

**AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAMME**

**Certification Report**

**Certificate Number: 2000/13**

**KeyCorp Ltd**

**MULTOS Version 4.02 (Release 1N`-AMD)**

Issue 1.0  
July 2000

© Copyright 2000



Issued by: -

**Defence Signals Directorate - Australasian Certification Authority**

© Commonwealth of Australia 2000

Reproduction of any or all of this report  
is prohibited.

**CERTIFICATION STATEMENT**

MULTOS Version 4.02 (Release 1N`-AMD) is an operating system for integrated circuit cards (also known as smart cards) developed by KeyCorp Ltd. In summary, MULTOS provides a common development and operating platform which allows multiple applications to be securely loaded and executed on a MULTOS enabled card.

This report describes the evaluation findings of MULTOS Version 4.02 (Release 1N`-AMD) product to the ITSEC Assurance Level E6. It also includes recommendations by the Australasian Certification Authority (ACA) that are specific to the secure use of the product in order to meet the ITSEC E6 level of assurance. It concludes that the product has met the target Assurance Level of E6.

**Originator**

\_\_\_\_\_

Chris Pennisi  
Certifier  
Defence Signals Directorate

**Approval**

\_\_\_\_\_

Peter Lilley  
Manager, Australasian Information Security Evaluation Programme  
Defence Signals Directorate

**Authorisation**

\_\_\_\_\_

Lynwen Connick  
Australasian Certification Authority  
Defence Signals Directorate

## TABLE OF CONTENTS

<b>CERTIFICATION STATEMENT</b> .....	<b>ii</b>
<b>TABLE OF CONTENTS</b> .....	<b>iii</b>
<b>Chapter 1 Introduction</b> .....	<b>1</b>
Intended Audience.....	1
Identification of Target of Evaluation .....	1
Evaluation .....	1
General Points .....	2
Scope of the Evaluation.....	2
<b>Chapter 2 Security Overview of MULTOS</b> .....	<b>3</b>
Background .....	3
Overview of the TOE .....	3
Documentation .....	4
<b>Chapter 3 Evaluation Findings</b> .....	<b>5</b>
Introduction .....	5
Assurance Results .....	5
<i>Correctness – Construction</i> .....	5
<i>Correctness – Operation</i> .....	7
<i>Effectiveness – Construction</i> .....	8
<i>Effectiveness – Operation</i> .....	9
Specific Functionality.....	11
Discussion of Unresolved Issues.....	11
General Observations .....	11
<b>Chapter 4 Conclusions</b> .....	<b>12</b>
Certification Result .....	12
Scope of the Certificate .....	12
Recommendations .....	12
<b>Appendix A References</b> .....	<b>14</b>
<b>Appendix B Glossary of Terms</b> .....	<b>16</b>
<b>Appendix C Summary of the Security Target</b> .....	<b>18</b>
Security Target .....	18
Product Rationale for the TOE.....	18
<i>Security Objectives</i> .....	18
<i>Intended Method of Use and Intended Environment</i> .....	18
Summary of Security Features of the TOE .....	20
<i>Application Load and Authentication SEF</i> .....	20
<i>Application Separation SEF</i> .....	20
<i>Application Transport Confidentiality SEF</i> .....	20
<i>Application Deletion SEF</i> .....	21
<i>Object Reuse SEF</i> .....	21
<i>Smart Card Authentication SEF</i> .....	21
<i>Key Installation SEF</i> .....	21
<i>Cryptography Control SEF</i> .....	21

---

**Appendix D Identification of the TOE .....22**  
Configuration for Evaluation .....22  
Identification of the evaluated version of MULTOS .....22

## Chapter 1 Introduction

### Intended Audience

- 1.1 This certification report states the outcome of the IT security evaluation of the MULTOS Version 4.02 developed by Keycorp Ltd. (hereafter referred to as MULTOS). It is intended to assist potential users when judging the suitability of the product for their particular requirements, and to advise security administrators on ensuring the product is used in a secure manner.

### Identification of Target of Evaluation

- 1.2 The version of MULTOS evaluated was Version 4.02 (Release 1N' AMD) software operating on the Infineon (Siemens) SLE66CX160S processor.
- 1.3 MULTOS is an operating system for integrated circuit cards (also known as smart cards), providing a common development platform for applications. It allows multiple applications to be loaded and executed without interfering with or being interfered with by other applications.
- 1.4 MULTOS consists of the following components:
  - a) Software - MULTOS Keycorp Version 4.02 (Release 1N' AMD)
  - b) User Manuals for the MULTOS Carrier Device (MCD) Issuer, Application Writer and the Application Loader
- 1.5 For further details of the evaluated components of MULTOS, including details of how to identify the evaluated version, refer to Appendix D.

