

# Java Card Development Kit

## A One-Stop Solution for Applet Development

November 27, 2024

Nicolas Ponsini  
Consulting Product Manager  
Java Platform Group

Syamkumar Cheedela  
Lead Principal Engineer



ORACLE



# Agenda

## Java Card Development Kit Features

What is the purpose ?

Which features are offered ?

## Java Card Development Kit Workflow

How to create and configure a project ?

How to develop and debug an Applet ?

How to test and integrate with other tools ?

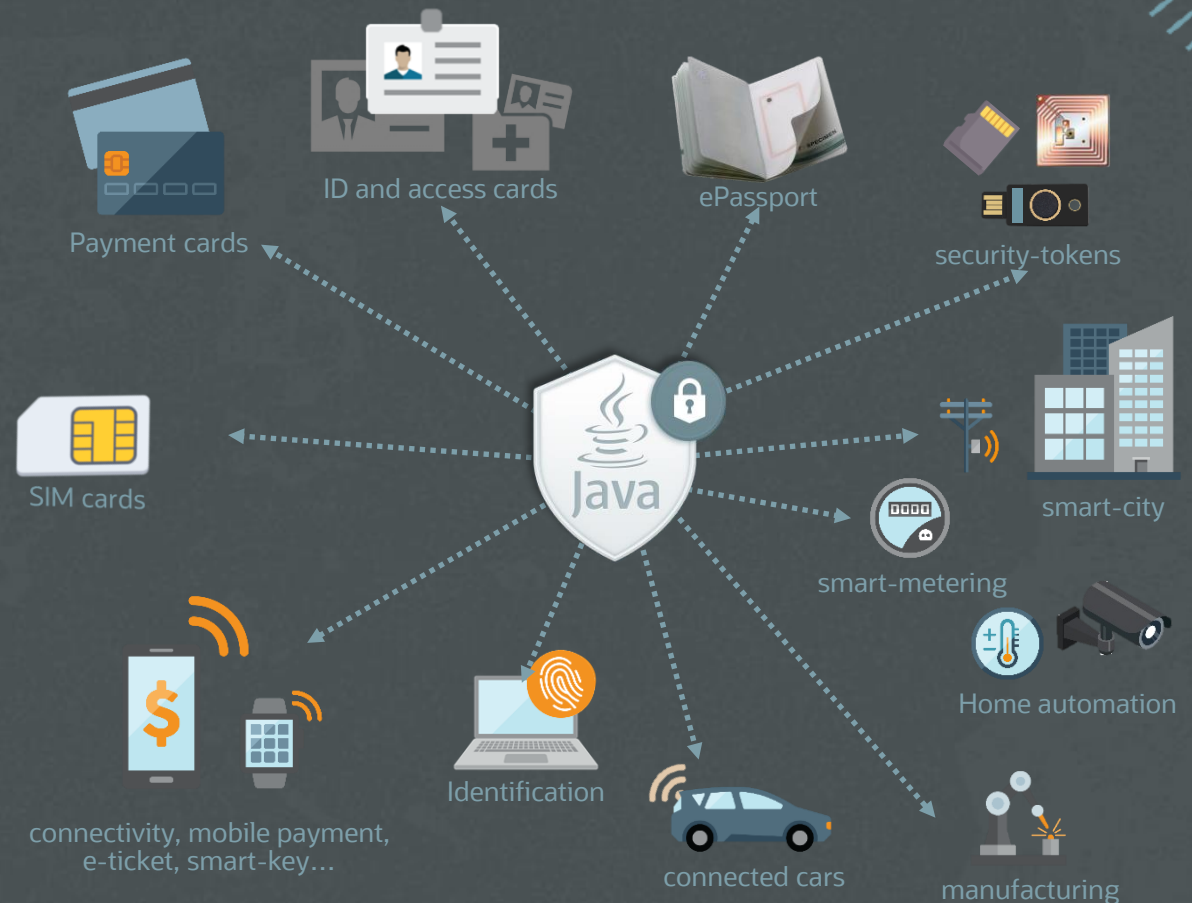
# Java Card Development Kit

## What is the purpose ?



# Java Card

Reference Platform  
for  
Secure Elements



2023 Webinar: An Introduction to Java Card – Basics for developers



# Purpose



Facilitate  
the Java Card application development  
path to final products



## Support Latest Version of Java Card Specification



- Demonstrate most advanced features
- Cover most optional specification features

## Facilitate Application Testing



- Integrate with users' tools
- Integrate with users' infrastructure

## A standalone Development Environment on PC/Laptop



- Windows and Linux
- No card / No card reader
- Tools and IDE Plugin for development

## Full Debugging Support



- Java Card Applet debugging with IDE
- Various tools to send commands

## Compatibility with Standards



- Communication protocols
- Deployment and management mechanisms

# Components

## Tools

The Java Card Development Kit Tools are used to convert and verify Java Card applications. The Tools can be used with products based on version 3.2 of the Java Card specifications, and can also be used with products based on versions, 3.0.5 and 3.1 of the Java Card Platform specifications.



