Type Approval Policy

MAO-DOC-TST-001 v3.1

Copyright

Trademarks

Document Information

Title	MULTOS Type Approval Policy
Reference	MAO-DOC-TST-001
Version	3.1
Date	November 2014

Target Audience

- MULTOS Consortium Members
- MULTOS and MULTOS step/one Licensees (including MULTOS Implementers)
- MAOSCO approved Testing Agents
- MAOSCO approved Evaluation Agents

Conventions

The use of the word "MULTOS" in relation to products refers to full MULTOS products only, step/one products are referred to explicitly as **step/one**.

Published by

MAOSCO Limited,
St. Andrews House,
The Links, Kelvin Close,
Birchwood,
Warrington.
WA3 7PB.
United Kingdom.

Tel: (+44) (0)1925 882050
Fax: (+44) (0)1925 882051
E-mail: kms_support@multos.com
Web: http://www.multos.com

1 Overview

MULTOS and **step/one** are high security, multi-application operating systems for secure micro-controllers. The specifications for these operating systems define in great detail the operational and security aspects of the systems. Due to the business and operational requirements for these products, the MULTOS Consortium recognises the need for a Type Approval process to test the compliance of such products with the MULTOS Implementation Specifications and MULTOS step/one Card Specification and to ensure products deliver appropriate security assurance.

The MULTOS Type Approval has four fundament pillars used to qualify an implementation as suitable for approval, which are:

1. Use of an approved chip
2. Protocol Testing
3. Interoperability Testing
4. Security Evaluation

This documents describes the details related to each of these pillars and also the process of awarding Type Approval

In some circumstances, MAOSCO may grant a concession on the completion of one or more of the components.

In some circumstances, MAOSCO may grant a temporary Type Approval to a product prior to the completion of one of more of the Type Approval components. This shall permit limited distribution according to the restrictions detailed in the notification of Type Approval. An implementer may not generally publicise the Type Approval of such a product, although it may be necessary and may be permitted to use the MULTOS branding in association to the product. MAOSCO must approve the use of the MULTOS brand with products granted temporary Type Approval prior to the use of the brand.

All MULTOS and **step/one** products that have achieved MULTOS Type Approval shall be listed on the MULTOS website.

Important

The MAOSCO Type Approval process does not approve individual vendors. The process allows products developed to the MULTOS and **step/one** specifications and requirements to be approved by MAOSCO.

MAOSCO issues Type Approval letters to eligible implementers against specific products for unlimited use internationally, unless restrictions are specified in the approval letter. A product is defined as the Operating System and all other components contained in either ROM or EEPROM of the product, including but not limited to, operating system executable code, Codelets, ROMlets,

fixed and variable keys and any other data contained in the AMD. Type Approval does not extend to the functionality of any Codelets, ROMlets or proprietary extensions contained within the product.

When granted, this Type Approval is provided by MAOSCO to record the successful examination of certain security and operational characteristics important to the MULTOS scheme as a whole. Type Approval does not under any circumstances include or imply any representations or warranties in relation to the approved product from MAOSCO or its affiliates, including, without limitation, any implied WARRANTIES OF MERCHANTABILITY, FITNESS FOR PURPOSE, OR NON-INFRINGEMENT, all of which are expressly disclaimed by MAOSCO and its affiliates. All rights and remedies regarding products and services which have received MAOSCO Type Approval shall be provided by the party providing such products or services, and not by MAOSCO.

Duration of Approval

MAOSCO does not normal specify a duration of Type Approval, however, if specified the Type Approval is valid only for the period stated on the relevant Type Approval letter.

Implementers should take into consideration that schemes usually only approve hardware (chips) for a limited period.

Moreover, MAOSCO constantly reviews its Type Approval process in the light of ongoing chip security developments, and reserves the right to remove Type Approval status for a product if MAOSCO believes that to do so is necessary to protect the security of MULTOS and **step/one**.

