AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAM

Certification Report

Certificate Number: 2003/30

Keycorp

MULTOS 1Q

Issue 1.0
October 2003

Issued by:

Defence Signals Directorate - Australasian Certification Authority

Executive Summary

This report describes the findings of the evaluation of Keycorp Limited's MULTOS 1Q under the Australasian Information Security Evaluation Program (AISEP). The report concludes that the product has met the target assurance level of Information Technology Security Evaluation Criteria (ITSEC) E6, and includes recommendations by the Australasian Certification Authority that are specific to the secure use of the product. The evaluation was performed by LogicaCMG Australasia and was completed in September 2003. The AISEP independently verified the cryptographic mechanisms implemented by MULTOS 1Q and found them suitable for Australian Government use.

Keycorp MULTOS 1Q is an Integrated Circuit Card (ICC) operating system that implements the MULTOS Version 4 specification defined and licensed by the MULTOS Consortium (MAOSCO Limited). MULTOS 1Q is capable of handling multiple applications resident on the one ICC. MULTOS 1Q ensures that each application is securely managed and cannot interfere with another application's operations, nor the operation of the MULTOS 1Q operating system.

MULTOS 1Q has been found to uphold the claims made in the Security Target (Ref [12]). Potential customers are urged to consult this document before planning to implement the product. Potential customers should also ensure that the product is deployed within its intended operational environment (as stated in the Security Target), in conjunction with the recommendations outlined in Chapter 8 of this report.

Ultimately, it is the responsibility of the customer to ensure that MULTOS 1Q meets their requirements. For this reason, it is strongly recommended that prospective customers of the product obtain a copy of the Security Target (Ref [12]) from the product vendor, and read this certification report thoroughly prior to deciding whether to purchase or implement the product.

Table of Contents

Chapter 1 Introduction

Intended Audience

This certification report states the outcome of the Information Technology Security Evaluation Criteria (ITSEC) evaluation of Keycorp Limited's MULTOS 1Q. It is intended to assist potential customers when judging the suitability of the product for their particular requirements. The most likely customer role would be that of MULTOS Carrier Device (MCD) issuer although other roles such as card manufacturer and application developer are possible.

Chapters 2 and 3 of this report deal with the security policy for the Target of Evaluation (TOE) and the intended environment for the TOE. These provide a high level view of the security problems that the TOE addresses and the way the TOE is used. These chapters are of particular interest to customers contemplating the MCD issuer role.

For those interested in the way that MULTOS 1Q fits into the greater MULTOS framework and the various roles that must be filled there is some information in Chapter 4: Documentation. All potential customers should be familiar with the MULTOS framework and the documentation available.

Chapters 5, 6 and 7 describe the evaluation and certification process. In particular, Chapter 5 breaks down the comprehensive testing that was performed by the evaluators. Chapter 7 provides some information on the history of the evaluation and the process involved in the evaluation and certification of the product.

Recommendations for potential customers are contained in Chapter 8. The recommendations are targeted at the card issuer role.

The appendices contain summary information that might be of use to potential customers. Appendix A contains a summary of the Keycorp MULTOS 1Q Security Target. Appendix B and C contain useful acronyms and references respectively. Appendix D contains a brief summary of all six ITSEC assurance levels.

Description of the TOE

The TOE is MULTOS 1Q, developed by Keycorp Limited. MULTOS 1Q is an Integrated Circuit Card (ICC) operating system that implements the MULTOS Version 4.06 specification defined and licensed by the MULTOS Consortium (MAOSCO Limited). MULTOS 1Q is capable of handling multiple applications resident on the one ICC (also referred to as MCD). Each application is securely managed and cannot interfere with another application's operations, nor the operation of the MULTOS 1Q operating system.

MULTOS 1Q is a single threaded operating system; only one application can be run at a time. All applications loaded on the MCD are written in the MULTOS specific language called MULTOS Executable Language (MEL). MEL applications are interpreted by MULTOS, rather than being compiled and executed directly by the smart card processor. Shared code routines, known as codelets can be called by an

executing application and although they execute in the context of the calling application, they have their own address space.

Possible MULTOS 1Q customers should note that the use of MULTOS 1Q directly leads to participation in the MULTOS commercial and security framework described by MAOSCO as the MULTOS Scheme and documented by MAOSCO in A Guide to the MULTOS Scheme (Ref [7]).

