achelos
the experts in eID

JC Inspector – Test Suite for Secure Java Cards™

Make Security and Quality Visible

Attacks on Java Cards are no Rarity

In addition to payment applications a variety of other applications can be installed simultaneously on a multi-application Java Card™. The firewall of the Java Card has the task to securely separate applications from each other and to protect data from unauthorised access, spying or manipulation.

Firewall attacks are often detected only after e.g. a credit card has been misused. Apart from a high loss of reputation and trust, unexpected consequential damage may arise, especially when payment applications have been accessed.

Areas of Application and Potential Hazards

Java Card technology is increasingly being built into devices as an embedded solution, e.g. (e)UICC. As a central communication unit, it is therefore becoming a target for hackers. achelos experts have developed test suites that are suited for various target groups:

- Issuers
- System integrators
- Test laboratories
- Service providers
- Network providers
- Chip card manufacturers

With JC Inspector you can reliably test the security and quality of your Java Card solution, even in the embedded area.

SecurITy
made in Germany
Trust Seal
www.teletrust.de/itsmig

JC Inspector is the ideal extension for the official Java Card TCK test suite*. With more than 20,000 test cases, JC Inspector is one of the most comprehensive Java Card test suites on the market. In this test depth it highlights a large variety of test aspects and offers ideal protection for your Java Card.

JC Inspector

JC Inspector + Qumate.Testcenter = Flexible Test Management for Java Cards

Based on the high-performance Qumate.Testcenter from achelos, the JC Inspector was developed for the Qumate.Security.World. With this powerful combination you can conveniently apply automated security, functionality and conformity checks to your Java Card solution before and after development, as well as in the field. JC Inspector reveals weak points in the implementation of a Java Card. Risks become apparent and, if necessary, protective measures can be applied immediately.

achelos particularly focuses on the security and function of the firewall, the virtual machine (VM) and the cryptography of a Java Card. To test a large range of cards, the tests cover all cards back to JC version 2.2.1.

Qumate.Testcenter contains comprehensive reporting and debugging options for professional and verifiable test management. It helps analyse the detected errors. JC Inspector and Qumate.Testcenter are entirely implemented in Java, which makes them quick and efficient to adapt and extend, even without special knowledge.

* Java Card Technology Compatibility Kit (Java Card TCK) and the test bench. This software was developed by Oracle.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

achelos
the experts in eID

Safeguard the Integrity of your Java Card

A variety of Java cards have no way to check the integrity of the loaded applets during installation on the card Correct behaviour according to Java Card specifications is indispensable, especially for the functioning of security-critical components of the Java Card operating system, such as the firewall of the runtime environment, the virtual machine or the crypto API.

JC Inspector from achelos supports a large number of Java Card versions (back to version 2.2.1) and types, such as (e)UICC, EMV or M2M. The test suite exclusively uses official Java Card and GlobalPlatform interfaces and protocols.

JC Inspector:

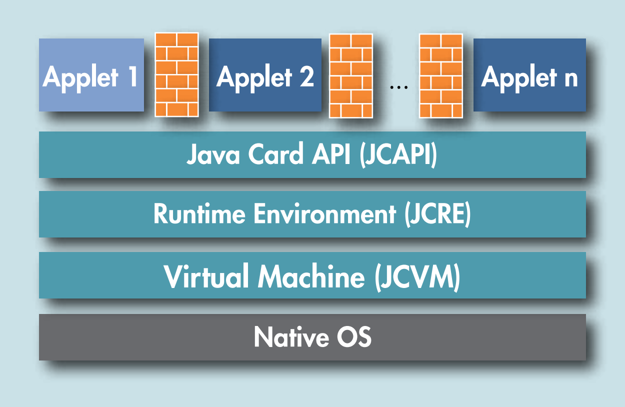
- Executes automated test cases
- Coordinates intelligent loading and
- Deleting of Java card applets
- Displays the test results in detail

Moreover, JC Inspector also includes the complete test specification of the tests so that detailed analysis of the detected errors and risks can be carried out by the user.

