FIF

MULTOS KMA File Interface

maos-gkc-spc-002/1 v7.3

© 2017 MAOSCO Limited.

MULTOS is a registered trademark of MULTOS Limited.

Copyright

© Copyright 2017 MAOSCO Ltd. This document is confidential. No part of this document may be reproduced, published or disclosed in whole or part, by any means: mechanical, electronic, photocopying, recording or otherwise without the prior written permission of MAOSCO Ltd. This document is made available under the terms of the confidentiality agreement signed with MAOSCO Ltd. and must not be disclosed to any other person or organisation otherwise than as set out in the terms of that confidentiality agreement.Preface

This document defines the data files used to communicate with a MULTOS KMA (Key Management Authority) using the StepNexus StepServer/StepXpress system. Note that this document applies equally to the MAOSCO approved Global KMA and any iKMA.

Objectives

The objective is to ensure that external parties can easily communicate with a KMA and a KMA can efficiently process orders.

Scope

This document covers all the external interfaces to a KMA from Issuer and Bureaux, MULTOS implementers and application providers

Audience

Anyone involved in the design and implementation of elements within the MULTOS scheme.

Related Documents

Integrated circuit card(s) with contacts - Part 3: Electronic Signals and transmission protocols
ISO/IEC 7816-3

Integrated circuit card(s) with contacts - Part 5: Registration System for international applications in integrated circuit(s) cards
ISO/IEC 7816-5

Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 4: Transmission protocol
ISO-IEC 144433-4

Secure Hash Standard (SHS)
FIPS-PUB 180-1

Assumptions

It is assumed that the reader knows the basics of MULTOS and KMA Interfacing.

Issues

None.

MULTOS is registered trademark of MULTOS Limited.

Table Of Contents

 © 2016 MAOSCO Limited.

MULTOS is a registered trademark of MULTOS Limited.

1 Introduction

This document defines the external interface to a KMA for data transfer to / from Issuers, Bureaux and similar bodies.

It defines the format and content of the files used to transfer information. In this document, numbers prefixed with 0x are hexadecimal representations of single or multiple byte numbers.

2 File Types

The following file type codes are used to define the different types of data file. This list may grow with time.

File Type Code	File Contents	File Name Extension
-	MCD_ID list included in requests	-
-	Application Provider Public Key	-
-	Application Definition File (optional when registering applications)	.adf, .aif, .dat, .json, .xml
MSML	MSM Controls response sent by KMA	.msm
ALCR	ALC response sent by KMA	.alr
ADCR	ADC response sent by KMA	.adr
TKCK	MULTOS Transport Key Certification Key	.key
HASH	MULTOS Hash Modulus	.mhm
ADMD	Additional MULTOS Data	.amd

Notes

Each file carries at the start a 4 byte File Type Code followed by two one byte fields. The first of these is the File Protection method ID - this defines the way the file is protected. The second byte is the File Structure Method ID. This defines the way the data in that type of file is assembled. The meanings of these control bytes are context dependent on the file type.

Response files generated by the KMA will be named <Batch_GUID>,<filename extension>, where <Batch_GUID> is a filename that will allow the user to track the request uniquely. When a response is ready for collection an email will be sent informing the user of the filename.

All file data is stored as binary data with no record delimiters. All multi-byte binary values are stored in "Big-Endian" or Motorola format.

In the following sections, data items in *italics* will be found in the data dictionary. Items in **bold** are the subject of tables in their own right. Items in parentheses thus { } are repeated. Items in normal font are simple length or integer values that do not need further explanation.

 © 2017 MAOSCO Limited.

MULTOS is a registered trademark of MULTOS Limited.

3 MCD_ID List File

When ordering enablement it s a requirement that the requester upload a binary file specifying which cards are to be enabled. When ordering load or delete certificates there is also an option to upload a binary file specifying which per-card certificates are required.

3.1 MCD_ID file format

Data	Definition
{ ***MCD_ID List Record*** }	Occurs multiple times. See note below

The maximum permitted number of MCD_ID List Records that may be included in one request file is currently 200,000. It is highly recommended however that all requests are for 20,000 sets of enablement or less, since the resulting response files can be extremely large and difficult to transfer and store.

3.2 MCD_ID List Record

Data	Definition
IC_Manufacturer_ID	Binary, 1 byte
IC_Type	Binary, 1 byte
MCD_ID	Binary, 6 bytes

This list is expected to be in a single file, consisting simply of repeated MCD ID List Records as shown above, with no record delimiters, header information or checksums of any kind. It is not expected that the MCD IDs within the file are in any order. This facility is provided to allow the easy generation of enablement requests from a list provided by the card manufacturer. Note therefore that the Issuer or Bureau generating this request will have to obtain that file from the manufacturer first (or generate the list themselves by interrogating the cards).

It is essential that every MCD in a request file is of the same ROM mask, as indicated by the IC_Manufacturer_ID and IC_Type fields.

4 Application Provider Public Key File

An application provider can optionally sign their applications. To do so, they must pass the entity requesting load certificates a copy of their public key. It is assumed that the public exponent of the key has a fixed value of 0x03. The modulus is passed in the following format.

MULTOS is registered trademark of MULTOS Limited.

Data	Definition
Modulus_Length	Binary, 2 bytes. The length in bytes of the Application Provider modulus
Modulus	Binary, Modulus_Length bytes. Modulus of key used to sign the Application Unit

5 Application Definition File

When registering applications it is possible to import an Application Definition File rather than completing all the details on-screen. This file would be supplied by the application provider. The application definition can be written in 3 formats:

- Comma separated values (CSV) – A legacy format (.adf, .aif, .dat).
- XML (.xml)
- JSON (.json)

If an application provider requires assistance in creating such a file or to obtain the schema definition files then please contact Customer Support at a MULTOS KMA for guidance.

5.1 JSON and XML Formats

The following table contains a breakdown of each element. Optional elements which are not specified will assume its default value.