### Evaluation

- 1.6 The evaluation was carried out in accordance with the rules of the Australasian Information Security Evaluation Programme (AISEP) which is described in Evaluation Memorandum 1 and Evaluation Memorandum 2 (refs [1], [2] respectively).
- 1.7 The purpose of the evaluation was to provide assurance about the effectiveness of the Target of Evaluation (TOE), MULTOS, in meeting its Security Target (ref [3]). The criteria against which the TOE is judged are expressed in the ITSEC (ref [4]). This describes how the degree of assurance is expressed in terms of the levels E1 to E6 and E0, where the latter indicates that the TOE has failed to meet its targeted level of assurance. The methodology used is described in the ITSEM and Evaluation Memoranda 4 and 5 (refs [5], [6], [7]).

- 1.8 The evaluation was performed, concurrent with the development, by CMG Admiral between January 1998 and May 2000, and was monitored by the Certification Group on behalf of the Australasian Certification Authority (ACA). The evaluation of the cryptographic mechanisms was conducted by DSD in parallel with the AISEP evaluation with the Certification Group being advised of its completion in October 1999 (ref [16]). Further, the evaluation of the underlying smart card hardware was performed independently by MONDEX International in parallel with the MULTOS evaluation. At the end of the evaluation, an Evaluation Technical Report (ETR) (ref [8]) describing the evaluation and its results was presented to the ACA. This Certification Report was then produced, based on the contents of the ETR and the Certification Group's knowledge of the evaluation, the results of the cryptographic evaluation and the results of the SLE66CX160S hardware evaluation (ref [17]).
- 1.9 The Security Target (ref [3]) claimed an assurance level for the product of E6, and claimed that all non-cryptographic security mechanisms of the TOE are impregnable to direct attack.

#### **General Points**

- 1.10 Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with higher evaluation levels) that exploitable vulnerabilities remain undiscovered. However, at the ITSEC E6 level of assurance, this probability is lowest.
- 1.11 The MULTOS product should only be used within the intended environment and in accordance with the method of use as explained in (ref [3]). In addition, users should be aware of the certifiers' recommendations as given in Chapter 4 of this report.
- 1.12 Ultimately, it is the responsibility of the user to ensure that the MULTOS product meets their requirements. For this reason, it is *strongly* recommended that a prospective user of the product obtains a copy of the Security Target from the product vendor, and reads this Certification Report thoroughly prior to deciding whether to purchase the product.

#### **Scope of the Evaluation**

- 1.13 The scope of the evaluation is limited to those claims made in the Security Target. All security related claims in the Security Target were evaluated by CMG Admiral. The cryptographic mechanisms were evaluated by DSD for Australian Government use and found to be appropriate for the protection of material classified RESTRICTED, and non-National Security classifications including IN-CONFIDENCE, PROTECTED and HIGHLY PROTECTED.
- 1.14 A summary of the Security Target is provided in Appendix C of this Certification Report.

## Chapter 2 Security Overview of MULTOS

- 2.1 Potential users are *strongly* recommended to read the Security Target (ref [3]). This explains the security functionality of the MULTOS product in greater detail, as well as the intended environment and method of use for the product. A summary of the Security Target can be found in Appendix C. A full copy of the Security Target can be obtained from Keycorp Ltd.

### Background

- 2.2 Keycorp Ltd, in its role as a member of the MAOSCO consortium, was commissioned to develop an open, high-security, multi-application operating system. This operating system is called MULTOS.

### Overview of the TOE

- 2.3 This section provides a summary of the operational role of the TOE together with the functions it is designed to perform.
- 2.4 MULTOS is an operating system for integrated circuit cards (also known as smart cards). It is designed to allow multiple smart card applications to be securely loaded and executed on a smart card.
- 2.5 The user of the smart card accesses the application loaded on it via an Interface Device (IFD), which could be a Point-of-Sale terminal, Automatic Teller Machine, or some other device which supports ISO 7816 smart card protocols.
- 2.6 By means of command-response pairs, MULTOS allows:
- i. applications to be loaded onto and deleted from the smart card;
  - ii. an IFD to access data and applications which are loaded on the card; and
  - iii. information specific to the card to be retrieved by an IFD.
- 2.7 MULTOS is a single-threaded operating system. Only one application can be executing at any given time. MULTOS does not provide mechanisms for concurrency or multi-tasking.
- 2.8 Applications to be loaded on MULTOS-based smart cards are written in a hardware independent language called MULTOS Executable language (MEL). MEL applications

are interpreted by MULTOS, rather than being compiled and executed directly on the smart card processor.

- 2.9 MULTOS also provides for shared code routines, called Codelets, which can be called by an executing application. Codelets can be loaded into MULTOS during IC manufacture or a smart card personalisation time. A Codelet has its own code address space but executes in the context of the calling application, so has access to the application's data.
- 2.10 MULTOS provides for two security objectives that preserve the confidentiality and integrity of loaded applications and their data and a third security objective to confirm the authority of all application load and delete requests. In providing these objectives, MULTOS implements eight security enforcing functions (SEFs). These are an Application Load and Authentication SEF, Application Separation SEF, Application Transport Confidentiality SEF, Application Deletion SEF, Object Reuse SEF, Smart Card Authentication SEF, Key Installation SEF and a Cryptography Control SEF.
- 2.11 More detailed information on the MULTOS SEFs can be found in the Security Target for the MULTOS product (ref [3]), and in Appendix C of this document.