## Simulator



The Java Card Development Kit Simulator offers a runtime reference to Java Card applications. It implements the version 3.2 of the Java Card specifications.

Available for Windows and Linux.

## Plugin for Eclipse IDE

The Java Card Development Kit Eclipse Plug-in offers an easy path for developing, testing and debugging Java Card applications.



# Resources on Oracle website

Download

Documentation

Developer Forum

Java Card Downloads

Learn more about Java Card technology Developer Forum

Development Kit Specification Protection Profile Archive

**ABOUT THE JAVA CARD DEVELOPMENT KIT**

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


- The Java Card Development Kit Tools are used to convert and verify Java Card applications. The Tools can be used with products based on version 3.2 of the Java Card specifications, and can also be used with products based on versions 3.0.4, 3.0.5 and 3.1 of the Java Card Platform specifications, Classic Edition.
- The Java Card Development Kit Simulator offers a runtime reference to Java Card applications. It implements the version 3.2 of the Java Card specifications.
- The Java Card Development Kit Eclipse Plug-in offers an easy path for developing, testing and debugging Java Card applications.

Together, these three downloads provide a complete, stand-alone development environment in which applications written for the Java Card platform can be developed and tested. For more information on the Java Card Development Kit, refer to the Release Notes and the User Guides. The Java Card Development Kit Simulator is only designed as an example of the functional behavior of a Java Card runtime. Always make sure to download the latest Java Card Development Kit Tools for up-to-date security. For more information on the Java Card Development Kit, refer to the User Guide.

**Tools Simulator**

Product/file description	File size	Download
Java Card Development Kit Simulator 24.1 for Windows	3.03 MB	<a href="#">java_card_devkit_simulator-win-bin-v241-b_289-06-OCT-2024.zip</a>
Java Card Development Kit Simulator 24.1 for Linux	1.80 MB	<a href="#">java_card_devkit_simulator-linux-bin-v241-b_289-06-OCT-2024.tar.gz</a>
Java Card Development Kit Eclipse Plug-in 24.1	1.79 MB	<a href="#">java_card_devkit_eclipse_plugin-bin-v241-b_274-06-OCT-2024.zip</a>

[www.oracle.com/java/technologies/javacard-downloads.html](http://www.oracle.com/java/technologies/javacard-downloads.html)

 **Development Kit**

**Simulator 24.1**  
[User Guide](#)  
[Release Notes](#)

**Tools v24.1**  
[User Guide](#)  
[Release Notes](#)

**Licensing Information User Manual v24.1**  
**LIUM**

[Download Development Kit](#)

[docs.oracle.com/en/java/javacard/index.html](https://docs.oracle.com/en/java/javacard/index.html)

Forums Search... Sign In

Java Card

**Announcement**

For appeals, questions and feedback about Oracle Forums, please email [oracle-forums-moderators\\_us@oracle.com](mailto:oracle-forums-moderators_us@oracle.com). Technical questions should be asked in the appropriate category. Thank you!

Interested in getting your voice heard by members of the Developer Marketing team at Oracle? Check out this post for AppDev or this post for AI focus group information.

**How to develop JCRE on my empty card?**

Started by 17068582-7762-473d-9390-c9581f148603 in Java Card --- 92 minutes ago 0 comments 3 views

[17048582-7762-473d-939...](#) created 92 minutes ago

Tap to Filter by tags

Show posts that include all selected tags

[forums.oracle.com/ords/apexds/domain/dev-community/category/java-card](https://forums.oracle.com/ords/apexds/domain/dev-community/category/java-card)





# Releases

Java Card Development Kit 24.0 - February 2024

Java Card Development Kit 24.1 - October 2024



[Java Card Home](#) [JCDK24.1 Download](#) [JCDK24.1 Release Notes](#) [JCDK24.1 User Guides](#) [Developer Forum](#) [Blog](#)





# Java Card Development Kit Features

# Java Card 3.2

- The Java Card Development Kit Simulator supports version 3.2 of the Java Card Platform specifications.
- The following Java Card optional features and packages are supported by the Java Card Development Kit Simulator:

## Options Framework and Extensions

- **Core**  
Integer Support  
Extended Length APDU  
Encodings for 4 or 20 Logical Channels  
Object Deletion  
ByteBuffer
- **Utilities**  
StringUtil  
BCDUtil, BigInteger and ParityBit classes  
TLV parser
- **Extended CAP files**  
>64K and multiple packages