Attribute	Definition	Mandatory	Default Value
applicationId	Application ID. Hexadecimal hex string between 2 and 32 characers (1-16 bytes)	Yes	
description	Application Description. Minimum of 1 character	Yes	
codeSize	Code size. Integer interpreted as decimal. Range from 0 – 65535.	Yes	
dataSize	Data size. Integer interpreted as decimal. Range from 0 – 65535.	Yes	
fciSize	File control information record size. Integer interpreted as decimal. Range from 0 – 65535.	Yes	
dirSize	Directory record size. Integer interpreted as decimal. Range from 0 – 65535.	Yes	
sessionSize	Session data size. Integer interpreted as decimal. Range from 0 – 65535.	Yes	
codeHash	Code Hash using SHA-1 or SHA-256. Hexadecimal hex string. 40 characters (20 bytes) for SHA-1 or 64 characters (32 bytes) for SHA-256	Yes	
aluType	Object – see definition below	No	See below for default values

 © 2017 MAOSCO Limited.

MULTOS is a registered trademark of MULTOS Limited.

Attribute	Definition	Mandatory	Default Value
signed	Indicates that the application contains an application signautre. Boolean (true or false).	No	false
encrypted	Inididates that the application contains encrypted areas. Boolean (true or false).	No	fale
historicalBytes	Object – see definition below.	No	See below for default values
primaryAtr	The application has control over the historical bytes for the primary ATR. Boolean (true or false).	No	false
secondaryAtr.	The application has control over the historical bytes for the secondary ATR. Boolean (true or false).	No	false
ats	The application has control over the historical bytes for the ATS. Boolean (true or false).	No	false
fileModeType	Object – see definition below.	No	See below for default values
applicationType	The application's operating mode. String. Possible values are: • Normal • Shell • Default • Proprietary	No	Normal
dualFci	Indicates whether an application contains a contact and contactless file control information record. If false, then it assumed that the application contains a single FCI. Boolean (true or false).	No	false
memoryAllocationInBlocks	Indicates whether the application's data size is in multiple of 255 byte blocks. If false, then the data size is to be interpreted in bytes. Boolean (true or false).	No	false
proprietaryLoad	Indicates whether an application should be loaded in a proprietary defined way. Boolean (true or false).	No	false
accessList	Object – see definition below	No	See below for default values
strongCryptography	Indicates whether an application uses strong cryptographic algoritms. Boolean (true or false).	No	false
contactInterface	Indicates whether an application can be executed over the contact interfae. Boolean (true or false).	No	false
contactlessInterface	Indicates whether an application can be executed over the contactless interface. Boolean (true or false).	No	false

MULTOS is registered trademark of MULTOS Limited.

Attribute	Definition	Mandatory	Default Value
gsmAuthenticate	Determines if the application supports supports the GSM authenticate protocol. Boolean (true or false).	No	false
cardBlock	Determines if the application can have the ability to block the card. Boolean (true or false).	No	false
cardUnblock	Determines if the application can have the ability to un-block the card. Boolean (true or false).	No	fale
retainSessionData	Determines if an application's session data should be maintained between application selection. Boolean (true or false).	No	False
processEvents	Determines if an application should be executes in particular events. Boolean (true or false).	No	False
cardManagerApplication	Determines if an application implements application specific lifecycle functionality. Boolean (true or false).	No	false
peripheralAccess	Determines if an application should have access to off-chip peripherals. Boolean (true or false).	No	false
pinAccess	Determines what level of access an application to the pin object. String. Possible values are: • Own • GlobalBasic • GlobalStandard • GlobalFull	No	Own

 © 2017 MAOSCO Limited.

MULTOS is a registered trademark of MULTOS Limited.

5.1.1 JSON Format

Application definition files using the JSON format must have the file extension .json.

5.1.1.1 Schema

The schema definition is as follows:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "version": "1.0",
   "type": "object",
   "title": "MULTOS Application Defifintion File Format vXXXX ",
   "description": "Used to define an application whhich can be used for application registeration.",
   "additionalProperties": false,
   "properties": {
         "applicationId": {
               "type": "string",
               "pattern": "^([0-9a-fA-F]{2}){1,16}$",
               "title": "ApplicationId schema.",
               "description": "The Application ID (hexadecimal string)."
         },
         "description": {
               "type": "string",
               "minLength": 1,
               "title": "Description schema.",
               "description": "The application description."
         },
         "codeSize": {
               "type": "integer",
               "multipleOf": 1,
               "maximum": 65535,
               "minimum": 0,
               "exclusiveMaximum": false,
               "exclusiveMinimum": false,
               "title": "CodeSize schema.",
               "description": "The application code size in decimal."
         },
         "dataSize": {
               "type": "integer",
               "multipleOf": 1,
               "maximum": 65535,
               "minimum": 0,
               "exclusiveMaximum": false,
               "exclusiveMinimum": false,
               "title": "DataSize schema.",
               "description": "The application data size in decimal."
         },
         "sessionSize": {
               "type": "integer",
               "multipleOf": 1,
               "maximum": 65535,
               "minimum": 0,
               "exclusiveMaximum": false,
```


MULTOS is registered trademark of MULTOS Limited.

```
                "exclusiveMinimum": false,
                "title": "SessionSize schema.",
                "description": "The application session data size in decimal."
        },
        "dirSize": {
                "type": "integer",
                "multipleOf": 1,
                "maximum": 65535,
                "minimum": 0,
                "exclusiveMaximum": false,
                "exclusiveMinimum": false,
                "title": "DirSize schema.",
                "description": "The application DIR data size in decimal."
        },
        "fciSize": {
                "type": "integer",
                "multipleOf": 1,
                "maximum": 65535,
                "minimum": 0,
                "exclusiveMaximum": false,
                "exclusiveMinimum": false,
                "title": "FciSize schema.",
                "description": "The application FCI data size in decimal."
        },
        "historicalBytes": {
                "type": "object",
                "title": "HistoricalBytes schema.",
                "description": "Determines whether the application has control of the historical
bytes",
                "properties": {
                        "primaryAtr": {
                                "type": "boolean",
                                "title": "PrimaryAtr schema.",
                                "description": "The application has control over the historical bytes for
the primary ATR.",
                                "default": false
                        },
                        "secondaryAtr": {
                                "type": "boolean",
                                "title": "SecondaryAtr schema.",
                                "description": "The application has control over the historical bytes for
the secondary ATR.",
                                "default": false
                        },
                        "ats": {
                                "type": "boolean",
                                "title": "Ats schema.",
                                "description": "The application has control over the historical bytes for
the ATS.",
                                "default": false
                        }
                },
                "additionalProperties": false
        },
        "aluType": {
```


 © 2017 MAOSCO Limited.

MULTOS is a registered trademark of MULTOS Limited.