### **Documentation**

- 2.12 Before using the product, prospective users should ensure that they are aware of and fully understand the relevant operational documentation. Application Loaders should ensure that they read installation guides pertaining to the load and delete of applications ref ([14], [15]). Application Writers should ensure that they read the programming guides in relation to MULTOS (ref [11], [12], [13]). It is also recommended that prospective purchasers, application loaders and application writers should read Chapter 4 of this document.

## Chapter 3 Evaluation Findings

### Introduction

- 3.1 The evaluation of MULTOS followed a course consistent with the generic evaluation work programme described in the ITSEM (ref [5]), with work packages structured around the evaluator actions described in the ITSEC (ref [4]). The results of this work are reported in the ETR (ref [8]) under the ITSEC headings. This report summarises the general results, followed by the findings in relation to the security functionality claimed in the Security Target (ref [3]).

### Assurance Results

#### *Correctness – Construction*

- 3.2 This aspect of the evaluation examined both the development process (including the Security Target, the Architectural and Detailed Designs, and the Implementation) and the development environment where the development took place.

#### *Requirements*

- 3.3 The final version of the Security Target (ref [3]) explained the Security Enforcing Functions (SEF) and mechanisms provided by the TOE, and contained a product rationale that included the intended method of use, the intended environment and the assumptions about physical, personnel and procedural security. The Security Target also explained how the functionality of the TOE was sufficient to counter the assumed threats.
- 3.4 The Security Target referenced a formal security policy model document (ref [9]) that specified the formal model of security policy enforced by the TOE, and a formal specification of the Security Enforcing Functions provided by the TOE. Further, the formal model of security policy document provided the informal explanations of how the formal security policy model is satisfied by the Security Target.
- 3.5 The above results have enabled the certifiers to conclude that the TOE met the requirements for ITSEC E6 in regard to its Security Target and Formal Security Policy Model.

#### *Architectural Design*

- 3.6 The final version of the formal Architectural Design correctly explained the general structure of the TOE and the external interfaces. The Architectural Design explained how

the SEFs from the Security Target are provided and how the architectural structure of the TOE provides for largely independent security enforcing components. The Architectural Design explained that the TOE was structured and separated into security enforcing components and security relevant components only.

- 3.7 The above results have enabled the certifiers to conclude that the TOE met the requirements for ITSEC E6 in regard to its Architectural Design.

#### *Detailed Design*

- 3.8 The final set of Detailed Design documents properly identified all of the security mechanisms, explained the realisation of the SEFs, and provided a mapping of the SEFs and their associated security enforcing mechanisms down to the functional units of the design, and adequately documented their interfaces. The evaluators were able to determine from the detailed design that all components were either security enforcing or security relevant, and that those components did not contain any functionality that was unnecessary for the TOE to enforce security.
- 3.9 The above results have enabled the certifiers to conclude that the TOE met the requirements for ITSEC E6 in regard to its Detailed Design.

#### *Implementation*

- 3.10 The evaluators were able to determine that the implementation was correct by ensuring that the SEFs identified in the Detailed Design are identifiable and correct in the source code, and consistent with the formal specification of the SEFs provided in the formal security policy model (ref [9]). The test documentation explained how the developer's tests covered the implementation of the TOE SEFs, and were assessed to be of a standard that allowed for the tests to be repeatable and reproducible.
- 3.11 The above results have enabled the certifiers to conclude that the TOE met the requirements for ITSEC E6 in regard to its Implementation.

#### *Development Environment*

- 3.12 The evaluators were able to determine that a tool-based configuration control system, appropriate quality practices and procedures, and appropriate levels of physical and procedural security supported the development environment, ensuring the confidentiality and integrity of the TOE and its associated documents during development.
- 3.13 Apart from two unresolved issues, the evaluators determined that the security of the development environment and the configuration control system satisfied the ITSEC E6

requirements.

- 3.14 The first issue referred to the lack of a time stamp in the auditing of objects under configuration control. Given the infrequency of changes to objects under configuration control and the rigorous configuration control procedures applied by the developer, the certifiers have judged that this issue does not affect the overall assurance or security of the TOE.
- 3.15 The second issue referred to the inability of the configuration control system to support the creation and handling of variable relationships between objects under configuration control. Given that all objects of the TOE are either security enforcing or security relevant, and the developer's manual process of examining the effect of a change on all objects of the TOE under configuration control, the certifiers have judged that this issue does not affect the overall assurance or security of the TOE.
- 3.16 As the TOE is comprised of software, the evaluators performed an assessment of programming languages and compilers. The evaluators were able to determine that a well-defined programming language was used in the implementation of the TOE, and that appropriate coding standards and guidelines were applied to the development of the TOE.
- 3.17 The above results, and the clearance of the outstanding issues by the certifiers, has enabled the certifiers to conclude that the TOE met the requirements for ITSEC E6 in regard to its Development Environment.