## Options Security Assets and Protocols

- **Sensitive Result**  
Assert results of operations for control-flow integrity
- **Sensitive Arrays**  
Assert integrity of arrays
- **System Time API**  
Time duration management
- **Certificate API**  
Optimize storage and certificate parsing
- **Monotonic Counter API**  
Anti-replay functions



# Java Card 3.2



## Cryptography

- **Digest API**  
to create a hash of data using SHA256, SHA384...
- **Random numbers API**  
deterministic (DRBG)
- **Digital Signature API**  
to sign and verify using DES, AES, DSA, RSA, HMAC, ECDSA, EDDSA...
- **Encryption/Decryption API**  
to encrypt or decrypt using DES, AES, RSA, AEAD...
- **Key Agreement API**  
to perform Diffie-Hellman key exchange (including ECDH with curves X25519, X448, ...)
- **Key derivation API**  
to derive keys (HKDF)

	Algorithms	Operations	Keys
Symmetric Cryptography	NIST SP 800-90A DRBG	Pseudo Random Generation	-
	CRC16, CRC32	Checksum	-
	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, MD5, RIPEMD-160	Message Digest	-
	HMAC (SHA-1, SHA-256)	Signature	up to 512 bits
	HKDF (SHA-1, SHA-256)	Key Derivation	up to 512 bits
	DES 3DES (2 keys, 3 keys)	Cipher, MAC Modes: ECB, CBC Paddings: ISO 9797 (M1,M2), PKCS5	64, 128, 192 bits
	AES	Cipher, AEAD, MAC Modes: ECB, CBC, CFB, XTS, CCM, GCM Paddings: ISO 9797 (M1,M2), PKCS5	128, 192, 256 bits
	Korean Seed	Cipher, MAC Modes: ECB, CBC	128 bits
	DSA	Signature	1024, 2048 bits
	RSA	Cipher, Signature schemes: PKCS1, PSS, OAEP	up to 4096 bits
Asymmetric Cryptography	DH	Key Agreement	1024, 2048 bits
	ECC	ECDSA, EdDSA Signature ECDH & PACE Key Agreement	ECC FP (112 to 521 bits) ECC F2m (112 to 521 bits) Edwards Curves (25519, 448)



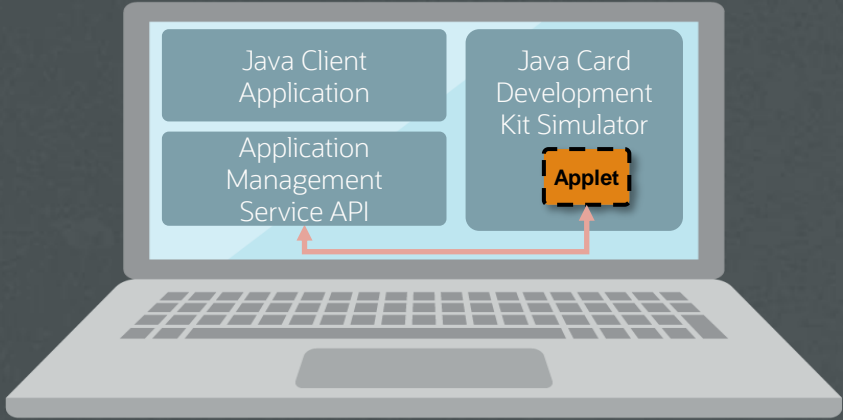


# Application Management

- Compliant with GlobalPlatform Common Implementation Configuration v2.1
- Enables the management of multiple hierarchies of GlobalPlatform security domains, reflecting the various business cases and models established by the Secure Element industry.

GlobalPlatform Privileges		GlobalPlatform Commands	
<ul style="list-style-type: none"><li>• Security Domain (SSD support)</li><li>• DAP verification</li><li>• Delegated Management</li><li>• Card Lock</li><li>• Card Terminate</li><li>• Card Reset</li><li>• CVM Management</li><li>• Mandated DAP Verification</li><li>• Trusted Path</li></ul>	<ul style="list-style-type: none"><li>• Authorized Management</li><li>• Token Verification</li><li>• Global Delete</li><li>• Global Lock</li><li>• Global Registry</li><li>• Final Application</li><li>• Global Service</li><li>• Receipt Generation</li><li>• Ciphred Load File Data Block</li></ul>	<ul style="list-style-type: none"><li>• DELETE</li><li>• GET DATA</li><li>• GET STATUS</li><li>• INTALL<ul style="list-style-type: none"><li>◦ for load</li><li>◦ for install</li><li>◦ for make selectable</li><li>◦ for personalization</li><li>◦ for extradition</li><li>◦ for registry update</li></ul></li></ul>	<ul style="list-style-type: none"><li>• LOAD</li><li>• MANAGE CHANNEL</li><li>• SET STATUS</li><li>• PUT KEY</li><li>• STORE DATA</li></ul>