2 MULTOS Type Approval Components

The MULTOS Type Approval process is designed to ensure compliance with the MULTOS Implementation Specifications (and MULTOS step/one Card Specification, if appropriate) at both a technical and business requirements level. The process checks that all products sold under the MULTOS brand embody the MULTOS Consortium's shared values of high security, high assurance, quality, correctness and interoperability of implementations. This extends not only to the technical operation of a product internally and within a system, but also the way in which it is developed, manufactured and delivered to an end customer.

Without Type Approval, MULTOS products will not be loaded onto either the Global KMA or Independent KMAs and cannot therefore be issued.

Each component of the Type Approval process focuses on a separate area of the requirements for a MULTOS or **step/one** branded product. The components are described below:

2.1 Security Evaluation

This ensures that MULTOS products attain the highest levels of security assurance possible for commercially available products and gives customers of these products the highest measure of confidence that the product is both correctly implemented and can protect their assets within the product and may remove the need to evaluate the product to their own standards.

NOTE: This is not required for **step/one** products or qualifying MULTOS derivatives.

The evaluation scope and level of assurance **must** be either:

- Common Criteria EAL4+ or higher. In every case, the targeted assurance level must be augmented with the components AVA_VAN.5, ADV_IMP.2 and ALC_DVS.2 OR
- An approved payment scheme security evaluation, e.g. Mastercard C.A.S.T.

The evaluation process must be undertaken by an independent evaluation laboratory recognised by the scheme.

There are instances where MAOSCO may waive the requirement to complete the Security Evaluation process. These instances are typically where an individual product is to be developed for and supplied to a specific customer and shall be submitted for a security evaluation meeting that customer's own security requirements. In these instances, restrictions may be placed on the supply of product and the use of the MULTOS branding. An implementer that develops a product that is not developed, evaluated and certified in accordance with the process described in this document shall NOT offer that product for sale or otherwise provided for use in any way whatsoever; the implementer will not be permitted to use the MULTOS branding and the product shall NOT be referred to as a MULTOS Product.

2.2 Approved Chips

Type Approval requires that approved chips must be used.

Approved chips are those which have one or more of the following.

- Common Criteria Approval to a level of EAL4 or above with augmentation to AVA_VAN.5 and ALC_DVS.2. A list of CC approved chips is available at http://www.commoncriteriaportal.org/products/
- EMVCo Approval at the time of applying for Type Approval. A list of EMVCo certified chips is available at http://www.emvco.com/approvals.aspx?id=81

2.3 Protocol Testing

MULTOS and **step/one** products provide contact and proximity interfaces to terminals or other Interface Devices. These interfaces are typically implemented according to the ISO/IEC 7816 and ISO/IEC 14443 series of specifications. Testing of compliance to these standards must be done in accordance with the current EMVCo *Level 1Card Test* plan.

However, a majority of end user customers deploy MULTOS and **step/one** products as financial payment cards for use in EMV compliant terminals. Therefore these products must additionally comply with the EMVCo *Level 2 Card Test* plan.

These tests usually form part of payment scheme card-type approvals.

The resultant reports must be submitted to MAOSCO for consideration and confirmation that the protocols are conformant to the relevant standards.

In some circumstances, for instance when a specific MULTOS or **step/one** product is to be deployed in a closed environment, with differing requirements MAOSCO may grant a concession on the completion of the protocol testing component or accept alternative testing processes,

