Java Security Domains

Introduction

15 Feb 2010

There are some restrictions for accessing certain method calls and APIs from MIDlets. In those cases it is possible that the user will either be prompted for confirmation to allow a certain method call or the access is blocked altogether, resulting a SecurityException to be thrown.

Making these prompts appear less frequently requires the developer to sign the MIDlet and the user to manually change the API access settings. Signing to the operator or manufacturer domain will remove the prompts completely, but this requires close collaboration with those parties.

Security domains

Mobile information device profile (MIDP) 2.0 specification defines four security domains to which the MIDlet can be installed:

- Third party protection domain (untrusted 3rd party)
- Identified third party protection domain (trusted 3rd party)
- Operator protection domain
- Manufacturer protection domain

API protection groups

Each of the protection domains have certain level of access to the protected (sensitive APIs). The access rights are grouped to a function groups:

- Net access (MIDP specification also defines low-level net access, but this has been combined on many phones to the Net access function group)
- Messaging (MIDP specification also defines restricted messaging)
- Application auto-start
- Local connectivity
- Multimedia recording
- Read user data (including files and PIM)
- Write/Edit user data (including files and PIM)
- Location
- Landmark store
- Smart card communication
- Authentication
- (Call control)
- (Phone call)

The MIDlet will have access settings defined to each of the function groups above that are supported by the phone. The setting can be one of the following, defined by the security domain policy of the phone:

- Always allow / Blanket access
- Ask first time / Ask once per session
- Ask every time
- Not allowed

API access definitions in Java ME standards

Java specifications include a number of versions for the available API access rights (Note that it is possible that there might not be a device available which would support the API access rights exactly the way they are defined in the specification!)

- MIDP 2.0 API access rights
- MIDP 2.0.1 API access rights
- MIDP 2.1 API access rights (same as in MSA)
- JTWI API access rights (only defines API access rights for the untrusted 3rd party domain)

NOTE: The MIDP specification defines that even a trusted 3rd party MIDlet cannot have networking and auto-start permissions simultaneously as Always Allowed!

(C) Copyright Nokia 2014. All rights reserved.

A MIDlet which has not been signed will be placed in the untrusted domain, which has most restrictions for accessing certain APIs. If the MIDlet has been signed and the corresponding certificate is stored in the certificate store of the phone, the MIDlet will be placed in the protection domain to which the certificate has been tied to (there are some complex checks which are done at the installation time, please see the MIDP 2 specification for more info).

Certificates to sign to a trusted 3rd party domain

If your application passes Java Verified testing, it will be signed with UTI root certificate, which will place your MIDlet to the trusted 3rd party domain. Other common certificates that place your MIDlet to the trusted 3rd party domain are available from:

- Thawte
- Verisign - installation test MIDlet for this certificate

Note that there are differences between different phone models on which certificates are installed on the phones. Additionally, the same phone model may have a different set of certificates depending on which region it was sold in. Operator variants of the phones can also have additional changes in the certificate availability.

Also note that the MIDP specification does not allow new certificates to be added on the phones to allow signing to the trusted 3rd party domain. This is, however, possible on S60 2nd Edition devices due to Archived:Signing certificates for MIDlets (Known Issue) implementation (instructions). Some operators have also implemented so-called developer certificates for their devices (Sprint and China Unicom). Consequently, make sure to check the available code-signing CA-certificates (or check this posting).

Security Domain policies some carriers that deviate from the standard

As the MIDP spec security domain policy is just a recommendation, some operators have defined their own security domains and API access rights. These include:

- AT&T Java security domains (Cingular) (entry on FN blogs)
- China Unicom Java security domains
- Hutchinson 3G security domains(entry on FN blogs) - note, that Orange Israel follows the Hutchinson 3G guidelines too
- Sprint Java security domains (entry on FN blogs)
- T-Mobile U.S. Java security domains (entry on FN blogs)

Security domain information from other manufacturers than Nokia

- Motorola Java ME Developer Guide (requires free registration) and Testing and Signing documentation.

Note: Motorola handsets do not support Thawte or VeriSign Certificates, only Motorola certs and JavaVerified [1]

API access settings on real phones

Generic phones also have different versions of the API access rights implemented:

- API access rights on phones, S60 2nd FP2, on generic 6630 (2.39.126)
- API access rights on phones, S60 2nd FP2 ver2, on generic 6680, 6630 (6.03.40)
- API access rights on phones, S60 2nd FP3, on generic N72
- Archived:API access rights on S60 3rd Edition devices, on generic E61i
- Archived:API access rights on S60 3rd FP1 devices, on generic N95
- Archived:API access rights on S60 3rd Edition devices, on generic 6210 Navigator
- API access rights on phones, S60 5th, on generic N97
- API access rights on phones, Series 40 3rd FP1, on generic 6131
- API access rights on phones, Series 40 3rd FP2, on generic Nokia 5300, 6300, 7373
- API access rights on phones, Series 40 5th FP1, on generic Nokia 6500 slide
- API access rights on phones, Series 40 6th
- API access rights on phones, Series 40 6th FP1, on generic Nokia X3-02

It is not possible to change the default settings available on the phone, but after MIDlet installation it is possible to change the API access settings from the default to the the available ones (not all options are available to untrusted MIDlets).

- S60 instructions
- Series 40 instructions

(C) Copyright Nokia 2014. All rights reserved.

References

- MIDP 2.0: Signed MIDlet Developer's Guide

(C) Copyright Nokia 2014. All rights reserved.