GlobalPlatform Card Specification v2.3.1, 2018  
GlobalPlatform Card API (org.globalplatform) v1.6  
GloaPlatform Secure Channel Protocol '03' – Amendment D v1.2



A proprietary Java API (**Application Management Service API**) to perform a few application management operations is delivered with the Development Kit (amservice.jar)

Note: Other APIs or tools can be used (or reused) c.f. next slides



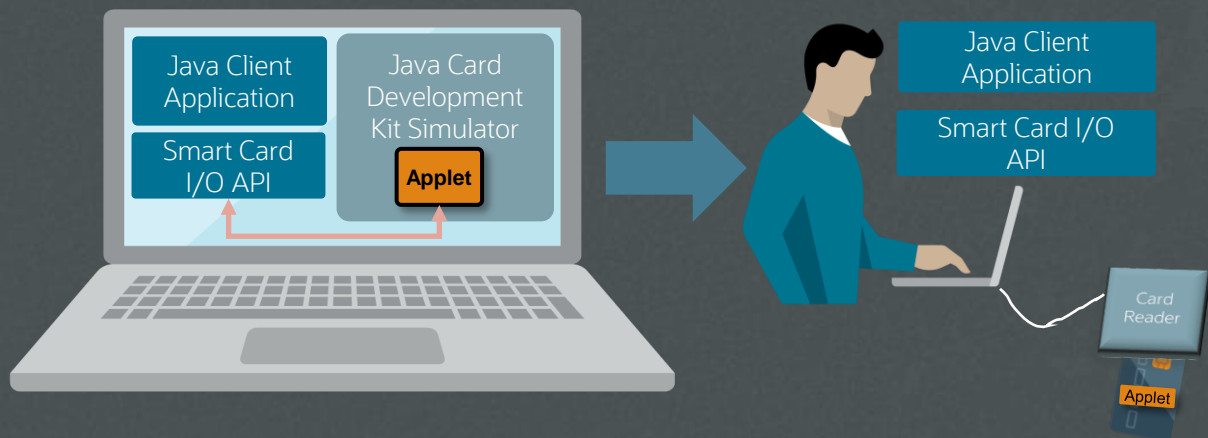


# Communication

The API and/or interface allowing communication with a smart card from a host environment are based on standards.

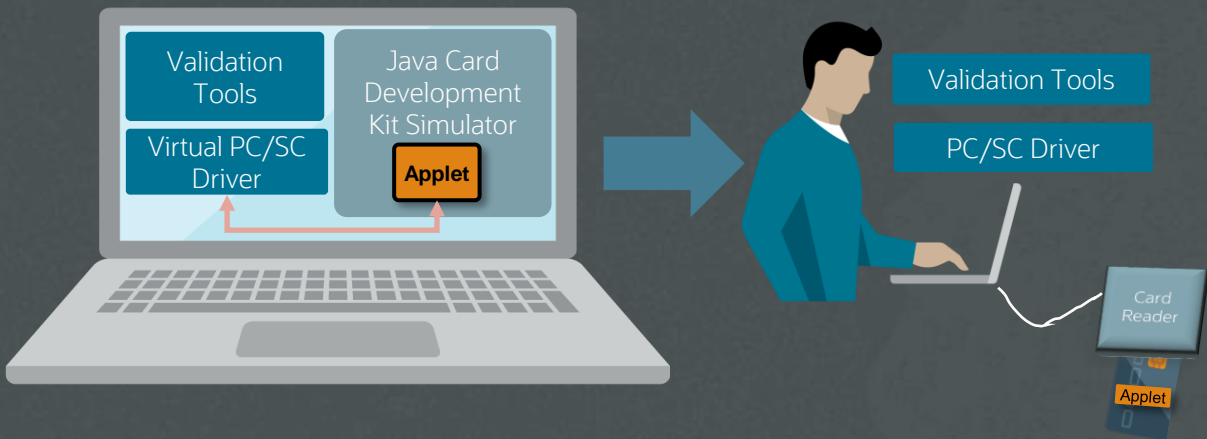
## Smart Card I/O

Java™ Smart Card I/O API (javax.smartcardio): This package defines a Java API for communication with Smart Cards using ISO/IEC 7816-4 APDUs, which allows Java applications to interact with applications running on the Smart Card, to store and retrieve data on the card, etc.