```
            "type": "object",
            "title": "AluType schema.",
            "description": "Determines how the application will be loaded.",
            "properties": {
                  "signed": {
                        "type": "boolean",
                        "title": "Signed schema.",
                        "description": "Indicates whether the application is signed.",
                        "default": false
                  },
                  "encrypted": {
                        "type": "boolean",
                        "title": "Encrypted schema.",
                        "description": "Indicates whether the application is encrypted.",
                        "default": false
                  }
            },
            "additionalProperties": false
      },
      "fileModeType": {
            "type": "object",
            "title": "FileModeType schema.",
            "description": "The properties which determines the application file_mode_type",
            "properties": {
                  "applicationType": {
                        "type": "string",
                        "enum": [
                              "Normal",
                              "Default",
                              "Shell",
                              "Proprietary"
                        ],
                        "title": "ApplicationType schema.",
                        "description": "Indidicates the type of applicaiton.",
                        "default": "Normal"
                  },
                  "dualFci": {
                        "type": "boolean",
                        "title": "DualFci schema.",
                        "description": "Indidates whether the application has contains a dual fci.
If false then it is assumed the application contains a single FCI.",
                        "default": false
                  },
                  "memoryAllocationInBlocks": {
                        "type": "boolean",
                        "title": "MemoryAllocationInBlocks schema.",
                        "description": "Indicates whether the application's data size is in
multiple of 255 byte blocks. If false, then the data size is to be interpreted in bytes.",
                        "default": false
                  },
                  "proprietaryLoad": {
                        "type": "boolean",
                        "title": "ProprietaryLoad schema.",
                        "description": "Determines if an application should be loaded in
proprietary defined way.",
                        "default": true
```


MULTOS is registered trademark of MULTOS Limited.

```
                        }
                  },
                  "additionalProperties": false
            },
            "accessList": {
                  "type": "object",
                  "title": "AccessList schema.",
                  "description": "The application's access list properties.",
                  "properties": {
                        "strongCryptography": {
                              "type": "boolean",
                              "title": "StrongCryptography schema.",
                              "description": "Determines if the application uses strong cryptography.",
                              "default": false
                        },
                        "contactInterface": {
                              "type": "boolean",
                              "title": "ContactInterface schema.",
                              "description": "Determines if the application can be executed over the
contact interface.",
                              "default": false
                        },
                        "contactlessInterface": {
                              "type": "boolean",
                              "title": "ContactlessInterface schema.",
                              "description": "Determines if the application can be executed over the
contactless interface.",
                              "default": false
                        },
                        "gsmAuthenticate": {
                              "type": "boolean",
                              "title": "GsmAuthenticate schema.",
                              "description": "Determines if the application supports the GSM Authenticate
protocol.",
                              "default": false
                        },
                        "cardBlock": {
                              "type": "boolean",
                              "title": "CardBlock schema.",
                              "description": "Determines if the application can have the ability to block
the card.",
                              "default": false
                        },
                        "cardUnblock": {
                              "type": "boolean",
                              "title": "CardUnblock schema.",
                              "description": "Determines if the application can have the ability to un-
block the card.",
                              "default": false
                        },
                        "retainSessionData": {
                              "type": "boolean",
                              "title": "RetainSessionData schema.",
                              "description": "Determines if application's session data should be
maintained between application selection.",
                              "default": false
```

 © 2017 MAOSCO Limited.

MULTOS is a registered trademark of MULTOS Limited.

```
                        },
                        "maintainSelection": {
                              "type": "boolean",
                              "title": "MaintainSelection schema.",
                              "description": "Determines if all select commands are routed to this
application if currently selected.",
                              "default": false
                        },
                        "processEvents": {
                              "type": "boolean",
                              "title": "ProcessEvents schema.",
                              "description": "Determines if an application should be executed in
particular events.",
                              "default": false
                        },
                        "cardManagerApplication": {
                              "type": "boolean",
                              "title": "CardManagerApplication schema.",
                              "description": "Determines if an application is a card manager application
which implements a specific application lifecycle functionality operating on behalf of the card's
issuer",
                              "default": false
                        },
                        "pinAccess": {
                              "type": "string",
                              "enum": [
                                    "Own",
                                    "GlobalBasic",
                                    "GlobalStandard",
                                    "GlobalFull"
                              ],
                              "title": "PinAccess schema.",
                              "description": "Determines what level of access an application has to the
pin object.",
                              "default": "Own"
                        },
                        "peripheralAccess": {
                              "type": "boolean",
                              "title": "PeripheralAccess schema.",
                              "description": "Determines if an application should have access to off-chip
peripherals.",
                              "default": false
                        }
                  },
                  "additionalProperties": false
            },
            "codeHash": {
                  "type": "string",
                  "pattern": "(^[0-9a-fA-F]{40}$)|(^[0-9a-fA-F]{64}$)",
                  "title": "CodeHash schema.",
                  "description": "The digest of the application code segment (hexadecimal string)."
            }
      },
      "required": [
            "applicationId",
            "description",
            "codeSize",
```


MULTOS is registered trademark of MULTOS Limited.

