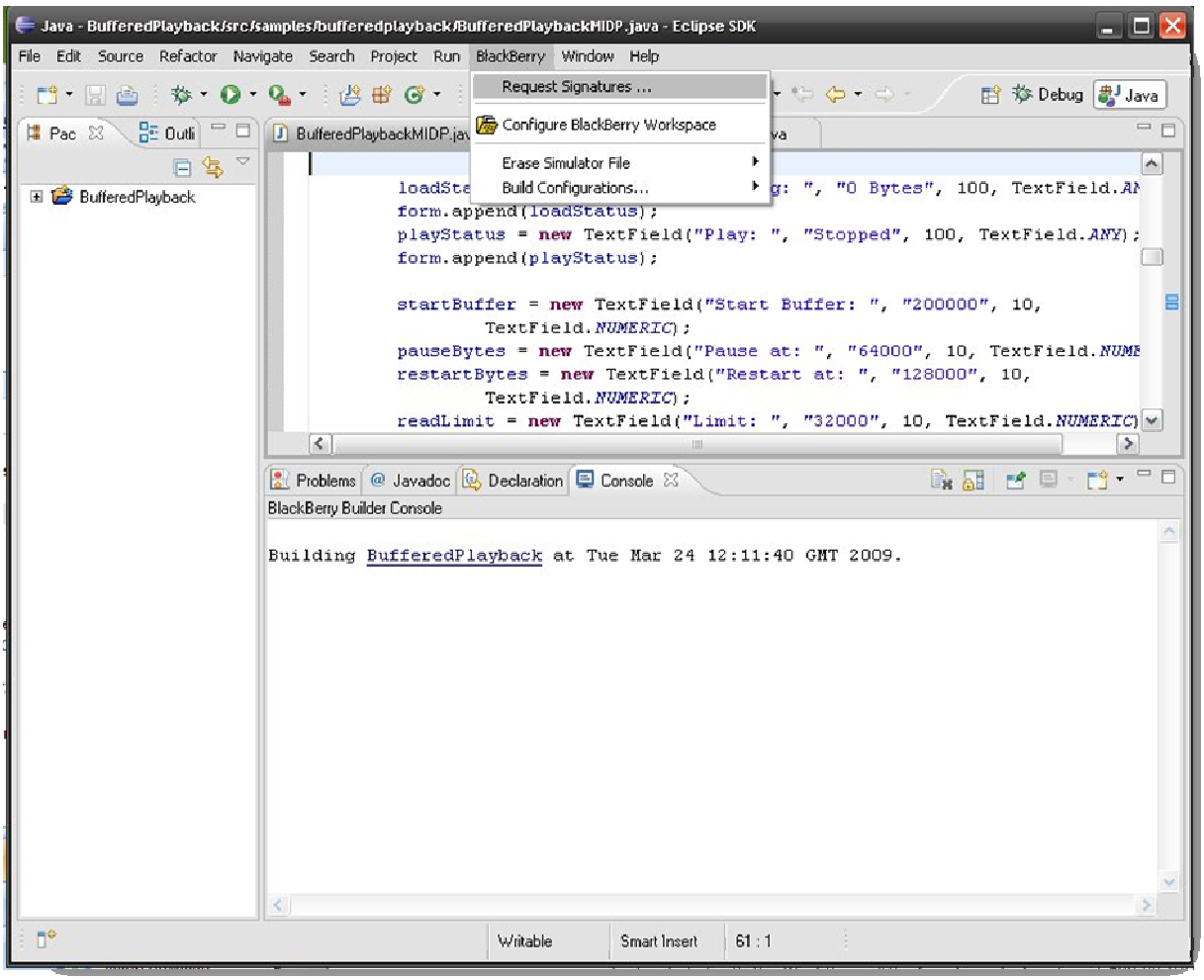


Figure 4

The application will display the Signature Tool which you use to request signatures (Figure 5). In our sample the keys are not required, but we can still sign the application. Note that we are actually signing the cod files and each time you create a new version of those files (ie. recompile your application) you will need to sign them again.