Intelligent Smart-Cap File-Loader Increases Test Suite Performance

The Smart-Cap File-Loader, developed by achelos for JC Inspector, is a tool for intelligent loading and deletion of test applets. By analysing the test plan to be executed, the Smart-Cap File-Loader prevents unnecessary loading or deletion processes of packages on the Java Card during test execution. This increases the performance of the test run and reduces the number of write accesses on the persistent memory of the Java Card.

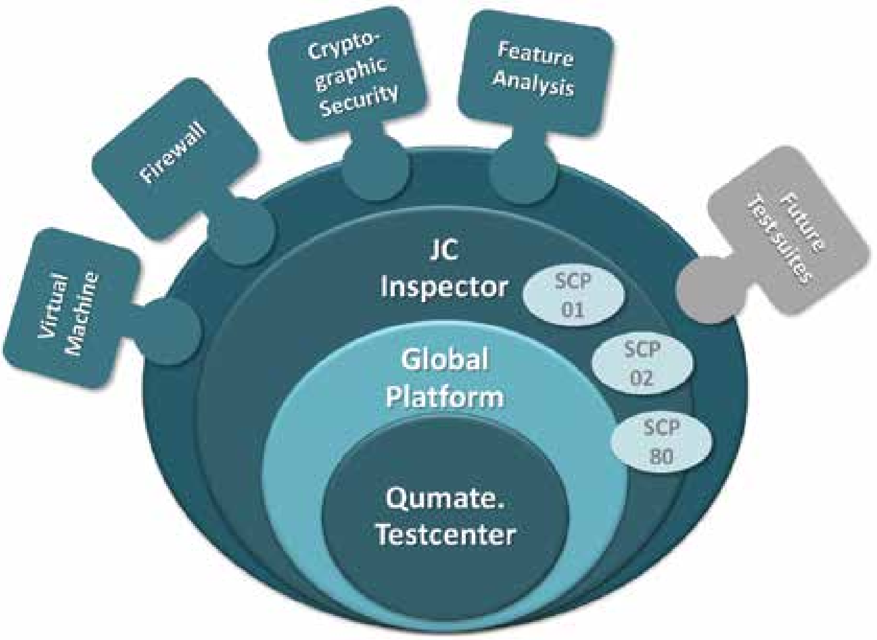
Java Card Platform



Check your Java Card with JC Inspector

With JC Inspector from achelos, you can check the functional security of Java Cards, the conformity with official specifications and the security of essential components, such as the Java Card firewall, virtual machine and cryptography.

Through high transparency and performance, JC Inspector enables test management at the highest level. Choose the best possible combination for your application from our various test suites. Tailored to meet the requirements of your project, we offer the following test suites from our JC Inspector series:



achelos
the experts in eID

Test Suites and Test Aspects - Overview

1. JC Inspector.Firewall.TS

The test suite controls the secure and correct implementation of the Java Card firewall. The tests check whether applets installed on the card have unauthorised mutual access to code or data (without shareable interface mechanism). The focus here is on accessing objects in the same or in different packages (so-called contexts). Furthermore, the correct implementation of JCRE entry point objects is checked.

The JC Inspector.Firewall.TS from achelos analyses, tests and logs all specified firewall rules with approx. 14,000 test cases. All applicable combinations of bytecodes, from bytecodes to objects/arrays and firewall contexts, are checked systematically.

2. JC Inspector.Cryptographic Security.TS

The test suite checks different aspects of a Java Card with respect to: Security of APIs, firewall and functionality.

- (in planning) Testing Aspect Cryptographic API:

Tests the correct implementation of the interfaces and the handling of the parameters passed.
The achelos experts know that a variety of APIs are not directly programmed in Java for performance reasons, but are implemented in native layers of the operating system. In order to exclude risks, the cryptographic API checks all parameters before execution for the valid range of values and correct behaviour, when used incorrectly.

- Testing Aspect Object Firewall:

Checks whether the crypto objects of a Java Card are accessed correctly. The approx. 3,000 test cases with their approximately 500,000 atomic tests systematically check all algorithms or crypto objects available on the Java Card for compliance with the specified firewall rules.

