



R&D Signature: explained

Q. What is an R&D Signature, and what is it intended for?

A: R&D Signing is a service that signs applications to the Identified Third Party Protection Domain (formerly the Trusted Third Party Domain) to enable them to be run on a device for testing purposes. The intention is to provide a way for developers to test how the application would behave on a live device after it has been signed with a Java Verified Signature.

Q. How long is an R&D Signature valid for?

A. Seven days from date and time of signing. This is to ensure that R&D signed applications are not distributed commercially. Please bear in mind that the signing certificate will have expired by the time you receive the signed application. In order to install the application you need to change the date and time of the device.

Q. How do I get my application signed with an R&D Signature?

A. To submit an application for R&D signing, please follow these steps within the Submission Portal:

1. Submit a JAD/JAR pair to the Submission Portal
2. On the Submission home page, click on the JAD/JAR pair that you would like to get R&D Signed.
3. On the submission details page under the “R&D signature” heading, select “Sign application”.
4. After the application has been signed, it can be downloaded from the “Submitted JAD/JAR pair details”-page. This step takes time, so please be patient.

Q. What do I then need to do with the application and the device?

A. First, you need to ensure that the device on which you want to test the application has in it the root certificate used by Java Verified: the UTI root certificate.

Please refer to the online “Matrix of Supported Devices” at

http://javaverified.com/Device_matrix

The devices pre-installed with the UTI root certificate are indicated with a ‘+’.

Without the UTI root certificate, the R&D Signature will not work.

Also, make sure the validity period of the signing certificate and the date & time on the device match. When installing the application, the certificate in the application is valid from the day and time when it was signed and for the preceding six days. This is why the date of the device must be changed to meet the time when the signing certificate

To check the dates when the application can be installed:

1. Open the JAD file with a text editor (e.g. notepad)

2. Copy the contents of the “MIDlet-Certificate-1-1:” field (text starting from the colon and ending to the carriage return) and paste it to an empty text file.
3. Save the text file
4. Change the file extension to .cer
5. Open the file. The validity is presented in the “Valid from” field (see image below)