```
            "dataSize",
            "sessionSize",
            "dirSize",
            "fciSize",
            "codeHash"
    ]
}
```

 © 2017 MAOSCO Limited.
MULTOS is a registered trademark of MULTOS Limited.

5.1.1.2 Example


```
{
  "applicationId": "A0000000038010",
  "description": "Test Application",
  "codeSize": 1024,
  "dataSize": 256,
  "sessionSize": 128,
  "dirSize": 128,
  "fciSize": 128,
  "historicalBytes": {
         "primaryAtr": true,
         "secondaryAtr": false,
         "ats": false
   },
  "aluType": {
         "signed": true,
         "encrypted": true
   },
   "fileModeType": {
         "applicationType": "Normal",
         "dualFci": false,
         "memoryAllocationInBlocks": false,
         "proprietaryLoad": true,
   },
  "accessList": {
         "strongCryptography": true,
         "contactInterface": true,
         "contactlessInterface": false,
         "gsmAuthenticate": false,
         "cardBlock": false,
         "cardUnblock": false,
         "retainSessionData": false,
         "maintainSelection": true,
         "processEvents": true,
         "cardManagerApplication": true,
         "peripheralAccess": false,
         "pinAccess": "Own"
   },
   "codeHash": "5BA93C9DB0CFF93F52B521D7420E43F6EDA2784F"
}
```


MULTOS is registered trademark of MULTOS Limited.

5.1.2 XML Format

Application definition files using the XML format must have the file extension .xml.

5.1.2.1 Schema

The schema definition is as follows:

```
<?xml version="1.0" encoding="UTF-8" ?>
<xs:schema version="1.1" attributeFormDefault="qualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="applicationDefinitionFile">
    <xs:complexType>
      <xs:annotation>
        <xs:documentation>Used to define an application whhich can be used for application
registeration.</xs:documentation>
      </xs:annotation>
      <xs:all>
        <xs:element name="applicationId">
          <xs:simpleType>
            <xs:annotation>
              <xs:documentation>The Application ID (hexadecimal string).</xs:documentation>
            </xs:annotation>
            <xs:restriction base="xs:string">
              <xs:pattern value="([0-9a-fA-F]{2}){1,16}"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:element>
        <xs:element name="description">
          <xs:simpleType>
            <xs:annotation>
              <xs:documentation>The application description.</xs:documentation>
            </xs:annotation>
            <xs:restriction base="xs:string">
              <xs:minLength value="1"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:element>
        <xs:element name="codeSize">
          <xs:simpleType>
            <xs:annotation>
              <xs:documentation>The application code size in decimal.</xs:documentation>
            </xs:annotation>
            <xs:restriction base="xs:integer">
              <xs:minInclusive value="0"/>
              <xs:maxInclusive value="65535"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:element>
        <xs:element name="dataSize">
          <xs:simpleType>
            <xs:annotation>
              <xs:documentation>The application data size in decimal.</xs:documentation>
```

 © 2017 MAOSCO Limited.

MULTOS is a registered trademark of MULTOS Limited.

```
            </xs:annotation>
            <xs:restriction base="xs:integer">
              <xs:minInclusive value="0"/>
              <xs:maxInclusive value="65535"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:element>
        <xs:element name="sessionSize">
          <xs:simpleType>
            <xs:annotation>
              <xs:documentation>The application session data size in decimal.</xs:documentation>
            </xs:annotation>
            <xs:restriction base="xs:integer">
              <xs:minInclusive value="0"/>
              <xs:maxInclusive value="65535"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:element>
        <xs:element name="dirSize">
          <xs:simpleType>
            <xs:annotation>
              <xs:documentation>The application DIR data size in decimal.</xs:documentation>
            </xs:annotation>
            <xs:restriction base="xs:integer">
              <xs:minInclusive value="0"/>
              <xs:maxInclusive value="65535"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:element>
        <xs:element name="fciSize">
          <xs:simpleType>
            <xs:annotation>
              <xs:documentation>The application FCI data size in decimal.</xs:documentation>
            </xs:annotation>
            <xs:restriction base="xs:integer">
              <xs:minInclusive value="0"/>
              <xs:maxInclusive value="65535"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:element>
        <xs:element name="historicalBytes" minOccurs="0">
          <xs:complexType>
            <xs:all>
              <xs:element type="xs:boolean" name="primaryAtr" default="false" minOccurs="0">
                <xs:annotation>
                  <xs:documentation>The application has control over the historical bytes for the
primary ATR.</xs:documentation>
                </xs:annotation>
              </xs:element>
              <xs:element type="xs:boolean" name="secondaryAtr" default="false" minOccurs="0">
                <xs:annotation>
                  <xs:documentation>The application has control over the historical bytes for the
secondary ATR.</xs:documentation>
                </xs:annotation>
              </xs:element>
```


MULTOS is registered trademark of MULTOS Limited.

```
              <xs:element type="xs:boolean" name="ats" default="false" minOccurs="0">
                <xs:annotation>
                  <xs:documentation>The application has control over the historical bytes for the
ATS.</xs:documentation>
                </xs:annotation>
              </xs:element>
            </xs:all>
          </xs:complexType>
        </xs:element>
        <xs:element name="aluType" minOccurs="0">
          <xs:complexType>
            <xs:all>
              <xs:element type="xs:boolean" name="signed" default="false" minOccurs="0">
                <xs:annotation>
                  <xs:documentation>Indicates whether the application is signed.</xs:documentation>
                </xs:annotation>
              </xs:element>
              <xs:element type="xs:boolean" name="encrypted" default="false" minOccurs="0">
                <xs:annotation>
                  <xs:documentation>Indicates whether the application is encrypted.</xs:documentation>
                </xs:annotation>
              </xs:element>
            </xs:all>
          </xs:complexType>
        </xs:element>
        <xs:element name="fileModeType" minOccurs="0">
          <xs:complexType>
            <xs:all>
              <xs:element name="applicationType" default="Normal" minOccurs="0">
                <xs:simpleType>
                  <xs:annotation>
                    <xs:documentation>Indidicates the type of application.</xs:documentation>
                  </xs:annotation>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="Normal"/>
                    <xs:enumeration value="Default"/>
                    <xs:enumeration value="Shell"/>
                    <xs:enumeration value="Proprietary"/>
                  </xs:restriction>
                </xs:simpleType>
              </xs:element>
              <xs:element type="xs:boolean" name="dualFci" default="false" minOccurs="0">
                <xs:annotation>
                  <xs:documentation>Indidates whether the application has contains a dual fci. If
false then it is assumed the application contains a single FCI.</xs:documentation>
                </xs:annotation>
              </xs:element>
              <xs:element type="xs:boolean" name="memoryAllocationInBlocks" default="false"
minOccurs="0">
                <xs:annotation>
                  <xs:documentation>Indicates whether the application's data size is in multiple of
255 byte blocks. If false, then the data size is to be interpreted in bytes.</xs:documentation>
                </xs:annotation>
              </xs:element>
              <xs:element type="xs:boolean" name="proprietaryLoad" default="false" minOccurs="0">
```

 © 2017 MAOSCO Limited.

MULTOS is a registered trademark of MULTOS Limited.