Identification

Table 1 provides identification details for the evaluation. For more information about the evaluated configuration refer to Chapter 6: Evaluated Configuration.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Keycorp MULTOS
Version	1Q, including AMD with ID (0020v003)
Security Target	Keycorp MULTOS Security Target, Version 5.0, 28th March 2002
Evaluation Level	ITSEC E6
Hardware Platform	Infineon SLE66CX160P or Infineon SLE66CX320P
Evaluation Technical Report	Evaluation Technical Report for Keycorp MULTOS 1Q, Version 1.1, September 2003
Version of ITSEC	ITSEC Version 1.2, 28 June 1991
Methodology Used	Information Technology Security Evaluation Manual (ITSEM) Version 1.0, 10 September 1993
	ITSEC Joint Interpretations Library (JIL) Version 2.0, November 1998
	Manual of Computer Security Evaluation Part I - Evaluation Procedures (EM4), Issue 1.0, April 1995
	Manual of Computer Security Evaluation Part II - Evaluation Techniques and Tools (EM5), Issue 1.0, April 1995
Sponsor	Keycorp Limited.
Developer	Keycorp Limited.
Evaluation Facility	LogicaCMG Australasia
Certifiers	Katrina Johnson, Aaron Doggett, Andrew Boulton, Chris Clacher

Chapter 2 Security Policy

The underlying security policy for the TOE defines the set of laws, rules and practices regulating the processing of sensitive information and the use of resources by MULTOS.

At the E6 level of assurance, the sponsor is required to provide a formal model of the security policy to define the underlying security policy to be enforced by the TOE. A summary of the informal representation of the security policy has been provided below.

Informal Security Policy

The Informal Security Policy for MULTOS 1Q is outlined in section 3.2 of the Security Target (Ref [12]), and is summarised below.

- Every MCD shall be uniquely identified.
- Every application shall be uniquely identified.
- The MULTOS Security Manager (MSM) shall authorise all requests to load and delete an application onto and from a MCD.
- The MSM shall also authorise the ability to subsequently reload an application if it is deleted from the smart card.
- Every application shall be authenticated before it is loaded onto a MCD, unless specific authorisation is given by the MSM.
- For every application, the MCD domain in which the application can be loaded shall be authorised by the MSM.
- An application loaded onto a MCD shall be able to read code for execution only from its own code space or from a pool of common routines controlled by MULTOS 1Q. Also, the application shall not be able to write to the code space of any application on the MCD, including its own.
- An application loaded onto a MCD shall not be able to read from the data space of any other application loaded onto the MCD except via a mechanism provided by and controlled by MULTOS 1Q, and with the cooperation of the target application. Also, the application can only write to the data space of another application via a mechanism provided by and controlled by MULTOS 1Q.
- An application loaded onto a MCD shall not be able to read or write MULTOS 1Q data except, via a mechanism provided and controlled by MULTOS 1Q.
- An application loaded onto a MCD shall not be able to write to the code space of MULTOS 1Q.
- It shall not be possible to read data from an application after that application has been deleted from a MCD.

Chapter 3 Intended Environment for the TOE

This section outlines the requirements and assumptions that govern the intended environment in which the TOE is designed to operate, and for which the TOE has been evaluated. Organisations wishing to implement the TOE in its evaluated configuration should review the evaluation scope to confirm that all the required functionality has been included in the evaluation, and must ensure that any assumed conditions are met in their operational environment.

Method of Use

The evaluation of MULTOS 1Q assumed that the TOE would be used in the following ways:

- MULTOS 1Q will only allow the MCD to load appropriately authorised applications.
- MULTOS 1Q will support the loading of encrypted applications.
- MULTOS 1Q will ensure that no applications loaded on the MCD will interfere with any other applications.
- MULTOS 1Q allows an MCD to be authenticated as a valid MULTOS equipped MCD.
- MULTOS 1Q restricts the use of strong cryptography to authorised applications.
- MULTOS 1Q limits the number of failed sensitive operations performed by the MCD. These sensitive operations include key installation, application loading and deleting.

Intended Environment Assumptions

The evaluation of MULTOS 1Q assumed that it would be used in the following environment.

MULTOS 1Q is masked into ROM and runs on a Infineon SLE66CX160P or SLE66CX320P integrated circuit embedded into a smart card. MULTOS 1Q interacts with it's external environment via commands issued to the smart card with the aid of an Interface Device (IFD). MULTOS 1Q responds to these commands or passes them on to MCD resident applications.

