



Unified Testing Initiative Java Verified

**Why a signed MIDlet may
not work, when unsigned it did.**

This document explains the four most common issues that would cause Java ME applications to work before signing but not afterwards.

- High level explanation:
 1. Trouble with “MIDlet-” attributes in the JAD and JAR manifest files
 2. Problems with defined permissions
 3. The correct certificate authority (CA) certificate is not present in the device
 4. Date and time of the device are not correctly set
- For testing purposes Java Verified offers the R&D Signing service which allows signing of the application for testing purposes.



1. “MIDlet-” attributes

“MIDlet-” fields in JAD file

=

“MIDlet-“ fields in JAR manifest file

- If the equation is not true, then the application installation fails. There are only two exceptions, which are defined in the JAD file, however they must have correct information:
 - MIDlet-Jar-Size
 - MIDlet-Jar-URL
- Also the different format of the JAD file and JAR manifest file may cause problems.
 - > For example, if JAD has been created with a UNIX editor and JAR manifest with Windows notepad the line end characters may be different and thus the files are interpreted differently. That is why the equation does not match.



Java
Verified™

2. Permissions

Permissions must be declared correctly.

- Permissions are used to protect API calls that are sensitive and require authorization.
 - > Such as HTTP connections, SMS sending, etc.
- All the permissions which the application needs must be declared.
- The application will not install if permissions are declared for API calls which the device does not support.
- Sometimes several permissions need to be declared to use one feature.
 - > For example, in some cases with the use of push registry.



3. Certificates

The device must have the certificate matching the signature in the application.

- MIDP 2 specification defines that the signed application will not install if the certificate matching the signature is not present in the device.
- Please refer to the user manual of the device to find where the certificates are listed.
- If the certificate is not in the device, but the application is signed, the following steps can be done to install the application:
 - > Remove the following fields from the JAD
 - MIDlet-Certificate- fields
 - MIDlet-Jar-RSA-SHA1 field

4. Date and time

The certificate in the device and the signature in the application have a validity time period. The device date and time must be within the validity period. Otherwise the application will not install.

- The Java Verified R&D Signing signature has special validity period. Date change is needed to install the application.
- To check the validity of the signature, follow these steps:
 - > Open the JAD file with a text editor – Notepad is just fine.
 - > Copy the contents of the “MIDlet-Certificate-1-1:” field (text between the colon and the carriage return) and paste it into an empty text file.
 - > Save the text file



Java
Verified™

More information

- JavaVerified.com –> Resources and downloads
 - > Information about the Java Verified process and application signing
- “MIDP 2.0: Signed MIDlet Developer's Guide” at Forum Nokia web site
 - > All about Signing MIDlets, listing also permissions and API calls