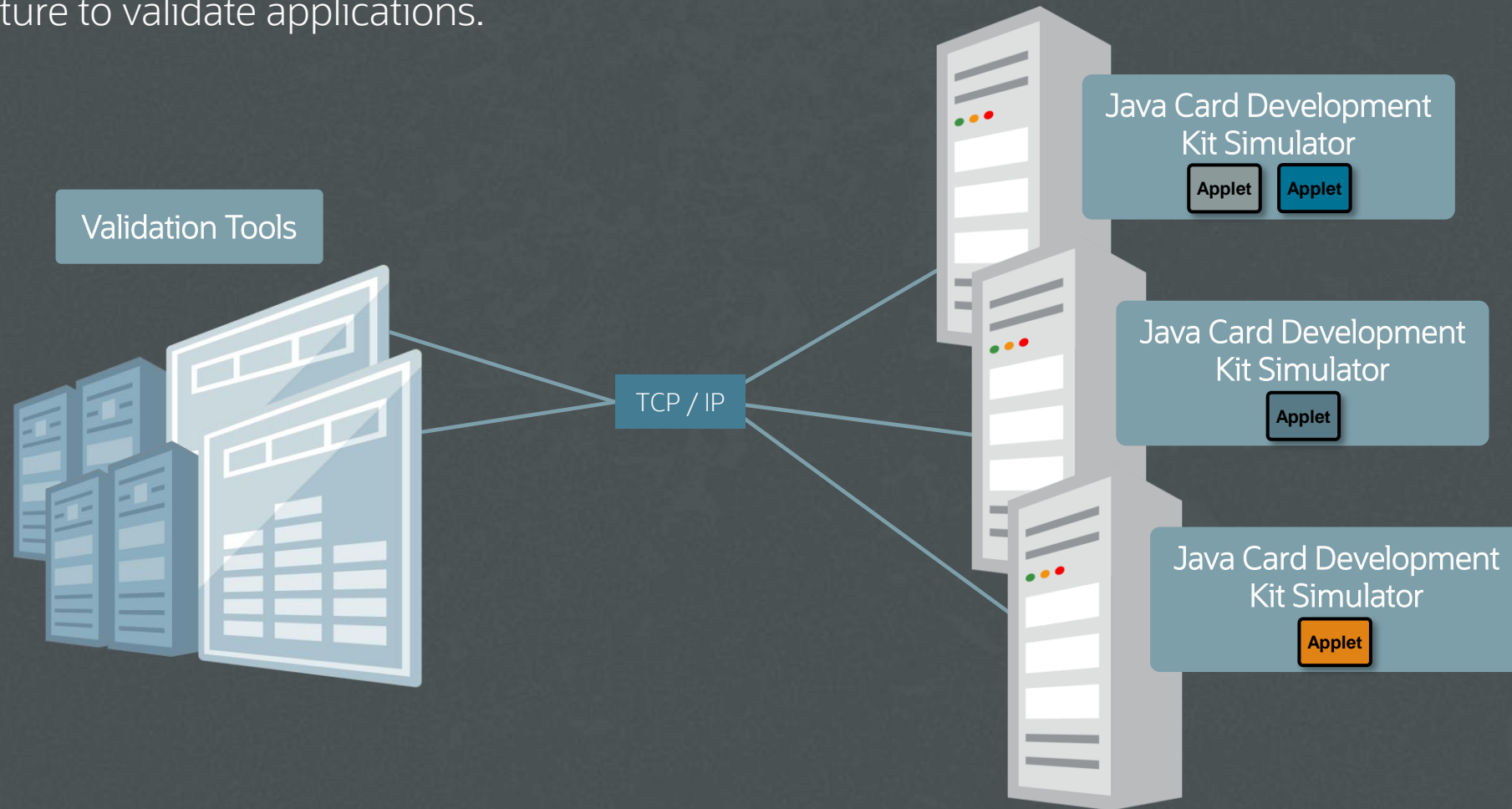
## PCSC\*

PCSC interface allows to communicate with the simulator as if it were a card reader.