#### *Correctness – Operation*

- 3.18 This aspect of the evaluation looked at how the delivery and configuration procedures maintain the security of the TOE, and how operational procedures ensure secure start-up and operation.
- 3.19 Due to the nature of the TOE, there is no action required on the part of the end user to ensure the secure start-up and operation of MULTOS, nor can any security enforcing functions be modified or de-activated during start-up or normal operation.
- 3.20 The evaluators determined that all administrative and user documentation consistent with supporting security infrastructure (section 2.4, ref [3]) explained all necessary procedures for usage of the TOE.
- 3.21 The evaluators determined that the startup and operation documentation explained the procedures for secure startup and operation of the TOE.
- 3.22 The evaluators determined that the procedures for generation of the TOE were explained.
- 3.23 The evaluators were unable to determine that the delivery documentation explained the

delivery arrangements from the development environment to the IC Manufacturer, as these had not been provided. These procedures (ref [10]) were provided to the Certification Group during certification. The certifiers determined that the delivery documentation explained how the delivery procedures guaranteed the authenticity of the TOE from the development environment to the IC Manufacturer. Further recommendations relating to the secure delivery and authentication of MULTOS are provided in Chapter 4 and Appendix D of this document.

- 3.24 The above results have enabled the certifiers to conclude that the TOE met the requirements for ITSEC E6 in regard to its Operational Documentation and Environment.

#### *Effectiveness – Construction*

- 3.25 This aspect of the evaluation dealt with:

- (i) the suitability of the TOE's security enforcing functions to counter the threats identified in the Security Target;
- (ii) the ability of the security enforcing functions and mechanisms to bind together in a way that is mutually supportive and provides an integrated and effective whole;
- (iii) the ability of the TOE's security mechanisms to withstand direct attack; and
- (iv) the question of whether known security vulnerabilities in the construction of the TOE could, in practice, compromise its security.

#### *Suitability Analysis*

- 3.26 The evaluators determined that the developer's Suitability Analysis, with further analysis by the evaluators, demonstrated that all of the threats listed in the Security Target were adequately countered by the stated SEFs and/or by a combination of other physical, personnel or procedural security measures.
- 3.27 As a result of the above determinations, the certifiers concluded that the TOE met the ITSEC E6 requirements for the Suitability Analysis.

#### *Binding Analysis*

- 3.28 The Binding Analysis must analyse all the potential relationships between security enforcing functions and mechanisms to ensure that there is no way for any mechanism or function to conflict with, or contradict the intent of, other security enforcing functions or mechanisms. The evaluators found that the developer's Binding Analysis, with further analysis by the evaluators, demonstrated that it was not possible for any binding element
-

to conflict with or contradict the intent of any other binding element.

- 3.29 As a result of the above determinations, the certifiers concluded that the TOE met the ITSEC E6 requirements for the Binding Analysis.

#### *Strength of Mechanisms Analysis*

- 3.30 The Strength of Mechanisms Analysis correctly identified the mechanisms of the TOE. All mechanisms of the TOE, which could possibly be subverted by direct attack, were cryptographic in nature and thus subject to evaluation by DSD. These were found to be suitable for Australian Government use. An analysis was provided that justified the claim that the non-cryptographic mechanisms of the TOE were of a type that was impregnable to direct attack.
- 3.31 As a result of the above determinations, the certifiers concluded that the TOE met the ITSEC E6 requirements for the Strength of Mechanisms Analysis.

#### *Construction Vulnerability Assessment*

- 3.32 For this aspect of the evaluation, the evaluators examined the developer's Construction Vulnerability Assessment that claimed three categories of vulnerabilities in the construction of the TOE. The evaluators determined that the developer's analysis showed that each identified vulnerability could not be exploited in practice. The evaluators also performed their own assessment to search for potential vulnerabilities in the TOE. The evaluators were unable to find any vulnerabilities in the construction of the TOE which had not been identified by the developer. Further, testing of the TOE by the evaluators did not reveal any exploitable vulnerabilities due to its construction.
- 3.33 As a result of the above determinations, the certifiers concluded that the TOE met the ITSEC E6 requirements for the Construction Vulnerability Assessment.

#### *Effectiveness – Operation*

- 3.34 This aspect of the evaluation entailed checking how easy the TOE is to use in a secure manner, and making an assessment of the known vulnerabilities in its operation to determine whether they could, in practice, compromise its security.