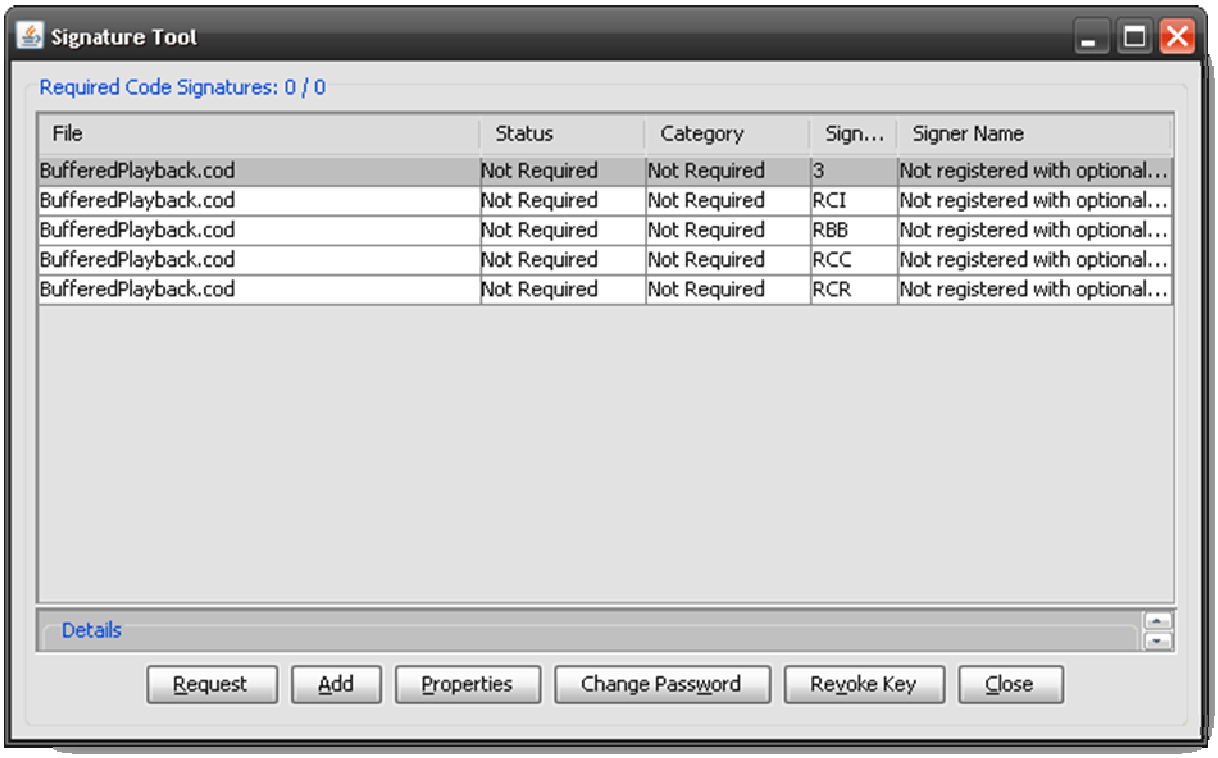


Figure 5

The other method to sign a cod file is to double click on the cod file itself (Figure 6). This will launch the Signature Tool automatically.

When you click on the Request button, the application will ask you for your password, and shortly after will let you know if the signing operation was successful (Figure 7).

Assuming the signing operation was successful, you can exit the Signature Tool and deploy your application to your device.

If you need to change your password or revoke the key, you can do this within the Signature Tool application itself.