- (in planning) Testing Aspect Functionality:

All algorithms available on the Java Card and their correct calculation are checked. Standardised test vectors for e.g. DES, AES, RSA and ECC operations are used to verify the valid calculation of the various algorithms.

3. JC Inspector.Virtual Machine.TS

The test suite loads tests with instructions for the virtual machine of the Java Card as applets onto the test object. The virtual machine interprets the bytecodes in the loaded applets at runtime and translates these into the machine commands of the target platform. The tests check the correct behaviour of the Java Card with respect to the bytecodes to be executed, including variants against the official Java Card specification.

JC Inspector.Virtual Machine.TS contains approx. 1,600 test cases, from good case tests for numerous bytecodes to a large number of negative tests for each of these bytecodes. Particularly security-relevant bytecodes, e.g. check cast (checks object types and bytecodes, which are responsible for the access to defined fields and have to adhere to field boundaries) are explicitly checked by a large number of tests.

4. JC Inspector.Feature Analysis.TS

There is a wide range of different Java Cards on the market, which can be found in parameters, e.g. Java Card version, GlobalPlatform version, protocols, memory size, or additional preinstalled packages.
The JC.Inspector.Feature Analysis.Testsuite checks these and other key figures of a Java Card and logs them for further analysis purposes. Further, parts of this test suite serve as preliminary test for all aforementioned tests in order to ensure that only appropriate tests are executed on the test object.

With Feature Analysis.Test Suite, JC Inspector provides you with a tool that initially checks, analyses and documents the different features of a card. It generates a crypto profile of your Java Card that is used dynamically by the test suite. The test results clearly display the available and the non-available features of the Java Card. The analysis results are temporarily stored internally and support the efficient execution of the entire test.

These Features include, among others:

- Coding the ATR
- Content of the file control information of the issuer security domain
- AIDs of loaded packages and installed applets
- Supported cryptographic algorithms
- Supported key lengths
- Status and size of the non-volatile memory (NVM)

achelos
the experts in eID

Products and Solutions for a Secure Java Card

The achelos JC Inspector solution is complemented by a number of services and support services. Our experts will help you analyse and fix possible implementation errors, offer support with testing and the execution of test cases, writing automated tests and the certification process according to e.g. Common Criteria.

Our service and support services include:

Support:

- Launching and configuration support
- Error analysis and bug fixing
- Update Qumate.Testcenter (bug fixing)
- Jira ticketing system: for quick registration of the request or problem description

Additional Services:

- Upgrade of Test suites (new version of the official specification)
- Upgrade Qumate.Testcenter (new releases)
- Security analyses of Java cards based on JC Inspector
- Solution development for existing / detected security errors
- Custom extensions of JC Inspector, e.g.:
  - Additional secure channel protocols
  - Analysis and testing of proprietary Java Card packages

Continuous Extension with further Test Modules

Qumate.World

Qumate makes quality ... visible!

JC Inspector was developed by achelos and is based on Qumate.Testcenter. Managing requirements and test specifications, as well as the actual tests, form an integral part of Qumate.Testcenter. Qumate is continuously being extended with additional test modules and offers wide scope customer-specific solutions and implementations.

www.qumate-world.com

More Advantages at a Glance:

- Based on the Eclipse Rich client platform
- Modular architecture
- Extendible with customer plug-ins
- Automated test execution and report generation
- Easily modifiable tests
- Reproducible test results
- Professional documentation of test procedures

Technical Data:

Supported GP secure channel protocols	▪ SCP01 (i=05) ▪ SCP02 (i=15, i=55) ▪ SCP80 (planned)
Available test suites	▪ JC Inspector.Virtual Machine ▪ JC Inspector.Firewall ▪ JC Inspector.Cryptographic Security ▪ Object Firewall ▪ Crypto API (planned) ▪ Crypto functionality (planned) ▪ JC Inspector.Feature Analysis Testsuite (planned)
Number of test cases	▪ Approx. 20,000 tests
Supported standards	▪ Java Card specification as of version 2.2.1 ▪ GP as of version 2.1.1
Supported card readers	▪ PC/SC ▪ Micropross MP300 ▪ CT API ▪ SICCT
Database	▪ MySQL ▪ SQLite