#### *Ease of Use Analysis*

- 3.35 The evaluators found that the TOE could not be configured or used in a manner which was insecure but which an end-user would reasonably believe to be secure. Further, the evaluators found that the TOE could be used securely using only the user manuals as

guidance for application loaders and application writers (defined in Appendix B and C of this document), and that all possible failure modes were adequately documented, along with their effects.

- 3.36 The evaluators reported an unresolved issue at the conclusion of the evaluation. This issue referred to the fact that an application residing on MULTOS could inadvertently write confidential data to the public area due to errors in the applications implementation. The evaluators determined that this issue does not contradict the Security Target or the Security Policy Model (Ref [3], [9]) of the TOE, and is unlikely due to the architectural design of MULTOS. The certifiers conclude that this issue is outside the scope of the TOE and therefore risk of an application writing its own sensitive data to the public area is the responsibility of the application writer, which can be reduced by security evaluation of applications intended for use on the MCDs. The certifiers judged that this issue did not affect the overall assurance or security of the TOE.
- 3.37 The above results have enabled the certifiers to conclude that the TOE met the ITSEC E6 requirements for the Ease of Use Analysis.

#### *Operational Vulnerabilities Assessment*

- 3.38 For this part of the evaluation, the evaluators assessed the known vulnerabilities in the operation of the TOE to determine whether they could, in practice, compromise the security of the TOE. The evaluators found that the developer's Operational Vulnerability Assessment correctly identified several vulnerabilities in the operation of the TOE. Analysis and testing of the TOE by the evaluators did not reveal any exploitable vulnerabilities in the operation of the TOE that were not satisfactorily countered by physical security measures implemented by the MULTOS Security Manager.
- 3.39 The evaluators reported an unresolved issue at the conclusion of the evaluation. In performing their own Operational Vulnerability Analysis the evaluators determined that, it is possible that a malicious application on MULTOS could elicit information from the end user. The evaluators noted that this could be achieved by a rogue application impersonating a sensitive application, which could reside on the MCD. The certifiers conclude that the risk of loading a malicious application onto an MCD is the responsibility of the application loader. This risk can also be reduced by security evaluation of applications intended for use on the MCDs. The certifiers judged that this issue did not affect the overall assurance or security of the TOE.
- 3.40 As a result of the above determinations, the certifiers concluded that the TOE met the ITSEC E6 requirements for the Operational Vulnerability Assessment.

**Specific Functionality**

- 3.41 The Security Enforcing Functions (SEFs) provided by the MULTOS are specified in section 4 of the Security Target (ref [3]) and summarised in Appendix C of this report.
- 3.42 The evaluators found that the product correctly and effectively provided the functionality specified in the Security Target (ref [3]).

**Discussion of Unresolved Issues**

- 3.43 At the conclusion of the evaluation process, five issues identified by the evaluators remained unresolved, which were addressed during certification. These issues have been identified and discussed in previous sections of this chapter. As such, there are no unresolved issues remaining from the evaluation.

**General Observations**

- 3.44 The certifiers would like to acknowledge the invaluable assistance provided Keycorp staff during the evaluation. Without the due attention to problems found, and their technical assistance, the process could not have succeeded in the same time frame.
- 3.45 Further, the certifiers would like to acknowledge the efforts of CMG Admiral in ensuring prompt delivery of the Evaluation Technical Report for certification.

## Chapter 4 Conclusions

### Certification Result

- 4.1 After due consideration of the Evaluation Technical Report (ref [8]) produced by the evaluators and the conduct of the evaluation as witnessed by the certifiers, the Australasian Certification Authority has determined that MULTOS has met the requirements of the ITSEC E6 Assurance level.

### Scope of the Certificate

- 4.2 This certificate applies only to version 4.02 (Release 1N' AMD) of the product. This certificate is only valid when MULTOS is installed on the designated hardware. These components are identified in Appendix D. A description explaining how an application loader and application writer can verify this version information on delivery is also provided in Appendix D.

### Recommendations

- 4.3 The following recommendations include information highlighted by the evaluators during their analysis of the developer's deliverables, during the conduct of the evaluation, and during the additional activities performed by the Certification Group.
- 4.4 MULTOS should only be used in accordance with the intended environment described in section 2.4 of the Security Target (ref [3]), including consideration of all physical, personnel and procedural security measures.

### *Verification of the Evaluated Version of the TOE*

- 4.5 To verify that the product received is the evaluated version, noted in Chapter 1 of this document, government purchasers should request their chosen application loader and/or application writer to verify the authenticity of the material provided and confirm it does comprise the evaluated version. The application loader and application writer have the facilities to query a smart card to confirm that it is a MULTOS card. A corollary to this recommendation is for the purchaser to ensure that the Application Loader is a trusted party and has the appropriate facilities to confirm the evaluated version of the TOE.