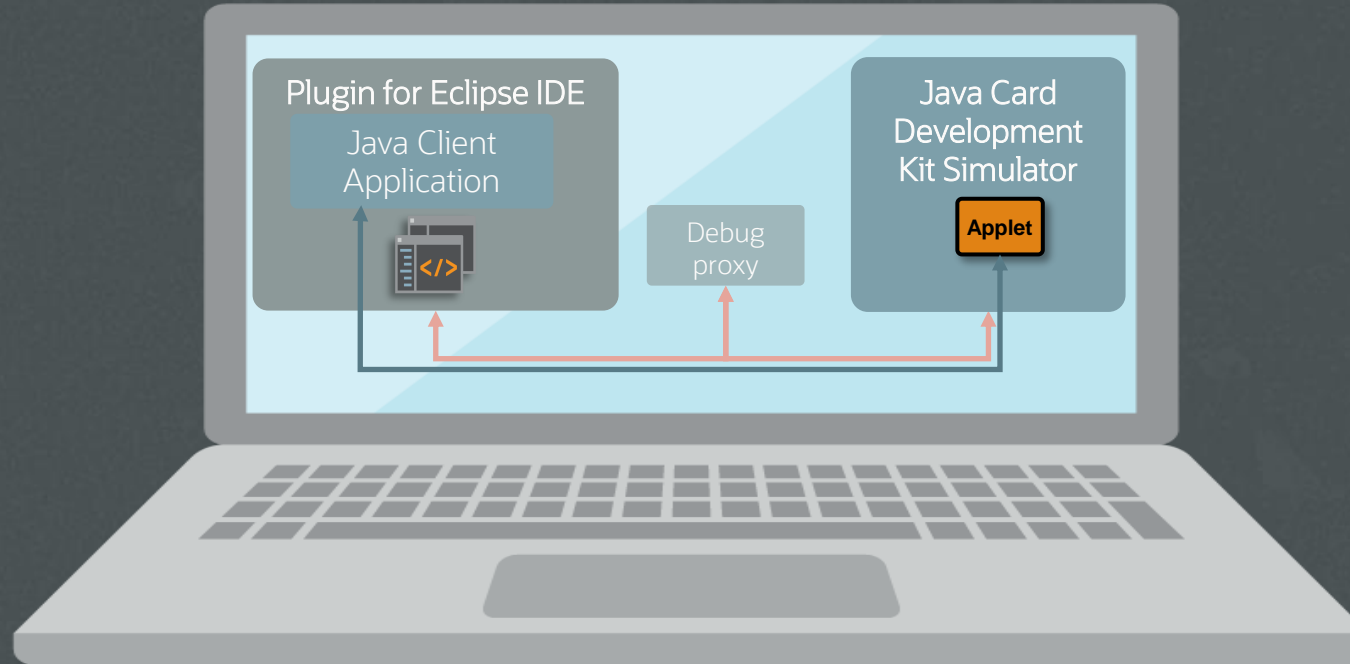
# Facilitate Testing

The transport layer is based on sockets allowing for various possibilities to integrate in an existing infrastructure to validate applications.



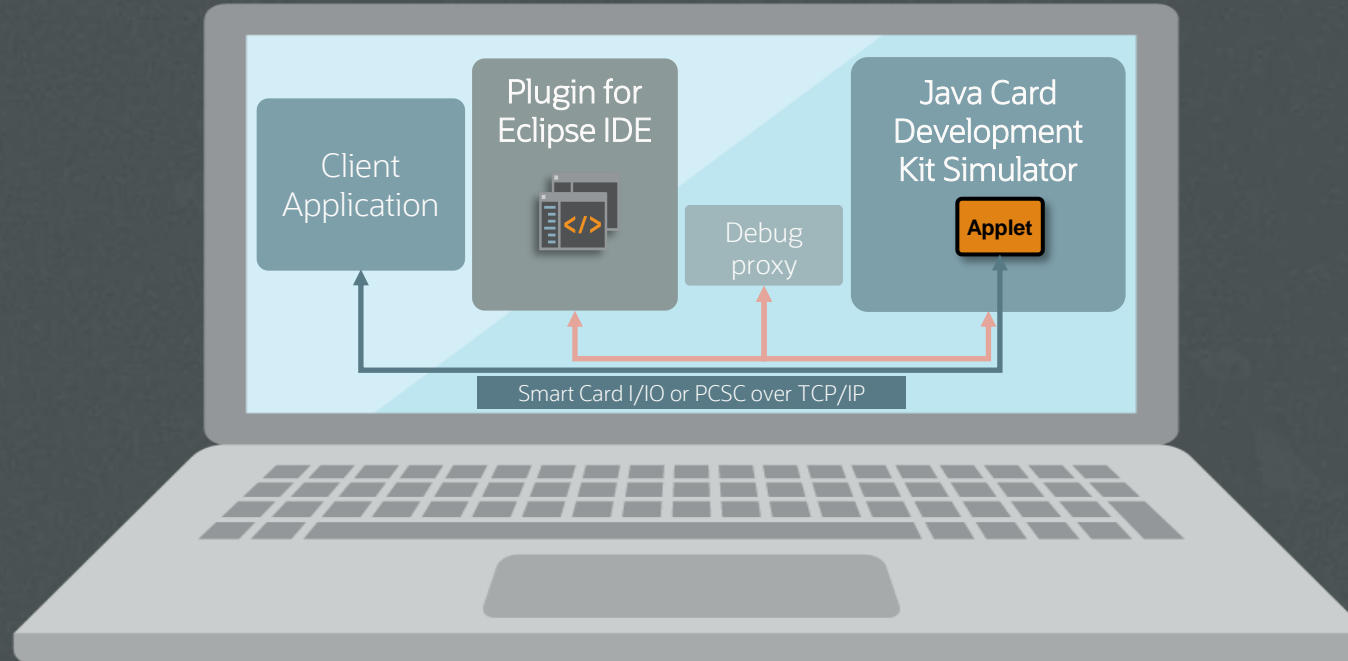
# Debugging

- The Java Card Development Kit Eclipse Plug-in offers an easy path for debugging Java Card applications.