MULTOS 1Q equipped smart cards and MULTOS applications are manufactured and distributed within a commercial framework that provides a procedural security infrastructure.

Chapter 4 Documentation

The MULTOS framework described in the MULTOS 1Q documentation is a commercial model with ten roles identified in the Security Target (Ref [12]). These identified roles are:

1. MULTOS Security Manager (MSM)
2. MULTOS Implementor
3. IC Manufacturer
4. MCD Manufacturer
5. MCD Issuer
6. Application Writer
7. Application Provider
8. Application Issuer
9. Application Loader
10. MCD User

Potential MULTOS 1Q customers should read the Security Target (Ref [12]) to ensure that they understand these roles. The evaluators found that the MULTOS 1Q documentation met the ITSEC E6 requirements for user and administrator guidance. In particular, the MAOSCO document A Guide to the MULTOS Scheme (Ref [7]) contains a simplified description of the MULTOS framework. Anybody wishing to obtain an understanding of the MULTOS framework should consult this document.

The evaluators found that MAOSCO and Keycorp Limited have further documentation available for each specific user category mentioned above where it is required to explain the secure operation of the TOE.

Chapter 5 IT Product Testing

The objectives associated with the testing phase of evaluation can be placed into the following categories:

- **Functional testing:** Tests performed to ensure that the TOE operates according to its specification and is able to meet the requirements stated in the Security Target (Ref [12]).
- **Penetration testing:** Tests performed by the evaluators on the TOE to confirm whether or not known vulnerabilities are actually exploitable in practice.

Functional Testing

As part of the implementation work package the evaluators checked the developer's test documentation to ensure that it contained the purpose of the tests, traceability, procedure, justification of coverage and the developer results. The developers also provided a library of test programs that the evaluators used to repeat selected developer tests. This allowed the evaluator to verify the developer tests and also to provide input into the development of penetration tests described below.

Penetration Testing

The developers provided a construction vulnerability analysis and an operational vulnerability analysis for MULTOS 1Q. They identified possible vulnerabilities that were addressed by MULTOS 1Q design and developer testing. The evaluators also devised further tests to address these possible developer-identified vulnerabilities.

The evaluators also independently developed further penetration tests based on the functional tests described above and based on identified generic IT system vulnerabilities.

Summary

Testing was carried out on test MCDs and on MCD emulators. The evaluators tested MCDs based on the SLE66CX320P chip and MCDs based on SLE66CX320P and SLE66CX160P emulation. By duplicating tests on these three platforms the evaluators were able to obviate the need for testing MCDs based on the SLE66CX160P chip without a loss of assurance.

Through a process involving testing, duplicate testing and re-testing the evaluators determined that no potential vulnerabilities had been found to be exploitable within the scope of the Security Target (Ref [12]).

Chapter 6 Evaluated Configuration

The TOE underwent no version changes during the course of the evaluation. The evaluated version was MULTOS 1Q, which implements the MAOSCO MULTOS 4.06 standard.

The evaluated configuration was:

- Software – MULTOS Keycorp 1Q, including AMD with ID (0020v003)
- Hardware – Infineon SLE66CX160P or SLE66CX320P

The Keycorp MULTOS Mask Verification Procedure document (Ref [15]) describes how a MCD manufacturer or MCD issuer or a bureau acting on their behalf can use the MULTOS Check Data command to verify the authenticity of MULTOS 1Q prior to the loading of MSM Controls Data.

Chapter 7 Results of the Evaluation

Evaluation History

The E6 evaluation of Keycorp Limited's MULTOS 1Q completed in September 2003. This followed an E6 evaluation of MULTOS 1N', which was completed by the same evaluation facility in May 2000. The certification report for the MULTOS 1N' product (Ref [3]) indicates that it implemented an earlier version of the MULTOS V4 specification running on an earlier Infineon integrated circuit. For MULTOS 1Q the implemented version of MULTOS has increased at the minor version level and runs on more recent Infineon integrated circuits as described in Chapter 6 of this certification report.