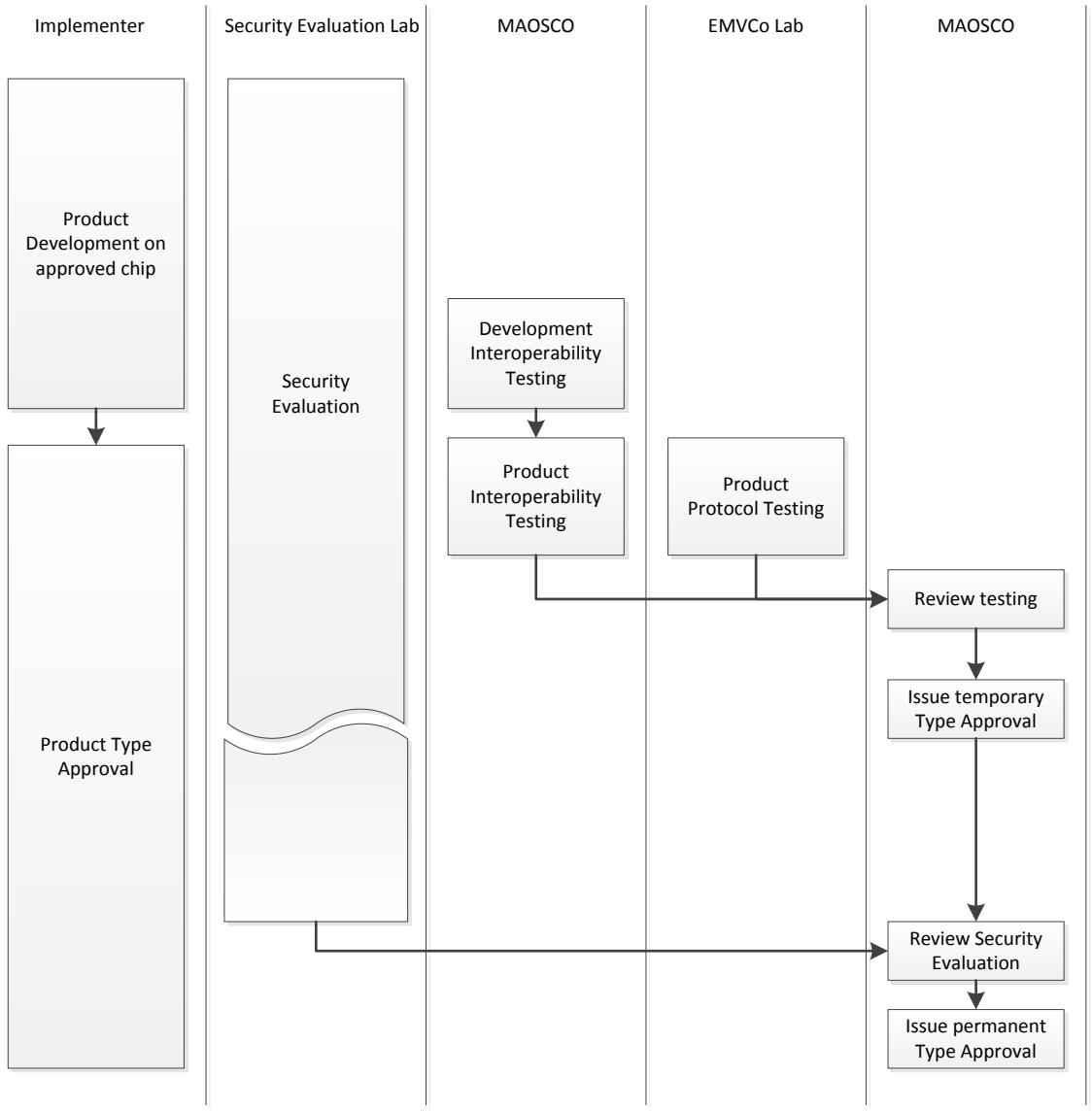
2.4 Interoperability Testing

Interoperability testing is intended to test that a MULTOS or **step/one** Operating System implementation conforms to the MULTOS Implementation Specification (and in the case of **step/one**, the MULTOS step/one Card Specification) from an internal and external standpoint. This is to ensure that all MULTOS and **step/one** products provide the same operating environment and API for MULTOS on-card applications and that the external interfaces to terminals, smart card readers and systems are electrically and logically interoperable. The scope of this testing includes the mechanisms for manufacturing and enabling a device, the application load and delete mechanism and for MULTOS, the product's integration into the MULTOS Key Management Authority infrastructure.