```
                <xs:annotation>
                  <xs:documentation>Determines if an application should be loaded in proprietary
defined way.</xs:documentation>
                </xs:annotation>
              </xs:element>
            </xs:all>
          </xs:complexType>
        </xs:element>
        <xs:element name="accessList" minOccurs="0">
          <xs:complexType>
            <xs:all>
              <xs:element type="xs:boolean" name="strongCryptography" default="false" minOccurs="0">
                <xs:annotation>
                  <xs:documentation>Determines if the application uses strong
cryptography.</xs:documentation>
                </xs:annotation>
              </xs:element>
              <xs:element type="xs:boolean" name="contactInterface" default="false" minOccurs="0">
                <xs:annotation>
                  <xs:documentation>Determines if the application can be executed over the contact
interface.</xs:documentation>
                </xs:annotation>
              </xs:element>
              <xs:element type="xs:boolean" name="contactlessInterface" default="false" minOccurs="0">
                <xs:annotation>
                  <xs:documentation>Determines if the application can be executed over the contactless
interface.</xs:documentation>
                </xs:annotation>
              </xs:element>
              <xs:element type="xs:boolean" name="gsmAuthenticate" default="false" minOccurs="0">
                <xs:annotation>
                  <xs:documentation>Determines if the application supports the GSM Authenticate
protocol.</xs:documentation>
                </xs:annotation>
              </xs:element>
              <xs:element type="xs:boolean" name="cardBlock" default="false" minOccurs="0">
                <xs:annotation>
                  <xs:documentation>Determines if the application can have the ability to block the
card.</xs:documentation>
                </xs:annotation>
              </xs:element>
              <xs:element type="xs:boolean" name="cardUnblock" default="false" minOccurs="0">
                <xs:annotation>
                  <xs:documentation>Determines if the application can have the ability to un-block the
card.</xs:documentation>
                </xs:annotation>
              </xs:element>
              <xs:element type="xs:boolean" name="retainSessionData" default="false" minOccurs="0">
                <xs:annotation>
                  <xs:documentation>Determines if application's session data should be maintained
between application selection.</xs:documentation>
                </xs:annotation>
              </xs:element>
              <xs:element type="xs:boolean" name="maintainSelection" default="false" minOccurs="0">
                <xs:annotation>
                  <xs:documentation>Determines if all select commands are routed to this application
if currently selected.</xs:documentation>
                </xs:annotation>
```


MULTOS is registered trademark of MULTOS Limited.

```
              </xs:element>
              <xs:element type="xs:boolean" name="processEvents" default="false" minOccurs="0">
                <xs:annotation>
                  <xs:documentation>Determines if an application should be executed in particular
events.</xs:documentation>
                </xs:annotation>
              </xs:element>
              <xs:element type="xs:boolean" name="cardManagerApplication" default="false"
minOccurs="0">
                <xs:annotation>
                  <xs:documentation>Determines if an application is a card manager application which
implements a specific application lifecycle functionality
                    operating on behalf of the card's issuer</xs:documentation>
                </xs:annotation>
              </xs:element>
              <xs:element type="xs:boolean" name="peripheralAccess" default="false" minOccurs="0">
                <xs:annotation>
                  <xs:documentation>Determines if an application should have access to off-chip
peripherals.</xs:documentation>
                </xs:annotation>
              </xs:element>
              <xs:element name="pinAccess" default="Own" minOccurs="0">
                <xs:simpleType>
                  <xs:annotation>
                    <xs:documentation>Determines what level of access an application has to the pin
object.</xs:documentation>
                  </xs:annotation>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="Own"/>
                    <xs:enumeration value="GlobalBasic"/>
                    <xs:enumeration value="GlobalStandard"/>
                    <xs:enumeration value="GlobalFull"/>
                  </xs:restriction>
                </xs:simpleType>
              </xs:element>
            </xs:all>
          </xs:complexType>
        </xs:element>
        <xs:element name="codeHash">
          <xs:simpleType>
            <xs:annotation>
              <xs:documentation>The digest of the application code segment (hexadecimal
string).</xs:documentation>
            </xs:annotation>
            <xs:restriction base="xs:string">
              <xs:pattern value="(^[0-9a-fA-F]{40}$)|(^[0-9a-fA-F]{64}$)"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:element>
      </xs:all>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

 © 2017 MAOSCO Limited.

MULTOS is a registered trademark of MULTOS Limited.

