# National Information Assurance Partnership


TM

# Common Criteria Evaluation and Validation Scheme Validation Report

## Innovation Data Processing

## FDRERASE Version 5.4, Level 50

**Report Number: CCEVS-VR-05-0109**

**Dated: 9 September 2005**

**Version: 1.7**

**National Institute of Standards and Technology**
**Information Technology Laboratory**
**100 Bureau Drive**
**Gaithersburg, MD 20899**

**National Security Agency**
**Information Assurance Directorate**
**9800 Savage Road STE 6740**
**Fort George G. Meade, MD 20755-6740**

## ACKNOWLEDGEMENTS

### Validator

Nicole M. Carlson
The Aerospace Corporation
El Segundo, California

The Validator also thanks Ms. Victoria Ashby, MITRE Corporation, for her support at TOE testing; and Dr. Deb Downs, for her work as Senior Validator.

### Common Criteria Testing Laboratory

Terrie Diaz, Lead Evaluator
Science Applications International Corporation (SAIC)
Columbia, Maryland

# Table of Contents

# 1. EXECUTIVE SUMMARY

This report documents assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Innovation Data Processing FDRERASE Version 5.4, Level 50 product. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in June 2005. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Extended and Part 3 Conformant**, and meets the assurance requirements of EAL 2 augmented with ADV_SPM.1 and ALC_FLR.2. The product is not conformant with any published Protection Profiles. All security functional requirements are derived from Part 2 of the Common Criteria or expressed in the form of Common Criteria Part 2 requirements.

Innovation's FDRERASE (the TOE) provides several functions that relate to secure erasure of data:

1. an "ERASE" function that overwrites data with zeroes;

2. a "SECURE ERASE" function that overwrites data with a random pattern, its binary complement, and a different random pattern;

3. a "VERIFY" function that randomly samples bits in the storage space assigned to the erased data to ensure that they were correctly overwritten.

Another function, "QUICK ERASE", is present in the product but is not part of the TOE. Though other functionality is present in the underlying product, the evaluation covered only these functions.

FDRERASE is a software-only TOE that is installed into a privileged library and may be used by privileged users.

During this validation, the validators monitored the activities of the SAIC evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test reports. The validator determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the validator concludes that the SAIC findings are accurate, the conclusions justified, and the conformance claims correct.

# 2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

**Table 1: Evaluation Identifiers**

| Item | Identifier |
|---|---|
| Evaluation Scheme | United States NIAP Common Criteria Evaluation and Validation Scheme |
| Target of Evaluation | Innovation FDRERASE Version 5.4, Level 50 |
| Protection Profile | None |
| Security Target | *Innovation FDRERASE Version 5.4, Level 50, Version 1.0, 1 July 2005* |
| Evaluation Technical Report | *Evaluation Technical Report for Innovation FDRERASE Version 5.4, Level 50*<br>• *Part 1 (Non-Proprietary), Version 3.0, 8 August 2005*<br>• *Part 2 (Propriety), Version 1.0, 7 July, 2005* |
| Conformance Result | Part 2 Extended and Part 3 Conformant, EAL 2 augmented with ADV_SPM.1 and ALC_FLR.2 |
| Sponsor | Innovation Data Processing |
| Developer | Innovation Data Processing |
| Evaluators | Science Applications International Corporation (SAIC) |
| Validator | The Aerospace Corporation |

# 3. SECURITY POLICY

Innovation FDRERASE Version 5.4, Level 50 provides security functions related to the secure erasure of data. Specifically, the TOE supports two grades[1] of secure erasure:

1. "ERASE": overwrites every track of the disk record with a track-length record, consisting of binary zeroes by default.

2. "SECURE ERASE": the data to be erased is overwritten at least three times; with a random pattern, its binary complement, and a different random pattern.

In addition, there is a "VERIFY" function, which samples bits on the Direct Access Storage Device (DASD) to ensure that the data has in fact been overwritten.

[1] A third grade of overwriting, "QUICK ERASE", is present in the product but is not part of the TOE.

# 4. ASSUMPTIONS

## 4.1. Usage Assumptions

A.Authorized_library

The TOE is installed in an authorized library in the TOE operating environment, such that only appropriately privileged users can install and execute it.