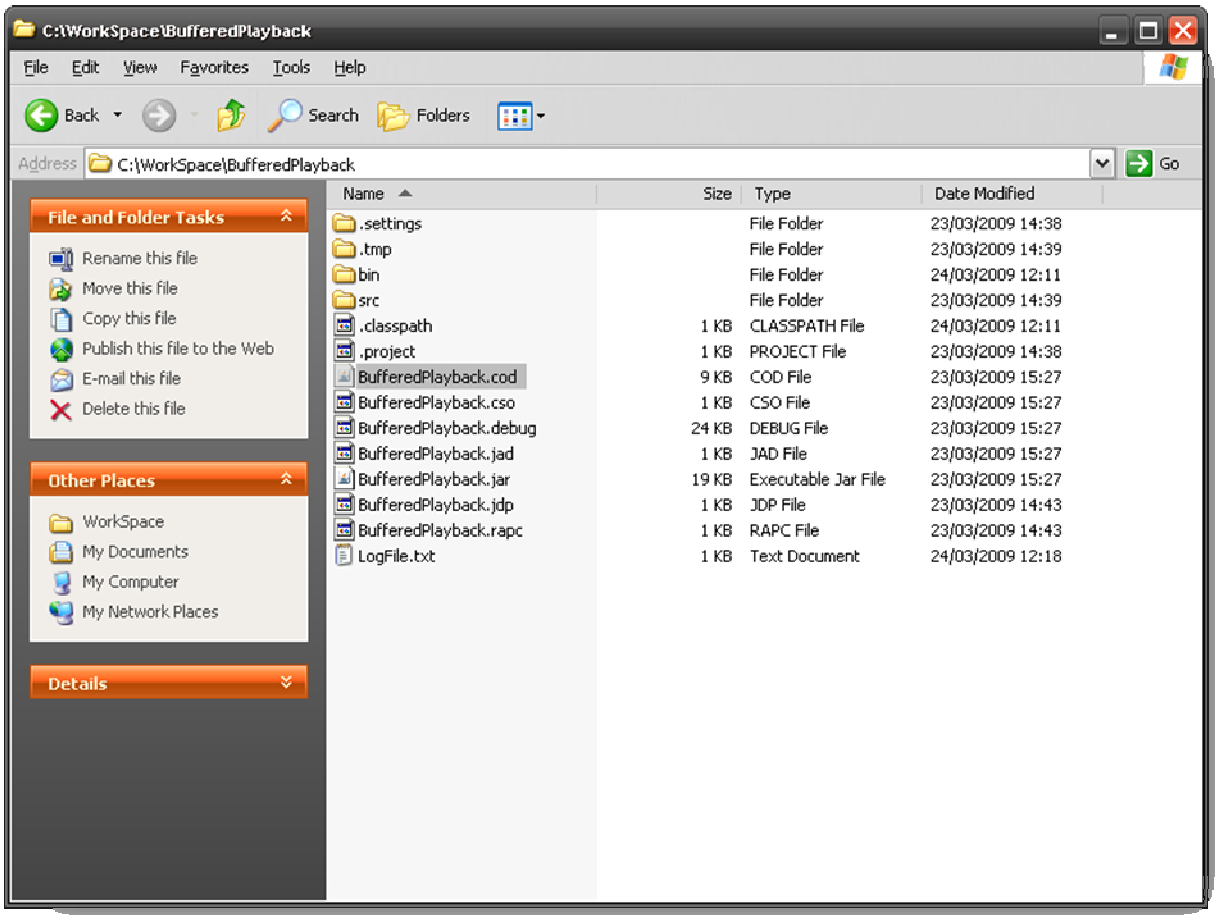


Figure 6

Figure 7

Certicom Keys

The Certicom cryptographic classes (Table 2) within the RIM cryptography API provide additional data security capabilities, including data encryption and decryption, digital signatures, data authentication, and certificate management.

A Certicom license is required to use these classes and is available from the Certicom website. Registration with RIM alone does not allow access to these classes.

RIM Cryptography API – Certicom Classes
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

Table 2

Please visit the Certicom website to get more information about how to obtain, install and use these keys:

http://www.certicom.com/

Carrier Keys

This only applies to MIDP applications. MIDP 2.0 has the concept of untrusted and trusted applications. If the application is signed, it is “trusted” otherwise it is “untrusted”. Untrusted applications will still work but the device will ask the user for permission to perform sensitive functions.

The most notable one is when the user wants to download the application, he/she will be notified that the application is untrusted and will be asked whether he/she would like to proceed.

To get your application signed by the carrier, you will need to contact the specific carrier directly. To run signed MIDlets on the device, the device must have a signing certificate from that specific carrier installed.

If you do not have the carrier signing certificate installed you will get the following error:

909 Application Authentication Failure Error.

Carrier code signing does not affect the application or the device IT policies in any way. All the IT policies applied by a BES administrator will remain unchanged.

Please contact your carrier to get more information about how to obtain, install and use carrier code signing keys.

Links

BlackBerry Developers Web Site:

http://na.blackberry.com/eng/developers/

Java Code Signing Keys:

http://na.blackberry.com/eng/developers/javaappdev/codekeys.jsp

Developer Video Library:

- Deploying and Signing Applications in the BlackBerry® JDE Plug-in for Eclipse:

  http://www.blackberry.com/DevMediaLibrary/view.do?name=deploying

- Deploying and Signing Applications in the BlackBerry® JDE:

  http://www.blackberry.com/DevMediaLibrary/view.do?name=deployingJDE

- How do I Leverage Carrier Code Signing?:

  http://www.blackberry.com/DevMediaLibrary/view.do?name=carrierfinal

Documentation:

- Documentation for the developers can be found here:

  http://na.blackberry.com/eng/support/docs/developers/?userType=21

Knowledge Base Articles:

http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/348583/customview.html?func=ll&objId=348583

Forums:

- The link to BlackBerry Development Forums:

  http://supportforums.blackberry.com/rim/?category.id=BlackBerryDevelopment