5.1.2.2 Example

```
<?xml version="1.0" encoding="UTF-8" ?>
<applicationDefinitionFile>
  <applicationId>A0000000038010</applicationId>
  <description>Test Application</description>
  <codeSize>1024</codeSize>
  <dataSize>256</dataSize>
  <sessionSize>128</sessionSize>
  <dirSize>128</dirSize>
  <fciSize>128</fciSize>
  <historicalBytes>
    <primaryAtr>true</primaryAtr>
    <secondaryAtr>false</secondaryAtr>
    <ats>false</ats>
  </historicalBytes>
  <aluType>
    <signed>true</signed>
    <encrypted>true</encrypted>
  </aluType>
  <fileModeType>
    <applicationType>Normal</applicationType>
    <dualFci>false</dualFci>
    <memoryAllocationInBlocks>false</memoryAllocationInBlocks>
    <proprietaryLoad>true</proprietaryLoad>
  </fileModeType>
  <accessList>
    <strongCryptography>true</strongCryptography>
    <contactInterface>true</contactInterface>
    <contactlessInterface>false</contactlessInterface>
    <gsmAuthenticate>false</gsmAuthenticate>
    <cardBlock>false</cardBlock>
    <cardUnblock>false</cardUnblock>
    <retainSessionData>false</retainSessionData>
    <maintainSelection>true</maintainSelection>
    <processEvents>true</processEvents>
   <cardManagerApplication>true</cardManagerApplication>
    <peripheralAccess>false</peripheralAccess>
    <pinAccess>Own</pinAccess>
  </accessList>
  <codeHash>5BA93C9DB0CFF93F52B521D7420E43F6EDA2784F</codeHash>
</applicationDefinitionFile>
```


MULTOS is registered trademark of MULTOS Limited.

5.2 CSV Format

The CSV format is a legacy format and it is important to note that this format will may not support new MULTOS features. For new feature support it recommended to use JSON or XML formats.

Application definition files using the CSV may have the following file extensions:

- .adf
- .aif
- .dat

This format conists of comma separated values in the following order:

0. <application id - hex>,
1. <description - text>,
2. <code size - decimal>,
3. <data size - decimal>,
4. <session size - decimal>,
5. <DIR size - decimal>,
6. <FCI size - decimal>,
7. <ATR setting – 'N' (for no ATR effect) , or any combination of: 'P' (for primary), 'A' (for alternate i.e. secondary), or 'T' (for ATS)>,
8. <shell mode – 'Y' (for shell) , or 'N' (for a MULTOS app)>, or 'D' (for a default app)
9. <signed app – 'Y' (for signed) or 'N' (for non signed)>,
10. <encrypted app – 'Y' (for encrypted) or 'N' (for clear)>,
11. <strong crypto – 'Y' (for strong crypto required), or 'N' (for not required)>,
12. <code hash - hash>,
13. <comms interface required – 'C' (for contact only), 'L' (for contactless only), or 'B' (for both)>,
14. <GSM – 'Y' to authenticate to GSM network, or 'N'>,
15. <card blocking – 'B' for block, and/or 'U' for unblocking, or 'N' for neither>,
16. <retain session – 'Y' to retain session until reset, or 'N'>,
17. <maintain selection – 'Y' or 'N'>,
18. <Dual FCI – 'Y' or 'N'>,
19. <memory allocation – 'Y' or 'N'>
20. <PIN Access – '0' (zero, for no access), '1' (for basic access), '2' (for standard access), or '3' (for full access).

Note that there should not be any line-breaks between parameters; they should all be in one long line. They have been shown split for clarity.

An example would be :

```
A0000000634B45592D47454E,KPKIKG001C,21,546,1,32,32,n,n,y,n,y,ED7015F0160FB8C6C5EA9CEA62E6FDF8D7EF12CB,C
```

 © 2017 MAOSCO Limited.

MULTOS is a registered trademark of MULTOS Limited.

6 Enablement Response File

6.1 Enablement Data List File

Data	Definition
File_Type_Code	ASCII, 4 characters. Set to "MSML"
File_Protection_Method_ID	Binary, 1 byte. Set to 0x01
File_Structure_Method_ID	Binary, 1 byte. Set to 0x02
Reserved	ASCII, 10 characters
Date	Date, 4 bytes
Time	Time, 3 bytes
Reserved	ASCII, 8 characters
Header_Record	
{ **Enablement_Data_List_Record** }	Occurs Number_Of_Enablement_Data_List_Records times. Entries are not sorted into any particular order
Hash_Code	Binary, 20 bytes. A SHA-1 hash of the complete header record and enablement data records

6.2 Header Record

Data	Definition
Issuer_ID	Binary, 4 bytes
Reserved	Binary, 1 byte. Set to value 0x01
MCD_Issuer_Product_ID	Binary, 1 byte
Bureau_ID	Binary, 4 bytes
Enablement_Data_Record_Size	Binary, 2 bytes. The size in bytes of each Enablement Data entry
MKD_PK_C_Size	Binary, 2 bytes. The size in bytes of each card public key certificate
Number_Of_Enablement_Data_List_Records	Binary, 4 bytes. This is the number of entries in the subsequent list

MULTOS is registered trademark of MULTOS Limited.

6.3 Enablement Data List Record

Data	Definition
MCD_ID	Binary, 6 bytes
Enablement_Data_Record	Binary, Enablement_Data_Record_Size bytes. The enablement record for the corresponding MCD_ID
MKD_PK_C_Record	

6.4 MKD PK C Record

Data	Definition
Internal data	Binary, 11 bytes
MKD_Cert_Method_ID	Binary, 2 bytes
MKD_Hash_Method_ID	Binary, 2 bytes
Internal data	Binary, 11 bytes
MCD_Issuer_Product_ID	Binary, 1 byte
Issuer_ID	Binary, 4 bytes
Enablement_Data_Date	Binary, 1 byte
MCD_Number	Binary, 8 bytes
Internal data	Binary, remaining bytes

7 ALC Response File

7.1 Load Certificate File Format

Note that the ALC response files contain fields which are conditional on the type of device being targeted.

Data	Definition
File_Type_Code	ASCII, 4 characters. Set to "ALCR"
File_Protection_Method_ID	Binary, 1 byte. Set to 0x02
File_Structure_Method_ID	Binary, 1 byte. Set to 0x03
Reserved	ASCII, 10 characters

 © 2017 MAOSCO Limited.