A.Competent_administration

The persons responsible for administration of the TOE environment and installation of the TOE are trusted, trained, competent, and follow all applicable guidance documentation.

A.Competent_use

The persons responsible for execution of the TOE are trusted, trained, competent, and follow all applicable guidance documentation.

A.DASDs_offline

All disks being overwritten are not accessible by user programs.

A.I&A

The TOE operating environment requires users to be identified and authenticated.

A.Secure_environment

The processing resources of the TOE will be located within controlled access facilities that will prevent unauthorized physical access. Furthermore, the underlying operating system operates correctly and is securely configured such that the operating system protects the TOE from any unauthorized users or processes.

A.Security_management

The TOE operating environment supports a security management role and functions to manage its access control policy.

A.Self_protection

The TOE operating environment ensures its own security functions cannot be bypassed, and protects itself from interference and tampering.

A.Proper_procedures

TOE users will abide by all higher authority directives, which could include a second person use of the TOE to verify the person executing the TOE overwrite operation did so on the intended disks, employing appropriate overwrite options.

A.Reliable_clock

The TOE operating environment includes a reliably functioning clock and issues a warning if there is no reliably functioning clock or the clock fails.

## 4.2. Environmental Assumptions

It is assumed that the IT environment provides support commensurate with the expectations of the TOE. For the testing platform, this was achieved by using evaluated products (or products in evaluation at the time of the writing of this VR) in the environment. The expectations of the TOE with respect to the security provided by the IT environment are captured in the ST in the environmental objectives, but were not verified by the evaluation.

# 5. ARCHITECTURAL INFORMATION[2]

This section provides a high level description of the TOE and its components as described in the Security Target.

The TOE is an application that is installed into an authorized library (a library containing programs with special privileges). The TOE is installed into an authorized library by a person with update privileges to that library. This person is acting in the role of "TOE Administrator".

The intended TOE operating environment is an IBM or IBM compatible mainframe capable of supporting the IBM z/OS operating system, located in a secure environment, i.e. a controlled facility that will prevent unauthorized physical access, where the operating system is securely configured such that it protects the TOE from any unauthorized users or processes and is staffed with trusted, trained and competent individuals.

The z/OS operating system (and its predecessor operating system, OS/390, both collectively referred to hereinafter as z/OS) is the computer operating system for the IBM line of large (mainframe) zSeries servers. IBM zSeries servers provide, among many other features, logical partitions (LPAR) that logically share a computer's clock, processors, memory, and storage so they appear as multiple virtual sets of resources. Each set of resources operates independently with its own operating system instance and applications. Each partition communicates with the other partitions as if the other partition is in a separate independent machine.

[2] Extracted from SAIC ETR Part 1 Version 3.0, 8 August 2005

# 6. DOCUMENTATION

The following documentation was used as evidence for the evaluation of Innovation FDRERASE Version 5.4, Level 50:[3]

## 6.1. Design documentation

| Document | Version | Date |
|---|---|---|
| INNOVATION Data Processing FDRERASE Solution Functional Specification, High-Level Design and Representation Correspondence Document | ERSDES12 | 1 June 2005 |
| Design Documents (ADV) Resubmission Letter 2 and Attachment For Evidence Elements ADV_FSP.1, ADV_HLD.1 and ADV_RCR.1 Innovation Data Processing, Inc. FDRERASE V54.50 | Resubmission Letter 2 | 7 June 2005 |

## 6.2. Guidance documentation

| Document | Version | Date |
|---|---|---|
| INNOVATION Data Processing FDRPAS and FDRERASE User Manual and Installation Guide | ERSDOC 1.12 | January 2005 |
| Guidance Documents (AGD) Resubmission Letter I and Attachment For Evidence Elements AGD_ADM.1 and AGD_USR.1 Innovation Data Processing, Inc. FDRERASE V54.50 | Resubmission Letter I | 6 May 2005 |

## 6.3. Configuration Management and Lifecycle documentation

| Document | Version | Date |
|---|---|---|
| INNOVATION Data Processing Software Development Configuration Management Developer Guide | ERSCFM 1.1 | 27 June 2005 |
| Configuration Management (ACM) Resubmission Letter I and Attachment For Evidence Element ACM_CAP.2 Innovation Data Processing, Inc. FDRERASE V54.50 | Resubmission Letter I | 14 March 2005 |