### *Environmental Security implemented by the MSM*

- 4.6 The operational environment of the TOE includes a commercially based supporting security infrastructure. It is recommended Australian Government Purchasers should ensure that the physical and procedural security measures in place at the MSM Global Key Centre are consistent with their own organisational security policies. A more detailed

explanation of the supporting security infrastructure is provided in the Security Target (ref [3]).

*Environmental Security of MULTOS Application Loaders and Application Providers*

- 4.7 The purchaser should ensure that the application loaders and application writers who provide the required applications for usage have appropriate physical and procedural security measures to guarantee the integrity of developed applications.

*Secure Operation of MULTOS Applications*

- 4.8 Purchasers are strongly recommended to request loading of those applications on the MULTOS smart cards, which have undergone evaluation to an appropriate level of assurance commensurate with the purchasers level of risk. This recommendation minimises the risk that an incorrectly implemented application could be loaded onto the MULTOS card, which could inadvertently disclose information that may need to be kept confidential to other applications.

*Trusted MULTOS Applications*

- 4.9 Purchasers are strongly recommended to request loading of those applications on MULTOS smart cards, which have been signed by the MULTOS Certification Authority. This recommendation minimises the risk that a malicious application could be loaded onto the MULTOS card, which could then masquerade as a valid application.

## Appendix A References

- [1] Evaluation Memorandum No. 1 - Description of the AISEP  
Defence Signals Directorate  
EM 1, Issue 1.1, March 1997
- [2] Evaluation Memorandum No. 2 - The Licensing of AISEFs  
Defence Signals Directorate  
EM 2, Issue 1.0, August 1994
- [3] MULTOS Security Target  
Keycorp Ltd.  
Issue 3.0, November 1998  
(COMMERCIAL-IN-CONFIDENCE)
- [4] Information Technology Security Evaluation Criteria (ITSEC)  
Commission of the European Communities  
CD-71-91-502-EN-C, Version 1.2, June 1991
- [5] Information Technology Security Evaluation Methodology (ITSEM)  
Commission of the European Communities  
Version 1.0, 10 September 1993
- [6] Manual of Computer Security Evaluation Part I - Evaluation Procedures  
Defence Signals Directorate  
EM 4, Issue 1.0, April 1995  
(EVALUATION-IN-CONFIDENCE)
- [7] Manual of Computer Security Evaluation Part II - Evaluation Techniques and  
Tools  
Defence Signals Directorate  
EM 5, Issue 1.0, April 1995  
(EVALUATION-IN-CONFIDENCE)
- [8] MULTOS Evaluation Technical Report  
CMG Admiral  
Issue 1.1, June 2000.  
(EVALUATION-IN-CONFIDENCE, COMMERCIAL-IN-CONFIDENCE)
- [9] MULTOS Formal Security Policy Model  
Keycorp Ltd.

Issue 2.0, 23<sup>rd</sup> November 1998.  
(COMMERCIAL-IN-CONFIDENCE)

- [10] MULTOS Delivery Process  
Keycorp Ltd.  
Version 1.1, 26<sup>th</sup> June 2000
- [11] MULTOS Developers Guide  
Keycorp Ltd.  
Version 1.2, 17<sup>th</sup> September 1999
- [12] MULTOS Developers Reference Manual  
Keycorp Ltd.  
Version 1.3, 17<sup>th</sup> September 1999
- [13] MULTOS Application Programmers Reference Manual  
Keycorp Ltd.  
Version 1.0, August 1997
- [14] MULTOS Guide to loading and Deleting Applications  
Keycorp Ltd.  
Version 2.2, 6<sup>th</sup> March 2000
- [15] MULTOS Application Load Unit Generation guide  
Keycorp Ltd.  
Version 2.4, 19<sup>th</sup> January 2000
- [16] Cryptographic Evaluation Report  
Defence Signals Directorate  
Version 1.0, 18<sup>th</sup> October 1999  
(COMMERCIAL-IN-CONFIDENCE)
- [17] Results of Hardware Evaluation Phase 3a Status Report on the Siemens  
SLE66CX160S  
Letter From Neal Harper to Peter Lilley  
Received 16<sup>th</sup> June 1999