MULTOS is a registered trademark of MULTOS Limited.

Data	Definition
Date	Date, 4 bytes
Time	Time, 3 bytes
Reserved	ASCII, 8 characters
ALC_Response_Record	
Hash_Code	Binary, 20 bytes. A SHA-1 hash of the ALC_Response_Record

7.2 ALC Response Record

Data	Definition
ALC_Record_Length	Binary, 2 bytes. The length of the ALC record
ALC_Record	ALC data
Reserved	Binary, 2 bytes. This field takes value 0x0000

7.3 ALC Record

Data	Definition
ALC_ID_Length	Binary, 2 bytes. The length of the following ID
ALC_ID	Binary, ALC_ID_Length bytes (always 8 bytes at present)
Rom_Identifier	Binary, 2 bytes
Pad_Length	Binary, 1 byte. Length of subsequent padding
Padding	Binary, Pad_Length bytes
ALC_DATA	Binary, ALC_Length bytes

7.4 ALC_DATA

Data	Definition
ALC_Length	Binary, 2 bytes. The length of this actual ALC_DATA record, including these length bytes
Internal data	Binary, 9 bytes
Cert_Method_ID	Binary, 2 bytes
Hash_Method_ID	Binary, 2 bytes
Public_Key_Length	Binary, 2 bytes. The length of the key being certified

MULTOS is registered trademark of MULTOS Limited.

Data	Definition
Certifying_Key_Length	Binary, 2 bytes. The length of the certifying key
Internal data	Binary, 7 bytes
App_Permissions	Binary, 76 bytes
Internal data	Binary, 18 bytes
Application_ID_Field	Binary, 17 bytes
Random_Seed	Binary, 8 bytes
File_Mode_Type	Binary, 1 byte
Code_Size	Binary, 2 bytes
Data_Size	Binary, 2 bytes
Session_Data_Size	Binary, 2 bytes
DIR_File_Record_Size	Binary, 2 bytes
FCI_Record_Size	Binary, 2 bytes
App_ATR_Type	Binary, 1 byte
Verify_Certificate_Flag	Binary, 1 byte
Verify_KTU_Flag	Binary, 1 byte
Access_List	Binary, 2 bytes
Application_Code_Hash_Length	Binary, 1 byte. The length of the following hash
Application_Code_Hash	Binary, Application_Code_Hash_Length bytes
Key_Certificate	Binary, variable bytes. The certified key

8 ADC Response File

8.1 Delete Certificate File Format

Note that the ADC response files contain fields which are conditional on the type of device being targeted.

Data	Definition
File_Type_Code	ASCII, 4 characters. Set to "ADCR"
File_Protection_Method_ID	Binary, 1 byte. Set to 0x02
File_Structure_Method_ID	Binary, 1 byte. Set to 0x03
Reserved	ASCII, 10 characters
Date	Date, 4 bytes

 © 2017 MAOSCO Limited.

MULTOS is a registered trademark of MULTOS Limited.

Data	Definition
Time	Time, 3 bytes
Reserved	ASCII, 8 characters
ADC_Response_Record	
Hash_Code	Binary, 20 bytes. A SHA-1 hash of the ADC_Response_Record

8.2 ADC Response Record

Data	Definition
ADC_Record_Length	Binary, 2 bytes. The length of the ADC record
ADC_Record	ADC data
Reserved	Binary, 2 bytes. This field takes value 0x0000

8.3 ADC Record

Data	Definition
ADC_ID_Length	Binary, 2 bytes
ADC_ID	Binary, ADC_ID_Length bytes
ROM_Identifier	Binary, 2 bytes
Pad_Length	Binary, 1 byte. Length of subsequent padding
Padding	Binary, Pad_Length bytes
ADC_DATA	

8.4 ADC_DATA

Data	Definition
ADC_Length	Binary, 2 bytes. The length of this actual ADC_DATA record, including these length bytes
Internal data	Binary, 9 bytes
Cert_Method_ID	Binary, 2 bytes
Hash_Method_ID	Binary, 2 bytes
Public_Key_Length	Binary, 2 bytes. The length of the key being certified

MULTOS is registered trademark of MULTOS Limited.

Data	Definition
Certifying_Key_Length	Binary, 2 bytes. The length of the certifying key
Internal data	Binary, 7 bytes
App_Permissions	Binary, 76 bytes
Internal data	Binary, 18 bytes
Application_ID_Field	Binary, 17 bytes
Random_Seed	Binary, 8 bytes
Internal data	Binary, remaining bytes. The meaning of this data is irrelevant to this document

9 TKCK File

9.1 TKCK File Format

This is required by an Application Provider when generating encrypted ALUs, to allow the verification of the mkd_pk_c. It is provided by a MULTOS KMA.

These files will always be distributed with a filename of the form:

'tkckxxxx.key'

where 'xxxx' represents the MKD_Cert_Method_ID.

Data	Definition
File_Type_Code	ASCII, 4 characters. Set to "TKCK"
File_Protection_Method_ID	Binary, 1 byte. Set to 0x01
File_Structure_Method_ID	Binary, 1 byte. Set to 0x01
Consignment_File_ID	ASCII, 8 characters. Set to 'TKCK', followed by 4 characters presenting the identifier (in hex). This will be the same as the *MKD_Cert_Method_ID*
Date	Date, 4 bytes
Time	Time, 3 bytes
MKD_Cert_Method_ID	Binary, 2 bytes
Key_Length	Binary, 2 bytes
Key_Data	Binary, Key_Length bytes. The actual TKCK public key
Hash_Code	Binary, 20 bytes. A SHA-1 hash of the *MKD_Cert_Method_ID*, Key_Length and Key_Data

 © 2017 MAOSCO Limited.

MULTOS is a registered trademark of MULTOS Limited.

10 Hash Modulus File

10.1 Hash Modulus File Format

This is required by an Application Provider when generating application signatures. It is provided by a MULTOS KMA.