[3] This documentation list is extracted from the Final Evaluation Technical Report, Part 1 v.3.0 (8 August 2005), developed by SAIC.

| | | |
|---|---|---|
| Innovation Data Processing Software Product Life Cycle Maintenance Support (Bug Track) User Guide | ERSBUG 1.1 | 11 March 2005 |
| Life Cycle Support (ALC) Resubmission Letter I and Attachment For Evidence Element ALC_FLR.2 Innovation Data Processing, Inc. FDRERASE V54.50 | Resubmission Letter I | 11 March 2005 |

## 6.4. Delivery and Operation documentation

| Document | Version | Date |
|---|---|---|
| INNOVATION Data Processing Software Distribution Process Description and Software Distribution Facility User Guide | ERSDOP 1.1 | 25 April 2005 |
| Delivery and Operation (ADO) Resubmission Letter I and Attachment For Evidence Elements ADO_DEL.1 and ADO_IGS.1 Innovation Data Processing, Inc. FDRERASE V54.50 | Resubmission Letter I | 25 April 2005 |

## 6.5. Test documentation[4]

| Document | Version | Date |
|---|---|---|
| Innovation Data Processing Testing Procedures and FDRERASE Test Documentation | ERSTST11 | 8 June 2005 |
| Tests (ATE) Resubmission Letter and Attachments For Evidence Elements ATE_COV.1, ATE_FUN.1 and ATE_IND.2 Innovation Data Processing, Inc. FDRERASE V54.50 | Resubmission Letter | 8 June 2005 |
| Validator's Report | 1.0 | 27 June 2005 |

## 6.6. Vulnerability Assessment documentation

| Document | Version | Date |
|---|---|---|

[4] Per SAIC ETR part 1: The actual results are contained in numerous syslog files and were copied to a CD that was submitted to the evaluation team.

| | | |
|---|---|---|
| INNOVATION Data Processing FDRERASE Vulnerability Assessment | ERSVUL11 | 18 May 2005 |
| Vulnerability Assessment (AVA) Resubmission Letter I and Attachment For Evidence Element AVA_VLA.1 Innovation Data Processing, Inc. FDRERASE V54.50 | Resubmission Letter I | 18 May 2005 |

**Security Target**

| Document | Version | Date |
|---|---|---|
| Innovation Data Processing, FDRERASE Security Target | 1.0 | 1 July 2005 |

# 7. IT PRODUCT TESTING

This section describes the testing efforts of the developer and the Evaluation Team

## 7.1. Developer Testing

Evaluator analysis of the developer's test plans, test scripts, and test results indicate that the developer's testing is adequate to satisfy the requirements of EAL2, augmented with ADV_SPM.1 and ALC_FLR.2.

The vendor provided a test suite that covered multiple test cases and multiple sub-tasks. All functions were checked, as well as the TOE's ability to default to a secure state.

During testing, this suite was run with no errors reported.

## 7.2. Evaluator Testing

### 7.2.1. Functional Testing

In addition to developer testing, the CCTL conducted its own suite of tests, which were developed independently of the sponsor. These also completed successfully.

### 7.2.2. Vulnerability Testing

The evaluators developed vulnerability test to address both management and TOE access security functions, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE.

# 8. EVALUATED CONFIGURATION

The TOE is a privileged application that runs on an IBM or IBM-compatible mainframe running IBM z/OS or OS/390. The test machine consisted of:

- IBM mainframe z800 zSeries processor
- DASD
    - IBM 2105-F20 and 2105-800
    - EMC 5830 and 8430
    - Hitachi 7700E and 9970V
- IBM z/OS V1.6 operating system
- FDRERASE, Version 5.4, Level 50
- Test programs and test utility programs

