Signing process in Java ME

Signing Process:

Java Verified™ Program is a standards-based application testing and signing program accepted by multiple operators and device manufacturers for third party applications.

Private and Public Key the Basics:

• Private key is used to sign the application

• Public key is used to verify that the signature is authentic
• Embedded in the phone by the manufacturer
• “Root certificate”

Example :

JAD file

MIDlet-Name:

MIDlet-Permissions:

MIDlet-Vendor:

after signing the JAD file

JAD file

MIDlet-Name: SigningDemo
MIDlet-Permissions: javax.microedition.pim.ContactList.read,javax.microedition.pim.ContactList.write
MIDlet-Vendor:

MIDlet-Certificate-1-1: MIIE6DCCA9CgAwIBAgIQc0PNrxYODJ/WiFY14.....

MIDlet-Certificate-1-2: VQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4xNzA1Bg....

MIDlet-Certificate-1-3: 5p/AfbdynMk2OmufTqj/ZA1k.....

-…
Signing
Installation time:
• Does the device have the corresponding root certificate?
Is the information correct?
No: Installation fails
Yes: Installation succeeds

Digital Signatures and Domains
• Access restrictions in Java™ Platform, Micro Edition (Java ME platform) fall into domains
• A signed application installs to the domain which has the corresponding root certificate in the device
• The access restrictions on APIs and permission types vary between domains

Unidentified 3rd party
protection domain
Identified 3rd party
protection domain

(C) Copyright Nokia 2014. All rights reserved.

Operator domain
Manufacturer domain

Permission Types
• Not allowed
• Ask every time
• Ask first time
• Always allowed

MIDP 2.0—Network Access
• Unidentified third-party protection domain: = Application is not signed
• Not allowed, Ask every time, Ask first time
• Identified third-party protection domain: = Java Verified Program signed application
• Not allowed, Ask every time, Ask first time, Always allowed

Signing in Java Verified Program
• Done after the application has passed the testing
• GeoTrust CA for UTI
• **Result:**
• The application cannot be altered
  • Application is installed to the Identified third-party protection domain of the device
• Better user experience:
  • The application is trusted by the device, no installation errors
  • The user has more options to control the application behaviour
• Access to certain APIs

Application Quality
• The test criteria has the main considerations for mobile applications
  • Use it at the application specification phase
• Use it at the application acceptance testing phase
• The criteria can easily be integrated as part of your application development process

Make sure the application works:
• Use it yourself!
• Get an independent test done (not by the coder)
• Exploit the available information
• Your operator/carriers and manufacturers developer program and tools they may provide

'***Why the Application Does Not'''***Install?
• **No “GeoTrust CA for UTI” in the certificate store, remove from JAD:**
• **MIDlet-Certificate-1-1**
• **MIDlet-Jar-RSA-SHA1**
• **“MIDlet-” in Java Application Descriptor (JAD) file = “MIDlet-” in Java Archive (JAR) file manifest**
• **Exceptions: MIDlet-Jar-Size and MIDlet-Jar-URL**
• **MIDlet-Permissions are correct?**
• **Date and Time settings on the device must match the certificate validity period**

(C) Copyright Nokia 2014. All rights reserved.

(C) Copyright Nokia 2014. All rights reserved.