



Unified Testing Initiative Java Verified

Signing Java™ Platform, ME Applications and the Renewed Java Verified Program

Risto Helin
Forum Nokia

2nd of June, 2009

- Signing Java ME applications
 - > Theory with practise
 - > What does signing mean?
 - > Signing opportunities
- Java Verified 3.0

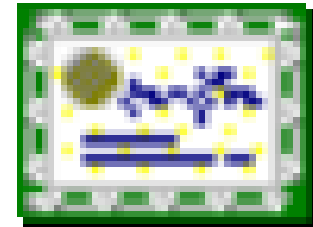
- Signing Java ME applications
 - > Theory with practise
 - > What does signing mean?
 - > Signing opportunities
- Java Verified 3.0

- **Private key** is used to sign the application
 - > Can you trust the signature in the application?
- **Public key** is used to verify that the signature is authentic
 - > Private and Public keys are mathematically related to each other.
 - > “**Root certificate**” is embedded in the phone by the manufacturer to verify the content which has been signed with the private key.

Example with a Publisher ID, three steps:

- Export the Publisher ID from the Internet Explorer
- Exporting the Publisher ID to a key store file
- Sign an application

- Protects the application
 - > What if I hack an application?
- After signing, two new fields in the JAD file:
 - > MIDlet-Certificate-1-1
 - > MIDlet-Jar-RSA-SHA1



- Signing Java ME applications
 - > Theory with practise
 - > **What does signing mean?**
 - > Signing opportunities
- Java Verified 3.0

- What is this that I'm installing?
 - > MicroEdition-Configuration: CLDC-1.0
 - > MicroEdition-Profile: MIDP-2.0
- Is the certificate valid?
 - > Date and time
- Permissions?
 - > Are they declared properly?
 - > Did you declare the right permissions?
 - MIDlet-Permissions-Opt:
- Domain



Manufacturer domain

Operator domain

Identified 3rd party
protection domain

Unidentified 3rd party
protection domain

Protection domain determines the user permissions

- **Not allowed**
 - > “No, the application cannot do that!”
- **Ask every time – one shot**
 - > “Every time the application wants to use a feature the user is prompted.”
- **Ask first time – session**
 - > “When I run the application, the first time the feature is used the user is prompted.”
- **Always allowed – blanket**
 - > “No questions asked”

- Unidentified 3rd party protection domain:
 - = Application is not signed
 - > Not allowed, **Ask every time**, Ask first time
- Identified 3rd party protection domain:
 - = Signed application
 - > Not allowed, Ask every time, **Ask first time**, Always allowed
- The Challenge: **Different implementations** in devices

- Signing Java ME applications
 - > Theory with practise
 - > What does signing mean?
 - > **Signing opportunities**
- Java Verified 3.0

- **Thawte** and **VeriSign** offer code signing certificates
 - > You have the physical private key at your disposal
 - > Requirements: Successful vetting & € / \$
 - > The corresponding root certificates are not in most of the devices
 - > The signature is valid only the time period the signing certificate is valid, 1-3 years.
- **Java Verified** offers different signing opportunities
 - > Intention of being “one stop shop” instead of multiple programs
 - > Signature is valid for 10 years

Which one to use?

- Signing Java ME applications
 - > Theory with practise
 - > What does signing mean?
 - > Signing opportunities
- **Java Verified 3.0**



Java
Verified™

What is happening in Java Verified

- To protect your identity and applications:
 - > **Publisher ID**
- To enable testing your application as signed:
 - > **R&D Signing**
- To make testing of applications easier
 - > **UTC 3.0**
- To make access to services easier
 - > **New portal**

- A passport to Java Verified services
 - > Can be obtained after successful **vetting**
 - > Valid for **one year**
 - > Cost is **\$200 US** per year
 - > Provided by **TC Trustcenter**
- To protect your application and identity
 - > A submitted application **must be signed with a Publisher ID**



Sign your
application
with
Publisher ID



Submit



Time of
signing
-7 days

Change
the date on
the device

Install to
your device
for testing
purposes!

- Outlining the **requirements** for Java ME applications:
 - > Application installation and start up
 - > UI clarity and consistency
 - > Language support and text problems
 - > Application and the phone co-operation
 - > Application creating connections and things related to that
 - > Using and accessing PIM data
- **Reducing the amount of testing**, basic thinking:
 - > First a “mother” version of the application is built
 - > That is used to port the application to several “children”

Combining UTC 3.0 and supported devices list

- Supported devices list has over **543** devices
 - > Split into **Lead device** (144)
 - > And **other** devices (369)
 - = **Device family**
- Adding a new element: **Platform**
 - > Consisting on **several device families**
- Basic rule:
 - > **Full test** of the application with **one device per platform**.
 - Tested on a lead device
 - > The **rest** of the application versions **receive reduced** amount of **testing**



Java Verified™

New access to the new services

JV Submission Portal Sign up for our Newsletter

About the UTI | Addressing Fragmentation | Java Verified Program | Java Verified Process | Promote Your App | Resources & Downloads

Develop

Use our developer resources to make your ideas successful!

Develop
Test & Sign
Go to Market

What's New

JavaOne 2009
Come join us at JavaOne 2009 - San Francisco, June 2-5, 2009
[more](#)

Press release: Java Fragmentation 2 June 2009 - Mobile industry collaborates to address Java fragmentation and deliver new benefits to Java developers
[more](#)

Welcome to the new Java Verified site

Learn about the enhancements we've made to the program:

- New streamlined [testing procedures](#) can reduce costs up to 50%
- New [Publisher ID](#) and [E&O signing](#)
- Re-designed [Submission Portal](#)
- New initiatives for addressing fragmentation - [letter from Martin Wipler, UTI chairman](#)

Join Us at

JavaOne

June 2-5, 2009

We want to see your apps and hear what you have to say.

Join us for the Java Verified - WIP Mobile Jam at the JavaOne Pavilion on Wednesday, June 3

Get A FREE PASS ▶

Information for Developers

Submission Portal

Supported Devices

Introducing JATAF

JATAF

Java™ Application Terminal Alignment Framework

UTI Member Companies

© 1994-2009 Sun Microsystems, Inc.
[Terms of Use](#) | [Privacy Policy](#) | [Glossary](#) | [FAQs](#) | [Contact Us](#)



Java Verified Submission Portal

v1.0.2

Java Verified Submission Portal

Please enter your email address and password. Mandatory input values are marked with *.

Login to the portal

Email address*:

Password*:

If you do not have an account yet, you can [register yourself for an account](#)

- Java Verified **root certificate** is the most widely available root certificate in Java ME devices.
- Java Verified program **reduces complexity** - “one stop shop” for application testing with the new services
- Java Verified is **required, recognized and supported** by major manufacturers and operators
- **For the biggest market exposure, use Java Verified Program**