Java Card Development Kit

Release Notes

for Java Card 3 Platform, Classic Edition, Version 3.0.5u3

E62057-06

April 2018

Table of Contents

Introduction

These release notes describe the Java Card Development Kit for the Java Card 3 Platform, Version 3.0.5u3. This version of the Java Card Development Kit is a maintenance release and includes bug fixes in the off-card CAP file verification tool. It also contains previous tool chain enhancements to enforce consistency between verified and loaded content, and extensions to maskgen to enable the inclusion of external CAP files in the mask. This release does not include the Trimming Tool.

Java Card technology combines a subset of the Java programming language with a runtime environment optimized for smart cards and similar small-memory embedded devices. The goal of Java Card technology is to bring many of the benefits of the Java programming language to the resource-constrained world of smart cards. The Java Card API is compatible with international standards such as ISO/IEC 7816, and industry-specific standards such as Europay, Master Card, and Visa (EMV).

The Java Card Development Kit, Version 3.0.5u3, is based on specifications for the Java Card 3 Platform, Version 3.0.5, Classic Edition.

New Features in this Release

The following are new features in Java Card 3 Platform, Classic Edition since version 3.0.4:

- Added the following new features in version 3.0.5 of the Java Card 3 Platform, Classic Edition API:
  - Elliptic curve domain conservation
  - PIN extensions for banking
  - Secure basic operations
  - Secure variables and arrays
  - Support of Java 7 language improvements
  - Utilities for analyzing an APDU's CLA byte
  - Static cryptography
  - Diffie-Hellmann support
  - One-to-many biometry support
- Added support for new cryptographic algorithms:
  - AES-CMAC
  - PACE
  - AEAD_CCM
  - AEAD_GCM
- Aligned the platform and its documentation with the latest ISO/IEC 7816-4 specification. In particular, the Java Card 3 Platform specifications in this release refer to the 2013 release of the ISO/IEC 7816-4 specification and align with the vocabulary of that specification.
- Added new methods in version 3.0.5 of the Java Card 3 Platform, Classic Edition API.
- Added support in the Java Card 3.0.5 and later tool chain for the following Java language enhancements that were introduced in Java SE 7 and are further described at https://docs.oracle.com/javase/7/docs/technotes/guides/language/enhancements.html#javase7:

  > **Note:**
  >
  > These features are available when compiling with the Java SE 7 (or higher) compiler with the source code release level set to 1.7 or 7.

  - **Binary Literals** – The integral types (`byte`, `short`, `int`, and `long`) can also be expressed using the binary number system. To specify a binary literal, add the prefix `0b` or `0B` to the number.
  - **Underscores in Numeric Literals** – Any number of underscore characters (_) can appear anywhere between digits in a numerical literal. This feature enables you, for example, to separate groups of digits in numeric literals, which can improve the readability of your code.
  - **Type Inference for Generic Instance Creation** – You can replace the type arguments required to invoke the constructor of a generic class with an empty

set of type parameters (<>) as long as the compiler can infer the type arguments from the context. This pair of angle brackets is informally called the diamond.

  - **Improved Compiler Warnings and Errors When Using Non-Reifiable Formal Parameters with Varargs Methods** – The Java SE 7 complier generates a warning at the declaration site of a varargs method or constructor with a non-reifiable varargs formal parameter. Java SE 7 introduces the compiler option `-Xlint:varargs` and the annotations `@SafeVarargs` and `@SuppressWarnings({"unchecked", "varargs"})` to suppress these warnings.
  - **Catching Multiple Exception Types and Rethrowing Exceptions with Improved Type Checking** – A single catch block can handle more than one type of exception. In addition, the compiler performs more precise analysis of rethrown exceptions than earlier releases of Java SE. This enables you to specify more specific exception types in the throws clause of a method declaration.

- In addition to the String Constant Annotations introduced in Java Card 3.0.4, the Java Card 3.0.5 and later tool chain supports the following compile-time pre-defined annotations (provided *`JCDK_HOME`*`/lib/api_classic_annotations.jar` is added to the compiler's classpath):
  - `|@Deprecated|` – A program element annotated `@Deprecated` is one that programmers are discouraged from using, typically because it is dangerous, or because a better alternative exists. Compilers warn when a deprecated program element is used or overridden in non-deprecated code.
  - `|@Override|` – Indicates that a method declaration is intended to override a method declaration in a supertype.
  - `|@SuppressWarnings|` – Indicates that the named compiler warnings should be suppressed in the annotated element and in all program elements contained in the annotated element.
  - `|||@SafeVarag |` – A programmer assertion that the body of the annotated method or constructor does not perform potentially unsafe operations on its `varargs` parameter.
- (3.0.5u2 November 2017) Enhanced the tool chain to enforce consistency between verified and loaded content:
  - Verifier has been extended to generate a digest for each CAP component verified. These digests can be used during the loading process to check that each loaded component matches the one verified.
  - Scriptgen has been modified to check the digest of components included in the loading script.
- (3.0.5u2 November 2017) Extended Maskgen to allow external CAP files in the mask, in addition to JCA files.
- (3.0.5u2 January 2018) Updated Java Card Development Kit 3.0.5u2 to fix a critical bug that prevented the Eclipse plug-in from functioning correctly. Any installed instance of Java Card Development Kit 3.0.5u2 must be removed before installing the update.

- (3.0.5u3 April 2018) Added the command-line option `-target` to the Off-card CAP file verification tool. This option specifies the target platform on which the CAP file is to be loaded.

