Java Card Development Kit

Simulator Release Notes

Version 25.0

F92101-07

April 2025

Table of Contents

Introduction

Java Card technology enables secure elements, such as smart cards and other tamper-resistant security chips to host applications called applets, which employ Java technology.

Java Card technology offers a secure and interoperable execution platform that can store and update multiple applications on a single resource constrained device, while retaining the highest certification levels and compatibility with standards. Java Card developers can build, test, and deploy applications and services rapidly and securely. This accelerated process reduces development costs, increases product differentiation, and enhances value to the customers.

The Java Card Development Kit is a suite of tools for designing implementations of Java Card technology and developing applets based on the Java Card Specifications. It is available as two independent downloads:

- The Java Card Development Kit Tools are used to convert and verify Java Card applications.

- The Java Card Development Kit Simulator offers a testing and debugging reference for Java Card applications. It includes a Java Card simulation environment and Eclipse plug-in.

Together, these two downloads provide a complete, stand-alone development environment in which applications written for the Java Card platform can be developed and tested.

These release notes describe the Java Card Development Kit Simulator, Version 25.0, which is based on version 3.2 of the Java Card Platform Specifications.

What's New

The complete set of Java Card Development Kit Simulator and Eclipse Plugin features is described in the Java Card Development Kit Simulator User Guide v25.0 in the Java Card Documentation web site.

New Features

- Visual Studio Code – The Java Card Development Kit v25.0 provides a launch configuration which, together with the Oracle Java Platform Extension for Visual Studio Code, permits to develop, debug and test a Java Card application using Visual Studio Code, while benefiting from features like formatting and linting.

- Simulator - OpenSSL – The Java Card Development Kit Simulator is delivered with the OpenSSL shared library 3.0 updated to the version 3.0.16 for 32-bit machine architecture.

- Simulator - Java Card API – Add the support for AES with Counter mode – CTR. A Cipher object instantiated with `Cipher.ALG_AES_CTR` or `Cipher.CIPHER_AES_CTR` constants permits to process blocks of data that may not have been received in their final order. That is, it allows for pipelining and parallelization.

- Simulator - GlobalPlatform – the security mechanism used to protect the integrity of the Java Card applications installed on the platform now supports Load File Data Block Hash (LFDBH) with SHA-384 and SHA-512 algorithms in addition to the SHA-256 and SHA-1.

- Samples – the build script now uses `-release 10` to compile java source files generating class files with format version 54 instead of 51 and allowing the use of latest JDK versions (>JDK17). See Java Card Development Tools Release Notes v25.0 for more details.

Bug Fixes

- Simulator - JCAPI – Fix Cipher internal context update after a `doFinal` operation.

- Simulator - JCAPI – Fix issue in `Signature.getLength()` throwing `SecurityException` when using an EC key with shared domain parameters.

- Simulator – JCAPI – Fix issue in `Signature.getCipherAlgorithm()` returning incorrect constant for EDDSA (ed25519, ed448).

- Simulator - JCAPI – Fix issue in `KeyAgreement.generateSecret()` when incorrect public data is used for ALG_EC_PACE_GM.

- Simulator - GlobalPlatform – Fix the implementation of the `SecureChannelx2` interface:

  - Fix issue when input/output buffers are in NVM (Non-Volatile Memory).

- Fix issue when using invalid parameters.
- Simulator - GlobalPlatform – Fix Card Capability Information for privileges that may be assigned to Applications.
- Simulator - GlobalPlatform – Fix incorrect parameters when calling `Personalisation.processData()` or `Application.processData()` methods.
- Simulator - GlobalPlatform – Fix returned error status if DELETE command is sent without token in Delegated Management context.
- Eclipse Plugin – Fix the Load command invoked from the terminal.
- Eclipse Plugin - Fix support of a run configuration for a Java Card project including multiple CAP files.

System Requirements

This product is targeted for use on a PC running on the operating systems:

- Microsoft Windows for versions 10 or 11
- Ubuntu Linux 24.04 LTS or Oracle Linux 9

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

- **Java Development Kit** (JDK): This release has been verified and tested with **Oracle JDK 17 (64 bit version) and OpenJDK 17 (64 bit version)**. Download the JDK software from:

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

  Install it according to the instructions on the website.