## Appendix B Glossary of Terms

- B.1 **MAOSCO Consortium:** An international consortium of 14 countries responsible for the development of smart card technology. The consortium members, as a group, are responsible for the MULTOS specification and its ongoing maintenance.
- B.2 **MULTOS Security Manager (MSM):** The individual responsible for policing the MULTOS security infrastructure and provides the criteria and services necessary for MULTOS participants to operate within the infrastructure. It acts as Certification Authority for the security infrastructure. It is assumed only one MSM exists. The MSM must be trusted by all participants in the infrastructure.
- B.3 **MULTOS Implementor:** the organisation that implements a MULTOS version. The MULTOS Implementor is licensed by MAOSCO and provides its MULTOS version to the IC Manufacturer. The MULTOS Implementor requests the MSM to provide MSM Controls Data, although this may be delivered to the MCD Manufacturer or MCD Issuer.
- B.4 **Integrated Circuit (IC) Manufacturer:** manufacturer of silicon from which chips and smart cards are made. It is assumed the IC Manufacturer is trusted to perform its task correctly. It is assumed that all security measures concerned with card manufacture are completed at the IC manufacture stage. This includes:
- i. the inclusion of security keys in the ROM mask
  - ii. the injection of security data into non-volatile memory
- Security keys and data are provided by the MSM. The initialised ICs are provided to MCD Manufacturers
- B.5 **MULTOS Carrier Device (MCD) Manufacturer:** responsible for embedding the IC in its plastic carrier and for background printing on the card. The result is an initialised MCD. This operation is assumed not to be security sensitive. The MCD manufacturer may also receive MSM Controls Data from the MSM and enable the MCDs. Initialised and enabled MCDs are provided to MCD Issuers.
- B.6 **MCD Issuer:** responsible for issuing to users the MCD itself. The MCD Issuer may also enable initialised MCDs, by loading MSM Controls Data received from the MSM onto the MCDs. MCD Issuers retain the ultimate authority over what applications are

loaded on their MCDs. MCD Issuers register applications with the MSM, provide information related to the applications and receive application load and delete certificates from the MSM.

- B.7 **Application Writer:** licensed by MAOSCO to produce applications for MULTOS. Supplies applications under contract to Application Issuers.
- B.8 **Application Issuer:** an organisation that wishes to offer an application to MCD users. The Application Issuer agrees with a MCD Issuer that the application can be loaded onto MCDs belonging to the MCD Issuer.
- B.9 **Application Provider:** the organisation that takes responsibility for an application, by certifying it with the organisation's public key and encrypting it where necessary. The Application Provider is a role that can be performed by an Application Writer, Application Issuer or MCD Issuer, rather than being an organisation in its own right.
- B.10 **Application Loader:** the organisation that takes responsibility for performing the technical operation of loading onto MCDs. The Application Loader enters into an agreement with one or more Application Issuers and MCD Issuers for loading applications supplied by one or more Application Providers.
- B.11 **MCD User:** final user of the MCD.

## Appendix C Summary of the Security Target

### Security Target

- C.1 A brief summary of the Security Target (ref [3]) is given below. Potential purchasers should attempt to obtain a copy of the full Security Target to ensure that the security enforcing functions meet the requirements of their security policy.

### Product Rationale for the TOE

#### *Security Objectives*

- C.2 MULTOS has the following IT security objectives:
- a) Preserve the mutual confidentiality of multiple applications loaded and executed on a single smart card.
  - b) Preserve the mutual integrity of multiple applications loaded and executed on a single smart card.
  - c) To confirm the authority of all application loaded and delete requests.

#### *Intended Method of Use and Intended Environment*

- C.3 The Intended Method of Use for MULTOS is:
- a) MULTOS will ensure all requests to load applications are appropriately authorised. MULTOS will support a capability to ensure the authenticity and integrity of an application when loading the application onto the smart card. MULTOS will also ensure all requests to delete applications are appropriately authorised. Reasons for wishing to delete applications may be because they are found to contain errors, because an updated application is available, or to make room on the smart card for a more desirable application.
  - b) MULTOS will support a capability to load encrypted applications onto the smart card, decrypt such applications and make them available to the smart card user for execution.
  - c) MULTOS will ensure no application loaded on the smart card can interfere with the operation of any other loaded application or with MULTOS. MULTOS will also

ensure that an applications code and data will not be available to other applications after it has been deleted.

- d) MULTOS will provide the capability to authenticate a card as a valid MULTOS-equipped smart card.
- e) MULTOS will provide the capability to restrict the use of regulated features of the smart card (e.g., strong cryptography) to authorised applications.
- f) MULTOS defines certain functions (installing keys, loading applications and deleting applications) as sensitive functions. For each of these functions, if the number of failed attempts to execute the function reaches a pre-defined limit over the life of the smart card, MULTOS will permanently disable the function. In the case of installing keys, this means the card is unusable, as no applications can be loaded until keys have been installed. In the cases of application loading and deleting, other functions of the card remain available.

#### C.4 The Intended Environment for MULTOS is:

- a) **TOE Location and Usage.** After MULTOS has been developed in software, the MULTOS executable will be masked in Read Only Memory (ROM) and embedded on smart cards.

Once the MULTOS chip has been embedded on a target smart card, interaction with it will be via commands issued to the card from an IFD or service request (i.e., MULTOS system calls, known as primitives) made by an executing application.

- b) **Supporting Hardware and Firmware.** MULTOS operates on the Siemens SLE66CX160S Smartcard Integrated Circuit (IC). Hardware support is also included for the implementation of cryptographic functions. This support is in the form of 512 and 1024 bit registers and associated instructions to manipulate data in these registers.

MULTOS requires firmware run-time libraries to support writing data to EEPROM. Siemens. supplies these. MULTOS requires the run-time libraries to execute correctly according to specification, to ensure data is written to the correct address within the EEPROM.