# Debugging

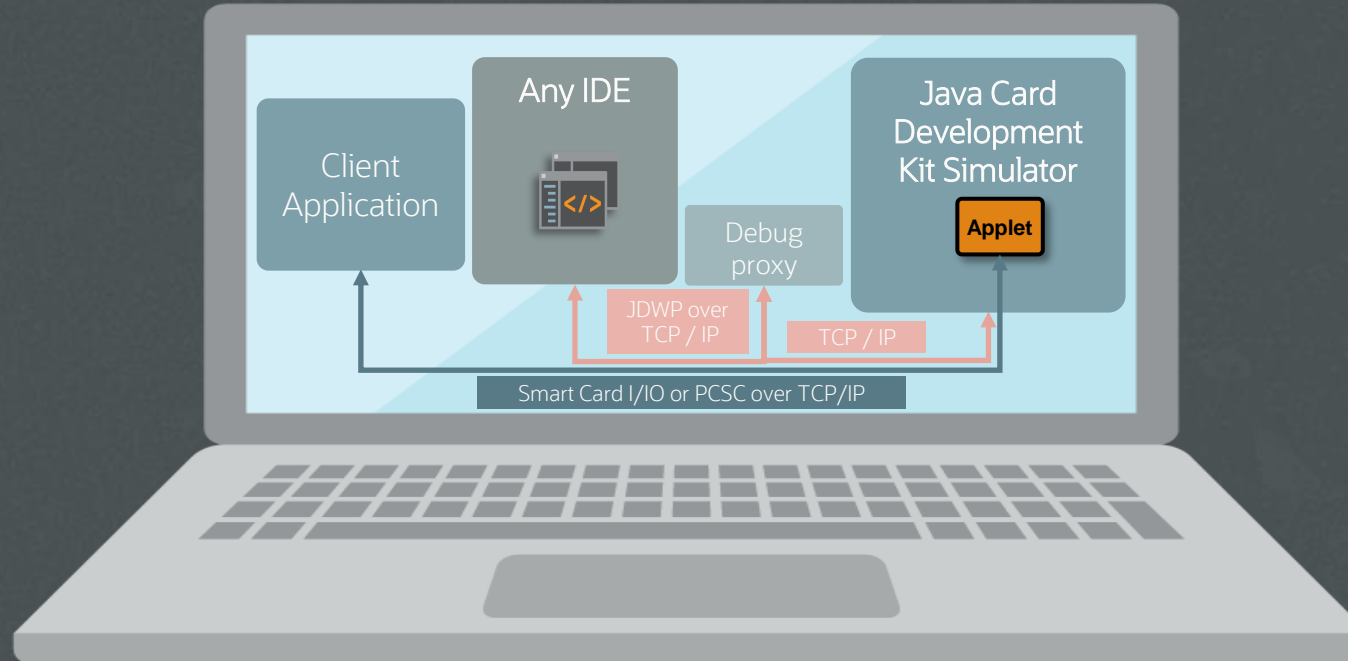
- Many combinations are possible
  - Client Applications can be outside the Plugin for Eclipse IDE





# Debugging

- Many combinations are possible
  - Client Applications can be outside the Plugin for Eclipse IDE
  - Another IDE can also be used for debugging applets



# Java Card Specifications & Development Kit



## Java Card Specification

Latest release of the Java Card specification and the reference for Java Card products.