Bug Fixes

The following fixes have been made in the Java Card 3 Platform, Classic Edition since the release of version 3.0.5:

- Fixed `updateAAD` method multi-part issue in AES CCM.
- APDU with class value FF is rejected.
- (3.0.5u3 April 2018) Fixed miscellaneous bugs in the Off-card CAP file verification tool.

System Requirements

This product is targeted for use on a PC running the Microsoft Windows 7 operating system.

The following software must be installed for the Java Card Development Kit to work:

- **Java Development Kit** (JDK) – This release has been verified and tested with JDK 1.7 and 1.8. Download the JDK software from:

  http://www.oracle.com/technetwork/java/javase/downloads

  Install it according to the instructions on the website.
- **Apache ANT** – This release has been verified and tested with Apache Ant 1.9.4 Download and install Apache Ant from:

  http://ant.apache.org
- **GCC Compiler** – To build the VM, this release requires Minimal GNU for Windows (MinGW) version 5.1.4 or later. MinGW can be obtained from http://prdownloads.sourceforge.net/mingw. For information on MinGW go to http://www.mingw.org.
- **Eclipse** – Development using the Java Card Development Kit requires installing Eclipse Neon or Oxygen from:

  https://www.eclipse.org/

Installation

The Java Card specifications, documentation, and Java Card Development Kit must be downloaded and installed individually.

- The Java Card 3 Platform documentation is provided at https://docs.oracle.com/javacard. See Documentation for a description of the Java Card documentation that is provided on the Oracle Java Card documentation web site.
- The Java Card Development Kit installer is provided on the Oracle Technology Network download site for the Java Card platform (http://www.oracle.com/technetwork/java/

embedded/javacard/downloads/javacard-sdk-2043229.html). Install the development kit by downloading and running the Java Card Development Kit. `.msi` installer. See the *Java Card 3 Platform Development Kit User Guide, Classic Edition Version 3.0.5u3* for procedures used to install the Java Card Development Kit.

Contents of the Development Kit

This release of the Java Card Development Kit contains tools and features required to support developing classic Java Card applet applications on a smart card.

The following table describes the development kit files and directories that are installed in the root installation directory (*`JC_CLASSIC_HOME`*).

Directory/File	Description
`api_export_files`	Contains the export files for the Java Card 3.0.5 API packages. If you have a development kit that includes cryptography, this also includes the directory `api_export_files\javacardx\crypto`.
`bin`	Contains all shell scripts or batch files for running the tools (such as the apdutool, capdump, and converter), and the cref binary executables.
`docs`	Contains subdirectories each with compilations of the Javadoc tool files for the APDU I/O API, the Java Card 3.0.5 API, and the Java Card Client RMI API.
`eclipse-plugin`	The repository for the Java Card plugin for Eclipse.
`legal`	Contains license files.
`lib`	Contains all Java programming language JAR files required for running tools by using the shell scripts or batch files provided in the `bin` directory.
`samples`	Contains sample applets and applications.
`COPYRIGHT.html`	Copyright file for the development kit. Also the directory `shared` contains related files.

Known Issues

The following issue has been identified in this release of the Java Card 3 Platform:

- The Converter generates incorrect code when the source code uses `int` expressions and the class is compiled with the `-g` option.

  Occasionally the converter generates incorrect code which fails verification. The workaround is to either not compile the class with the `-g` option or avoid using the `int` type.

Documentation

The following table describes Java Card documentation that is provided on the Oracle Java Card documentation web site (https://docs.oracle.com/javacard).

> **Note:**
>
> Open the HTML versions of the documentation by clicking on the `toc.htm` file rather than the traditional `index.htm` file.

Document	Description
Java Card 3 Platform Development Kit User Guide, Classic Edition Version 3.0.5u3	This document describes how to use the Java Card Development Kit to develop applications for Java Card 3 Platform, Classic Edition, Version 3.0.5u3 and later. It is available in HTML, PDF, ePub, and Mobi formats from the Oracle Java Card documentation web site at https://docs.oracle.com/javacard.
Java Card 3 Platform Programming Notes, Classic Edition, Version 3.0.5	This document contains tips and guidelines for developers of Java Card applets, applications, and vendor-specific frameworks. This document is not required for developers to use the Java Card Development Kit; but it does provide useful tips and guidelines for developers who are creating Java Card applets, applications, and vendor-specific frameworks. It is available in HTML, PDF, ePub, and Mobi formats from the Oracle Java Card documentation web site at https://docs.oracle.com/javacard.
Java Card 3 Platform Specifications bundle	This bundle contains the Java Card Runtime and the Java Card Virtual Machine specifications for the Java Card 3 Platform, Classic Edition, Version 3.0.5 and later. These specifications are only available in PDF format. You can download the `.zip` file containing the specifications from http://www.oracle.com/technetwork/java/embedded/javacard/downloads/index.html. The Specification Release Notes are available from the Oracle Java Card documentation web site at https://docs.oracle.com/javacard.
API documentation	The API documentation for the Java Card 3 Platform is provided in the development kit installation (see Contents of the Development Kit) and is only available in HTML format. You can also view the API documentation from the Oracle Java Card documentation web site at https://docs.oracle.com/javacard.

Product Information

The public Java Card technology web site is http://www.oracle.com/technetwork/java/embedded/javacard/overview/index.html.

We greatly appreciate your feedback on this reference implementation. Send email with your feedback for this release to:

javacard-docs_ww@oracle.com

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Java Card Development Kit Release Notes, for Java Card 3 Platform, Classic Edition, Version 3.0.5u3
E62057-06

Release notes for Java Card 3 Platform, Classic Edition.