Interoperability Testing shall be performed on behalf of the implementer by MAOSCO Ltd.

Successful completion of the Interoperability Testing does not indicate that the MULTOS or **step/one** Implementation is free of defects and does not constitute a warranty of future performance. MAOSCO Limited accepts no liability for any reliance placed on the results of the Interoperability Testing or any other part of the Type Approval process.

3 Type Approval



MULTOS Type Approval Process

When all components in section 2 have been complied with the Product will be awarded Type Approval without limitation.

3.1 Pre-certification Approval

It is recognised that the Security Evaluation processes may take a number of months to complete. To allow Implementers to sell their MULTOS products before the Security Evaluation certificate has been awarded, the MULTOS Consortium have developed and adopted a policy for the supply of

chips while this is pending. Such products must have been completed all of the remaining Type Approval Components.

The aim of the policy is to ensure that information regarding the pre-certification status of a MULTOS product is passed through the supply chain to the MULTOS Issuer and to any third party Application Providers in order to enable them to make informed decisions regarding the purchase and use of MULTOS products for which a security evaluation certificate is yet to be awarded. Full details of the policy and associated branding requirements can be found in the MULTOS Brand Manual MAO-DOC-MKT-002.

The following criteria must be satisfied for each MULTOS product version[1] before a product can be offered for sale or otherwise advertised or distributed

1. The product is on an approved chip and the Interoperability testing is complete.
2. The product must be developed in accordance with a methodology that is compatible with the Security Assurance being undertaken
3. The development must be complete with no remedial action outstanding.
4. The laboratory responsible for performing the evaluation must have been formally engaged to undertake the evaluation and evidence shown such as contract, purchase order or written statement from the laboratory.

Based upon this, MAOSCO may Issue a type approval letter with the conditions and restrictions noted, and also a restricted lifetime for the type approval. The product will loose its type approval status if the outstanding Type Approval components are not achieved by that time.

The Implementer must include a notice in its terms and conditions governing the supply of the pre-certified product and similarly, the Issuer must include a notice in its terms and conditions with third party Application Providers that:

- the Security Evaluation certificate has yet to be awarded;
- the Security Evaluation process has started, however, that there is a possibility that certification may not be obtained;
- MULTOS Type Approval has been obtained on a limited basis;
- all Issuers and third party application providers to whom the product has been supplied will be informed in writing of the outcome of the Independent Security Evaluation and Certification process, whether successful or unsuccessful, within 30 days of the Implementer being formally advised of the outcome;

[1] Note that where a product version is a modification of a previously evaluated and certified version, Type Approval may be limited to the modifications and aspects of the original version affected by those modifications.

- all Issuers and third party Application Providers to whom the product has been supplied will be informed in writing of any remedial action affecting them resulting from an unsuccessful certification (i.e. failing to achieve the intended level of assurance or an appropriate Strength of Mechanisms) within 30 days of the Implementer being formally advised of the remedial action;
- the product complies with MAOSCO Policy (as described in this document).

In addition, the Implementer must also inform MAOSCO in writing of product development and pre-certification status.

3.2 Failure to achieve Certification or Cancellation of the Security Evaluation process

If the product fails to achieve certification or the Security Evaluation process is cancelled, the Implementer may no longer sell that product and must notify all Issuers and third party Application Providers to whom the ***product*** has been sold of this failure and the reasons for the failure, in order for all parties to be aware of the situation and to be able to act accordingly. MAOSCO may also require from the Implementer that the product be de-configured at any MULTOS Key Management Authority with which it is associated.