<https://docs.oracle.com/en/java/javacard/3.2/>

PACKAGE	CLASS	TYPE	DEPRECATED	INDEX	HELP
ALL CLASSES					
Java Card™ Platform, Application Programming Interface, Classic Edition Version 3.2					
This is the Application Programming Interface (API) for the Java Card™ Platform, Classic Edition, Version 3.2.					
The list of packages is divided into two groups:					
• Core packages - mandatory packages providing the core features of the Java Card platform					
• Extension packages - optional packages providing specific features. These may not necessarily be available on all implementations of the Java Card Platform.					
All Packages	Core packages	Extension packages			
Package			Description		
java.io			Defines a subset of the Java .io package in the standard Java programming language.		
java.lang			Provides classes that are fundamental to the design of the Java Card technology subset of the Java program		
java.rmi			Defines the Remote interface which identifies interfaces whose methods can be invoked from card acceptance		
javacard.framework			Provides a framework of classes and interfaces for building, communicating with and working with Java Car		
javacard.framework.service			This optional extension package provides a service framework of classes and interfaces that allow a Java Car		
javacard.security			Provides classes and interfaces that contain publicly-available functionality for implementing a security and		
javacard.annotations			Extension package that contains annotations for defining character string constants.		
javacard.apdu			Extension package that enables support for ISO/IEC specification defined optional APDU related mechanis		
javacard.apdu.util			Extension package that contains the APDUUtil class which contains utility functions to parse CLA byte from		
javacard.biometry			Extension package that contains functionality for implementing a biometric framework on the Java Card plat		
javacard.biometry.t10n			Extension package that contains functionality for implementing a t10N biometric framework on the Java Card		
javacard.crypto			Extension package that contains functionality, which may be subject to export controls, for implementing a security and cryptography framework on the Java Card platform.		
javacard.external			Extension package that provides mechanisms to access memory subsystems which are not directly addressable by the Java Card runtime environment (Java Card RE) on the Java Card platform.		
javacard.framework.event			Extension package that defines a framework to handle different source of events.		
javacard.framework.math			Extension package to perfor		
javacard.framework.nio			Extension package that defi		
javacard.framework.string			Extension package that defi		
javacard.framework.time			Extension package that defi		
javacard.framework.tv			Extension package for manu		
javacard.framework.util			Extension package that con		
javacard.framework.util.intx			Extension package that con		
javacard.security			Extension package that con		
javacard.security.cert			Extension package that pro		
javacard.security.derivation			Extension package that pro		

Home / Java / Java Card Platform / 3.2

## Java Card 3.2 Documentation

Home



### Specifications

API Documentation  
Runtime Environment Specificati  
Virtual Machine Specification  
Specification Release Notes  
Java Card Platform Specification Download Page  
Java Card Options List

Java Card System – Open  
Configuration Protection  
Profile

Java Card™ Platform

Virtual Machine Specification, Classic Edition

Version 3.2

January 2023

IER TLV formatted data in I/O buffers.



## Java Card Development Kit Tools

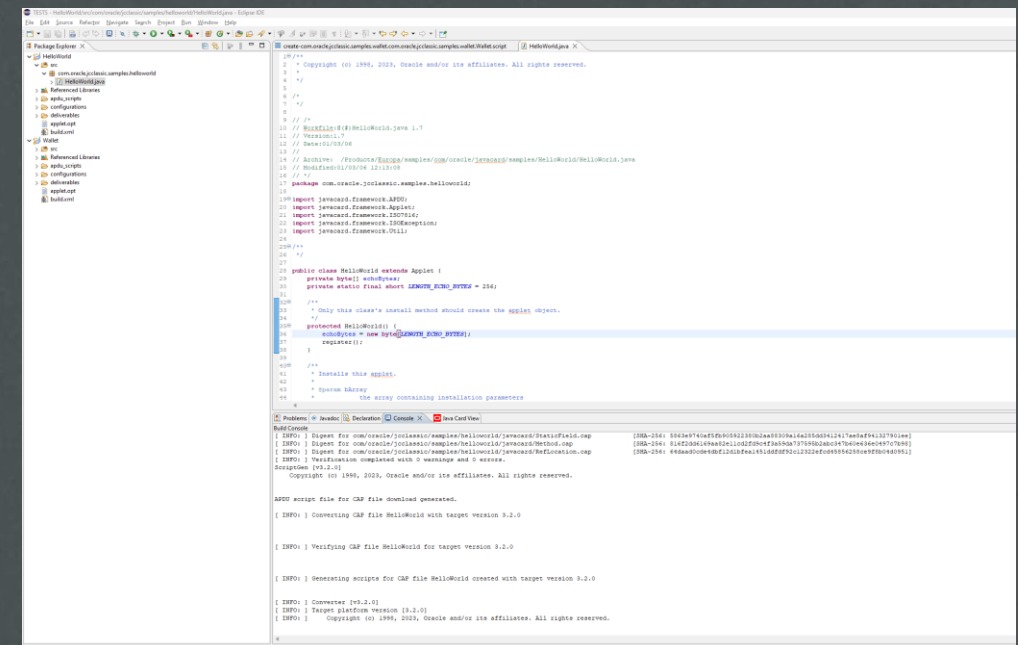
Used to convert and verify Java Card applications.

<https://www.oracle.com/java/technologies/javacard-sdk-downloads.html>

## Java Card Development Kit Simulator

A simulator component and Eclipse plug-in.

<https://www.oracle.com/java/technologies/javacard-sdk-downloads.html>





# Thank You