MULTOS also requires firmware runtime libraries to support manipulation of the 512 and 1024 bit registers required for the cryptographic functions.

- c) **Supporting Security Infrastructure.** MULTOS-equipped smart cards and MULTOS applications will need to be manufactured and distributed within a commercial framework that provides a procedural security infrastructure. Figure 2-1

in the MULTOS Security Target (ref [3]) details the MULTOS Infrastructure. It is assumed that the roles and responsibilities outlined in Appendix B of this document are within the infrastructure.

### **Summary of Security Features of the TOE**

C.5 The following Security Enforcing Functions (SEFs) are provided by MULTOS:

#### ***Application Load and Authentication SEF***

C.6 This function ensures that an application load request is authenticated as having been authorised by the MSM, prior to loading. A count of the number of failed attempts to load the application is maintained by the TOE. When the count reaches a defined limit, this function is permanently disabled. For an application load request to be successful the following conditions must be satisfied:

- MSM Controls Data must be loaded onto the smart card;
- The authorised application to be loaded must possess appropriate permissions before it is loaded;
- The application can not have previously been loaded, then deleted on the MULTOS card unless authorised by the MSM.

#### ***Application Separation SEF***

C.7 This function maintains separate storage and execution space for each application loaded onto a MULTOS card. In providing this function an application can only read code for execution from its own code space or from a pool of common routines controlled by MULTOS. A public area is available for the exchange of data to other applications and the outside world.

C.8 Functions residing on a MULTOS card can only execute or access other functions' resources via mechanisms provided and controlled by MULTOS.

#### ***Application Transport Confidentiality SEF***

C.9 This function enables the loading of authorised applications that have protected areas of code or data. Once the application is loaded MULTOS will remove the protection provided so it is available for execution. . A count of the number of failed attempts to execute this function is maintained by the TOE. When the count reaches a defined limit, this function is permanently disabled.

*Application Deletion SEF*

- C.10 This function enables the deletion of applications following the authentication that a delete request has been authorised by the MULTOS Security Manager. A count of the number of failed attempts to delete an application is maintained by the TOE. When the count reaches a defined limit, this function is permanently disabled.

*Object Reuse SEF*

- C.11 This function ensures that no part of an application's code or data, excluding data has placed into the Public data area, can be accessed after the application has been deleted.

*Smart Card Authentication SEF*

- C.12 This function provides a hash digest from selected areas of memory to determine that the smart card is an authentic initialised MCD. This function is only available on an initialised MCD, which has not been enabled.

*Key Installation SEF*

- C.13 This function ensures that an MCD can only load unique and protected MSM Controls Data once. A count of the number of failed attempts to execute this function is maintained by the TOE. When the count reaches a defined limit, this function is permanently disabled.

*Cryptography Control SEF*

- C.14 This function ensures that only applications specifically authorised by the MSM can access cryptography primitives. This function also verifies that the code of an application loaded onto an MCD is the same as the code originally approved for access to the cryptography primitives.

## Appendix D Identification of the TOE

### Configuration for Evaluation

D.1 The final evaluated configuration of the TOE is:

- a) Software - Keycorp MULTOS Version 4.02 (Release 1N' AMD)
- b) Hardware - Infineon (Siemens) SLE66CX160S

### Identification of the evaluated version of MULTOS

D.2 In order that an application loader or application writer can determine if a delivered product is in fact the evaluated product, the following procedures can be followed in making that determination.

D.3 Using a smart card terminal, the application loader and application writer can identify the MULTOS card by issuing a "Check Data" command with a random challenge value. This command will respond with a hash digest calculated over the entire MULTOS ROM image. Once the hash digest has been obtained, Keycorp Ltd. will verify that this is correct given the random challenge value chosen. The command can be issued in the manner described below:

1. Issue the "Check Data" command, detailed in section 8 of the MULTOS Developers Reference Manual (ref [12]), by entering the following hexadecimal query

```
>> BE 06 00 00 0C xx xx xx xx xx xx xx xx 00 00 80 00
```

Where *xx xx xx xx xx xx xx xx* is a random eight-byte challenge value.

2. The following data is displayed to the smart card reader stating that 10 hexadecimal bytes are available for checking

```
<< 61 10
```

3. Issue a Get Response command to view the 10 hexadecimal bytes response from the "Check Data" command

```
>> 00 0C 00 00 10
```

4. A sixteen-byte digest will be displayed dependent on the eight-byte challenge value chosen. This should be recorded.

```
<< rr rr rr rr rr rr rr rr rr rr rr rr rr rr rr rr
```

5. Request Keycorp Ltd. to perform a digest on a verified MULTOS card using the same random eight-byte challenge value chosen above. If the smart card is a MULTOS card, Version 4.02 (Release 1N' AMD), the digest produced by both parties should match.