The evaluation of MULTOS 1Q was an evolutionary increment of the evaluation of MULTOS 1N'. In general, evaluation procedures, tools and techniques used in the MULTOS 1N' evaluation were used as a basis for this evaluation. The testing procedures for MULTOS 1Q were refined and updated from the testing procedures used in the earlier evaluation. All tests in the procedures were re-done. The evaluators also performed the development environment assessment again.

Evaluation Procedures

The criteria against which the TOE is judged are expressed in the ITSEC (Ref [9]). The methodology used is described in the Joint Interpretations Library (JIL), Information Technology Security Evaluation Manual (ITSEM) and Evaluation Memoranda (EM) 4 and 5 (Refs [11], [10], [16], [17]). The evaluation was also carried out in accordance with the operational procedures of the AISEP (Refs [1], [2]).

Delivery Procedures

The certifiers independently considered the delivery procedures in place for the transfer of mask information from Keycorp Limited to Infineon and for the transfer of additional TOE component information from Keycorp Limited to the MULTOS CA. These procedures were deemed to be adequate when taken in conjunction with the secure delivery recommendation included in Chapter 8 that allows the MCD manufacturer or MCD issuer or bureau acting on their behalf to check that the MCD is the evaluated version.

Supporting Hardware

The certifiers also considered it important to independently consider the security of the Infineon SLE66CX160P and SLE66CX320P integrated circuits, as once the MCDs are dispersed to the end-user the integrated circuits could be subject to attacks outside the scope of this evaluation. The certifiers received information from MAOSCO (Ref [8]) that indicates that the Infineon SLE66CX320P integrated circuit has been given MULTOS Hardware Type Approval. The certifiers note that the SLE66CX160P has the same detailed specifications as the SLE66CX320P with the exception that it contains half of the amount of EEPROM. The certifiers are also

aware that both the Infineon SLE66CX320P and SLE66CX160P have been evaluated at the E4 assurance level by TÜViT of Germany (Refs [4], [5]). The certifiers have thus formed the view that the SLE66CX320P and SLE66CX160P are adequate for use in MULTOS 1Q MCDs.

Cryptography

The certifiers also note that all mechanisms of the TOE that could be subverted by direct attack were cryptographic in nature and thus subject to evaluation by DSD. These mechanisms were independently evaluated by DSD (Ref [6]). The cryptographic primitives provided by MULTOS 1Q include operations that are approved for Australian Government use. These approved primitives include DES and Triple-DES in CBC mode for signature generation, SHA-1 hashing algorithm and the MULTOS 1Q Random Number Generator. MULTOS 1Q also provides a DES encipher/decipher primitive in Electronic Code Book mode. Electronic Code Book mode is not approved for Australian Government use but can be used to build modes of use that are Australian Government approved. MULTOS 1Q also provides Modular Exponentiation primitives that can be used to implement RSA public key cryptography at an Australian Government approved length of 1024 bits.

The certifiers note that the MULTOS 1Q product uses 768-bit RSA public key cryptography in two instances to contribute to the optional application confidentiality feature of MULTOS 1Q. In one instance 768-bit RSA public key cryptography is used on a per-MCD basis to provide confidentiality to applications that are to be loaded onto each MCD. The certifiers consider 768-bit RSA public key cryptography adequate for this feature. The certifiers also note that 768-bit RSA public key cryptography is also used to provide certified copies of the public part of the above mentioned per-MCD keys to application developers who request to use application confidentiality for their applications. Given the peripheral nature of this security feature from the point of view of a potential Australian Government customer the certifiers have found that 768-bit RSA public key cryptography is suitable for this feature.

In summary, MULTOS 1Q has been found to use cryptographic mechanisms that are suitable for Australian Government use.

Certification Result

After due consideration of the Evaluation Technical Report (Ref [13]) produced by the evaluators and the conduct of the evaluation as witnessed by the certifiers, the Australasian Certification Authority has determined that MULTOS 1Q upholds the claims made in the Security Target (Ref [12]) and has met the requirements of the ITSEC E6 assurance level.

Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability that exploitable vulnerabilities remain undiscovered.

General Observations

The certifiers would like to acknowledge the invaluable assistance provided by LogicaCMG Australasia and Keycorp Limited staff during the evaluation. The successful completion of this evaluation and certification was made possible by their cooperation, technical assistance and attention to issues raised during the process.

Chapter 8 Recommendations

The following recommendations include information highlighted by the evaluators during their analysis of the developer's deliverables during the conduct of the evaluation. Recommendations from the Certification Report for MULTOS 1N' (Ref [3]) are also included as they are still valid.