# 9. RESULTS OF THE EVALUATION

The evaluation was conducted based upon the Common Criteria (CC), Version 2.1, dated August 1999 [1,2,3,4]; the Common Evaluation Methodology (CEM), Version 1.0, dated August 1999 [6]; and all applicable International Interpretations in effect on 1 April 2004. The evaluation confirmed that the Innovation FDRERASE Version 5.4, Level 50 product is compliant with the Common Criteria Version 2.1, functional requirements (Part 2), Part 2 extensions, and assurance requirements (Part 3) for EAL2 augmented with ADV_SPM.1 and ALC_FLR.2. The details of the evaluation are recorded in the CCTL's evaluation technical report; Evaluation Technical Report for the Innovation FDRERASE Version 5.4, Level 50 v12.6, Part 1 (Non-Proprietary) and Part 2 (Proprietary). The product was evaluated and tested against the claims presented in the Innovation FDRERASE Version 5.4, Level 50 Security Target v1.0, 1 July 2005.

The validator followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The validator has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validator therefore concludes that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL.

## 9.1. Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Innovation FDRERASE Version 5.4, Level 50 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

## 9.2. Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 2 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation.

## 9.3. Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification while in transit. The evaluation team

followed the Configuration Guide to test the installation procedures to ensure the procedures result in the evaluated configuration.

## 9.4. Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

In addition to the EAL 2 ADV CEM work units, the evaluation team applied the ADV_SPM.1 work units from the CEM supplement. The security policy model was evaluated to determine that it clearly and consistently described the rules and characteristics of the security policies and whether this description corresponds with the functional specification.

## 9.5. Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 2 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

## 9.6. Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 2 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance.

In addition to the EAL 2 ALC CEM work units, the evaluation team applied the ALC_FLR.2 work units from the CEM supplement. The vendor's flaw remediation procedures documentation and flaw remediation guidance documentation was evaluated to determine whether the developer has established flaw remediation procedures that describe the tracking of security flaws, the identification of corrective actions, and the distribution of corrective action information to TOE users.

## 9.7. Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE

enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

## 9.8. Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 2 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the developer misuse analysis, and the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

## 9.9. Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

# 10. VALIDATOR COMMENTS

The validators would like to reiterate that FDRERASE's QUICK ERASE function is not in the TOE and is therefore not evaluated.

The SUPERZAP program applies binary patches to an existing compiled program. Any such change, including patches marketed as "updates", may bring an installation out of the evaluated configuration. Please review all patches carefully before installation.

Note that the TOE is protected from unauthorized access to itself by the simple expedient of not providing internal access to its own executable: the only interfaces to the TOE are ERASE, SECUREERASE, QUICKERASE, and VERIFY, none of which can alter the TOE executable. Protection against interference from other TOE subjects or IT environment subjects is assured via operating system file locks.

# 11. SECURITY TARGET

*Innovation FDRERASE Version 5.4, Level 50 Security Target, version 1.0 1 July 2005*

# 12. GLOSSARY

| | |
|---|---|
| CC | Common Criteria |
| CCEVS | Common Criteria Evaluation and Validation Scheme |
| CCTL | Common Criteria Testing Laboratory |
| CEM | Common Evaluation Methodology |
| CM | Configuration Management |
| CMP | Configuration Management Plan |
| DASD | Direct Access Storage Device |
| DoD | Department of Defense |
| DBMS | Database Management Server |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| IT | Information Technology |
| JCL | Job Control Language |
| LPAR | Logical Partitions |
| NIAP | National Information Assurance Partnership |
| NIST | National Institute of Standards & Technology |
| NSA | National Security Agency |
| NVLAP | National Voluntary Laboratory Assessment Program |
| PP | Protection Profile |
| SAIC | Science Applications International Corporation |
| ST | Security Target |

| | |
|---|---|
| TOE | Target of Evaluation |
| TSF | TOE Security Function |
| TSFI | TOE Security Function Interface |
| VR | Validation Report |
| VTOC | Volume Table of Contents |

# 13. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[7] Innovation FDRERASE Version 5.4, Level 50 Security Target, v1.0, 1 July 2005

[8] Evaluation Technical Report for Innovation FDRERASE Version 5.4, Level 50. Part 1 (Non-Proprietary) v.1.0, 7 July 2005; Part 2 (Proprietary) v.3.0, 8 August 2005

[9] Evaluation Team Test Plan For Innovation FDRERASE Version 5.4 Level 50, ETR Part 2 Supplement (SAIC and Innovation Proprietary), Version 3.0, 8 August 2005.