- **Eclipse IDE**: Eclipse IDE is optional and is required only for using Eclipse plug-in. The Java Card Eclipse Plug-in requires **Eclipse 2024-06 (4.32) and JDK 17**. Download the Windows Eclipse IDE from the following URL, and install it according to instructions on the website:

  https://www.eclipse.org/

- **Visual Studio Code IDE**: Visual Studio Code IDE and the Oracle Java is optional and is required only for integrating a Java Card project within this IDE. The version against which the Java Card Development Kit Simulator has been validated is **v1.97.2**. Download the Visual Studio Code IDE from the following URL, and install it according to instructions on the website:

  https://code.visualstudio.com/download

- **Java Extension for Visual Studio Code**: Java Extension for Visual Studio Code is optional and is required only for integrating a Java Card project within this IDE. The version against which the Java Card Development Kit Simulator has been validated is **v23.1.0**. Install Java Extension for Visual Studio Code from the following URL, and install it according to instructions on the website: https://marketplace.visualstudio.com/items?itemName=Oracle.oracle-java

Installation

The Java Card Specifications, Development Kit Simulator, and Development Kit Tools must be downloaded and installed individually.

- See the Downloading the Specification Documents topic of the *Java Card Platform Specification Release Notes, Version 3.2* for more details on how to download the Java Card Specification bundle.

- See the Installation topic of the *Java Card Development Kit User Guide* for more details on how to install the Java Card Development Kit Simulator and Java Card Development Kit Tools.

Contents of the Development Kit Simulator

This release of the Java Card Development Kit Simulator contains Java Card simulation environment and Eclipse plug-in.

The following table describes the files and directories that are installed in the root installation directory (*JC_HOME_SIMULATOR*).

Directory/File	Description
client	Contains client components: an application management service API (`AMService.jar` file and javadoc documentation), a communication smartcardio API (`socketprovider.jar` file) and a debugger proxy (`jc-debug-proxy.jar` file) to manage, communicate, and debug Java Card applications.
drivers	It is only for the Linux version. It contains the IFD Handler (`libjcsdkifdh.so`) for PCSCLite allowing an application to communicate with the Java Card Development Kit Simulator based on PC/SC.
runtime	Contains the Java Card Development Kit Simulator binary executable as well as the OpenSSL shared library 3.0 (32-bit).
samples	Contains sample applets and the corresponding client applications.
tools	Contains a tool to configure the Java Card Development Kit Simulator (`Configurator.jar`) with a secure channel protocol key set and a Global PIN.

Known Issues

There are no known issues.

Documentation

The Java Card Documentation web site provides online product documentation for the Java Card Platform.

Document	Description
Java Card Platform Specifications.	The following specification documents are available for the Java Card Platform, Version 3.2: • *Java Card Platform Runtime Environment Specification, Classic Edition, Version 3.2* (PDF format) • *Java Card Platform Virtual Machine Specification, Classic Edition, Version 3.2* (PDF format) • *Java Card Platform Application Programming Interface, Classic Edition, Version 3.2* (HTML format) • *Java Card Platform Specification Release Notes, Version 3.2* (HTML and PDF formats)
Java Card Options List	This document describes the list of options available to implement a Java Card platform, based on the Java Card Specifications.
Java Card Development Kit Simulator - User Guide	This document describes how to use the Java Card Development Kit Simulator and Eclipse plugin to develop, test and debug applications for Java Card Platform. It is available in HTML and PDF formats.
Java Card Development Kit Tools - User Guide	This document describes how to use the Java Card Development Kit Tools to convert and verify applications for Java Card Platform. It is available in HTML and PDF formats.

Product Information

The Java Card Technology website provides useful information about the Java Card product.

Visit the Java Card Technology website to access the most up-to-date information on the following:

• Product news and reviews

• Release notes and product documentation

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at https://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 https://www.oracle.com/pls/ topic/ lookup?ctx=acc&id=info or visit https://www.oracle.com/pls/topic/lookup? ctx=acc&id=trsif you are hearing impaired.

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 customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.