MULTOS should only be used in accordance with the intended environment described in section 2.4 of the Security Target (Ref [12]), including consideration of all physical, personnel and procedural security measures.

Secure Delivery - Verification of the Evaluated Version of the TOE

The MCD manufacturer, MCD issuer or bureau acting on their behalf should use the Keycorp MULTOS Mask Verification Procedure (Ref [15]) to ensure that they are producing or using a genuine MULTOS 1Q MCD.

Environmental Security implemented by the MSM

The operational environment of the TOE includes a commercially based supporting security infrastructure. It is recommended Australian Government purchasers ensure that the physical and procedural security measures in place at the MSM Key Management Authority (MSM CA) are consistent with their own organisational security policies. A more detailed explanation of the supporting security infrastructure is provided in the Security Target (Ref [12]).

Environmental Security of MULTOS Application Providers

The MCD issuer should ensure that the application writers who provide the MCD applications have appropriate physical and procedural security measures to guarantee the integrity of developed applications.

Secure Operation of MULTOS Applications

MULTOS applications should be evaluated to a level of assurance commensurate with the purchaser's level of risk. This is required to minimise the risk that an incorrectly implemented application could inadvertently disclose information that may need to be kept confidential from other applications.

Use of Optional Application Signature in Application Load Certificates

Unless the MCD issuer is certain that any MULTOS Application Load Certificates are securely managed and that the application information provided by the application provider has guaranteed integrity then the MCD issuer should ensure that the MSM CA provides Application Load Certificates with settings that ensure that the optional application signature feature is enforced. The asymmetric key used for this application signature is generated by the application provider and can be up to 1024 bits long. The application provider must use the key space available to ensure security.

Appendix A Summary of the Security Target

A brief summary of the Security Target (Ref [12]) is given below. Potential purchasers should obtain a copy of the full Security Target to ensure that the security enforcing functions meet the requirements of their security policy. A copy of the Security Target can be obtained from Keycorp.

Security Objectives

MULTOS has the following IT security objectives.

- Preserve the mutual confidentiality of multiple applications loaded and executed on a single smart card.
- Preserve the mutual integrity of multiple applications loaded and executed on a single smart card.
- Confirm the authority of all application load and delete requests.

Intended Method of Use

The Intended Method of Use for MULTOS is:

U1 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.

U2 MULTOS will support a capability to load encrypted applications onto the smart card, decrypt such applications and make them available to the smart card for execution.

U3 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 application's code and data will not be available to other applications after it has been deleted.

U4 MULTOS will provide the capability to authenticate a card as a valid MULTOS-equipped smart card.

U5 MULTOS will provide the capability to restrict the use of regulated features of the smart card (e.g. strong cryptography) to authorised applications.

U6 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.

Intended Operating Environment

The intended operating environment for MULTOS 1Q is:

E1 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 via a service request (i.e., MULTOS system calls, known as primitives) made by an executing application.

E2 Supporting Hardware and Firmware. MULTOS operates on the Infineon Technologies SLE66CX160P and SLE66CX320P smart card integrated circuits. The integrated circuit provides the microprocessor to execute the instructions comprising the executable code of MULTOS. 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.

E3 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 1Q Security Target (Ref [12]) details the MULTOS infrastructure.

Summary of Security Features of the TOE

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

SEF 1 The application load and authentication SEF 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.

SEF 2 The application separation SEF 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.

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

SEF 3 The application separation SEF 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.

SEF 4 The application deletion SEF 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.

SEF 5 The object reuse SEF 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.

SEF 6 The smart card authentication SEF 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.

SEF 7 The key installation SEF 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.

SEF 8 The cryptography control SEF 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 B Acronyms

ACA	Australasian Certification Authority
ACE	AISEP Certificate Extension
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
AMD	Additional MULTOS Data
DSD	Defence Signals Directorate
EEPROM	Electrically Erasable Programmable Read Only Memory
ETR	Evaluation Technical Report
IC	Integrated Circuit
ICC	Integrated Circuit Card: The smart card.
IFD	Interface Device
ISO	International Standards Organisation
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
JIL	Joint Interpretations Library
MAOSCO	MULTOS Consortium (MAOSCO Limited)
MCD	MULTOS Carrier Device: The smart card.
MEL	MULTOS Executable Language
MSM	MULTOS Security Manager
MSM CA	MSM Key Management Authority
SEF	Security Enforcing Function
SOM	Strength of Mechanism
ST	Security Target
TOE	Target of Evaluation