3.3 Use of the MULTOS Brand Mark and/or Word Mark

Prior to receiving successful certification, cards offered for sale or otherwise advertised or distributed must comply with the following criteria:

- Where cards are branded with the MULTOS Brand Mark or Word Mark (as defined in the Brand Manual), the MULTOS Brand Mark or Word Mark must be used with an asterisk and the back of the card must display the words '* - *Security Evaluation certification pending*'. It is also recommended that the Issuer be able to identify by electronic means such cards in case they have to be withdrawn or modified (e.g. by version number, chip ID, etc).
- Where an Issuer chooses not to display the MULTOS Brand Mark nor the Word Mark with the asterisk and the above wording the MULTOS Brand Mark and Word Mark may not be used at all, however, the Issuer must be able to identify by visual or electronic means such cards in case they have to be withdrawn or modified (e.g. by version number, chip ID, or other mark defined by the Issuer).

Notes:

Note (1): It is possible for more than one laboratory to undertake an evaluation or parts of an evaluation, and for more than one Certification Body to be involved. The above criteria should be interpreted as including multiple laboratories or Certification Bodies where these circumstances occur.

Note (2): The above criteria assume that only properly qualified Common Criteria Certification Bodies are authorised to issue CC certificates, and that all laboratories are duly accredited by such Certification Bodies. The criteria for acceptable Certification Bodies shall be:

- those Certification Bodies qualified by for the Recognition Agreement of Information Technology Security Evaluation Certificates as selected by the Management Committee of the Agreement Group for the Senior Officials Group for Information Security (SOG-IS) of the European Commission;
- additional Certification Bodies based outside the European Union as selected by the MAOSCO Technical Advisory Group.

4 Derivative Products

Implementers may need to further enhance and develop Type Approved products to meet market and customer requirements. The Type Approval process for derivative products is designed to allow Implementers this flexibility of building upon a *Baseline Implementation* of a "Type Approved Product", without needing to repeat all the Type Approval testing for each and every product. In order to qualify a new product within the scheme, the Implementer shall submit an acceptable "Self-Certification Report for Derivative Product" to MAOSCO. MAOSCO shall determine whether the proposed product may be Type Approved as a derivative or whether the product shall be subject to some or all of the complete Type Approval process.

The qualification criteria that shall be used to qualify a product as a derivative are as follows:

- The *Baseline Implementation* on which the product is based must not be a derivative product but have completed the full Type Approval process. The Baseline Implementation must be clearly identified by reference to its Type Approval certificate number.
- The hardware platform for the product shall be from the same manufacturer and be the same or substantially similar to that of the *Baseline Implementation* although it may not necessarily have achieved a certificate.
- The Security Target (not applicable to **step/one)** of the product must be the same or a superset of that of the *Baseline Implementation*. The differences in Security Target must be due to either the changed hardware platform or improvements to the security enforcing features of the product. New security enforcing features may be introduced if they do not impact those previously evaluated by the Security Evaluation of the *Baseline Implementation*.
- The product must be developed within the same development environment as that of the *Baseline Implementation*. Any changes of the development environment, such as physical location, design methodology, development tools, third-party software libraries or testing environment must be declared. All product developments must continue to

use the methodology and rigorous processes used for the *Baseline Implementation*. Products must be designed and developed to achieve the same Security Evaluation assurance level as the *Baseline Implementation*, if it was required.

The “Self Certification Report for Derivative Products” should be submitted to MAOSCO at the earliest opportunity, prior to the request for MULTOS Type Approval, in order that MAOSCO may determine whether the product qualifies as a derivative. In many cases, components of the Type Approval process may be required to be repeated, at the discretion of MAOSCO. In some cases, even when a complete Security Evaluation is not required, MAOSCO may require components of the evaluation process to be completed in order to provide independent verification that the security of the product has not been affected by the changes from the base implementation.

Following successful completion of any required Type Approval processes, a letter of Type Approval will be issued which will indicate that the product is a derivative but otherwise the product may be issued as if it had completed the full Type Approval process.

The implementer shall provide a summary report that may be published on the MULTOS website and provide customers details of the differences between the product and the *Baseline Implementation*.

--- End of Document ---