Appendix C References

[1] AISEP Publication No.1- Description of the AISEP
AP 1, Version 2.0, February 2001
Defence Signals Directorate

[2] AISEP Publication No.2 - The Licensing of the AISEFs
AP 2, Version 2.1, February 2001
Defence Signals Directorate

[3] Certification Report for MULTOS Version 4.02 (Release 1N'-AMD)
AISEP Certificate Number: 2000/13
Issue 1.0, July 2000
Defence Signals Directorate

[4] Certification Report for Smart Card IC SLE 66CX160P
TÜViT file: TUVIT-DSZ-ITSEC-9121
September 2001
Bundesamt für Sicherheit in der Informationstechnik (BSI)

[5] Certification Report for Smart Card IC SLE 66CX320P
TÜViT file: TUVIT-DSZ-ITSEC-9115
August 2000
Bundesamt für Sicherheit in der Informationstechnik (BSI)

[6] Cryptographic Evaluation Report for Keycorp MULTOS 1Q
Defence Signals Directorate
23rd June 2003
(COMMERCIAL-IN-CONFIDENCE)

[7] Guide to the MULTOS Scheme
Version 2.00, 2000
MAOSCO Limited

[8] Hardware Evaluation Status Report for Infineon SLE66CX320P
September 2000
Mondex International Limited

[9] Information Technology Security Evaluation Criteria (ITSEC)
Version 1.2, June 1991
Commission of the European Communities

[10] Information Technology Security Evaluation Methodology (ITSEM)
Version 1.0, 10 September 1993
Commission of the European Communities

[11] Joint Interpretations Library (ITSEC JIL)
Version 2.0, November 1998
Joint Interpretations Working Group

[12] Keycorp MULTOS 1Q Security Target Version 5.0
March 2002
Keycorp Limited
(COMMERCIAL-IN-CONFIDENCE)

[13] Keycorp MULTOS 1Q Evaluation Technical Report (ETR)
Version 1.1, September 2003
LogicaCMG Australasia
(EVALUATION-IN-CONFIDENCE)

[14] Keycorp MULTOS Formal Security Policy Model
Version 4.0, March 2002
Keycorp Limited
(COMMERCIAL-IN-CONFIDENCE)

[15] Keycorp MULTOS Mask Verification Procedure
Revision 1.0, 2001
Keycorp Limited

[16] Manual of Computer Security Evaluation Part I - Evaluation Procedures (EM 4)
Issue 1.0, April 1995
Defence Signals Directorate
(EVALUATION-IN-CONFIDENCE)

[17] Manual of Computer Security Evaluations Part II - Evaluation Tools and Techniques (EM 5)
Issue 1.0, April 1995
Defence Signals Directorate
(EVALUATION-IN-CONFIDENCE)

Appendix D ITSEC Summary

ITSEC Assurance Levels

The requirements for each of the ITSEC assurance levels have been summarised in Table 2. Please note that MULTOS 1Q has met the requirements for ITSEC assurance level E6.

Table 2 – ITSEC Assurance Levels

Assurance Level	Description
E1	At this level there shall be a security target and an informal description of the architectural design of the evaluated Target Of Evaluation (TOE). Functionality testing shall indicate that the TOE satisfies its security target.
E2	In addition to the requirements for level E1, there shall be an informal description of the detailed design. Evidence of functional testing shall be evaluated. There shall be a configuration control system and an approved distribution procedure.
E3	In addition to the requirements for level E2, the source code and/or hardware drawings corresponding to the security mechanisms shall be evaluated. Evidence of testing of those mechanisms shall be evaluated.
E4	In addition to the requirements for level E3, there shall be an underlying formal model of security policy supporting the security target. The security enforcing functions, the architectural design and the detailed design shall be specified in a semiformal style.
E5	In addition to the requirements for level E4, there shall be a close correspondence between the detailed design and the source code and/or hardware drawings.
E6	In addition to the requirements for level E5, the security enforcing functions and the architectural design shall be specified in a formal style, consistent with the specified underlying formal model of security policy.

A detailed explanation of the assurance requirements for E6 can be found in the ITSEC (Ref [9]).