These files will always be distributed with a filename of the form:

'hashxxxx.mhm'

where 'xxxx' represents the Hash_Method_ID.

Data	Definition
File_Type_Code	ASCII, 4 characters. Set to "HASH"
File_Protection_Method_ID	Binary, 1 byte. Set to 0x01
File_Structure_Method_ID	Binary, 1 byte. Set to 0x01
Consignment_File_ID	ASCII, 8 characters. Set to 'HASH', followed by 4 characters presenting the identifier (in hex). This will be the same as the *Hash_Method_ID*. For example 'HASH0105'
Date	Date, 4 bytes
Time	Time, 3 bytes
Hash_Method_ID	Binary, 2 bytes
Key_Length	Binary, 2 bytes
Key_Data	Binary, Key_Length bytes. The actual Hash Modulus
Hash_Code	Binary, 20 bytes. A SHA-1 hash of the *Hash_Method_ID*, Key_Length and Key_Data

11 Additional MULTOS Data

11.1 Additional MULTOS Data File format

Data	Definition
File_Type_Code	ASCII, 4 characters. Set to "ADMD"
File_Protection_Method_ID	Binary, 1 byte. Set to 0x01

MULTOS is registered trademark of MULTOS Limited.

Data	Definition
File_Structure_Method_ID	Binary, 1 byte. Set to 0x01
Consignment_File_ID	ASCII, 8 characters
Date	Date, 4 bytes
Time	Time, 3 bytes
Hash_Code	Binary, 20 bytes. A SHA-1 hash of the complete MULTOS_Data_Record
MULTOS_Data_Record	

11.2 MULTOS Data Record

Data	Definition
Data_Length	Binary, 2 bytes. The length of the following data
Data_Image	Binary, Data_Length bytes. A binary image

12 DATA DICTIONARY

Type	Definition	Description
Access_List	Binary, 2 bytes	List of bit fields used to define MULTOS features such as access to cryptographic primitives
ADC_ID	Binary, 8 bytes	An identifier for an ADC
ADC_ID_Length	Binary, 1 byte	The length of an ADC_ID, currently always set to 8
ALC_ID	Binary, 8 bytes	An identifier for an ALC
ALC_ID_Length	Binary, 1 byte	The length of an ALC_ID, currently always set to 8
App_ATR_Type	Binary, 1 byte	Set to 0x41 for App_ATR Set to 0x00 for no App_ATR Set to 0x42 for Alt_App_ATR
Application_Code_Hash	Binary, variable	A hash over the application code space
Application_Code_ Hash_Length	Binary, 1 byte	Either 0x14 for SHA-1, or 0x00 for no hash
Application_ID	Binary, 16 bytes	The Application ID for an Issuer's application as defined in ISO/IEC 7816-5 (padded with 0xff if required)

 © 2017 MAOSCO Limited.
MULTOS is a registered trademark of MULTOS Limited.

Type	Definition	Description
Application_ID_Field	Binary, 17 bytes	Comprised of : 1 byte indicating how many bytes of the Application_ID are significant + *Application_ID*
App_Permissions	Binary, 76 bytes	*MCD_Issuer_Product_IDs* + *Issuer_ID* + *Enablement_Data_Dates* + *MCD_Number*
Bureau_ID	Binary, 4 bytes	Identifies a Bureau as the sender of a request for enablement data
Cert_Method_ID	Binary, 2 bytes	Used to match an ALC or ADC against a ROM mask in an MCD, to ensure correct algorithms and keys are applied
Code_Size	Binary, 2 bytes	The amount of code space an application needs on a MULTOS chip, as detailed in the Application Load Certificate
Data_Size	Binary, 2 bytes	The amount of data space an application needs on a MULTOS chip, as detailed in the Application Load Certificate
Date	Binary, 4 bytes year (2 bytes) + month (1 byte, 1..12) + day (1 byte, 1..31)	Note that data is stored big-endian, so that the year 1997 (0x07CD), would be stored as a byte of value 07 followed by a byte of value CD. Please note that these items are binary NOT BCD. 31st December 1997 would be coded in Hexadecimal as **07 CD 0C 1F**
DIR_File_Record_Size	Binary, 2 bytes	The length of the entry in the EF_{DIR} file for this application
Enablement_Data_ Date	Binary, 1 byte	The date on which MSM Controls were generated. This is an offset in months from January 1998 (= 0). Hence controls generated in September 1999 for example would have a date of 20 (decimal).
Enablement_Data_ Dates	Binary, 32 bytes	A 256 bit field of flags corresponding to each of the possible 256 possible *Enablement_Data_Date* values
FCI_Record_Size	Binary, 2 bytes	The number of bytes to be returned when an application is selected by a terminal
File_Mode_Type	Binary, 1 byte	An identifier for the type of application. A value of 0x5A defines a 'Shell' application. A value of 0xA5 defines a 'Default' application. A value of 0x00 defines a standard application
File_Protection_ Method_ID	Binary, 1 byte	Identifier for method used to protect the file. Meaning is in context of file type
File_Structure_Method_ ID	Binary, 1 byte	Identifier for how data is structured within the file. Its meaning is in context of file type
File_Type_Code	ASCII, no terminator, 4 bytes	Defines file type as defined in section 2
Hash_Code	Binary, 20 bytes	A SHA-1 hash as defined in FIPS PUB 180-1

MULTOS is registered trademark of MULTOS Limited.

Type	Definition	Description
Hash_Method_ID	Binary, 2 bytes	Used in an ALC or ADC to compare against the value in the ROM mask of an MCD to verify that the correct Hash Modulus is in use
IC_Manufacturer_ID	Binary, 1 byte	Used to identify the manufacturer of the silicon chip. A current list of possible identifiers can be requested from MAOSCO or MULTOS Customer Support
IC_Type	Binary, 1 byte	Used to identify a particular mask of a silicon chip. A current list of possible identifiers can be requested from MAOSCO or MULTOS Customer Support
Issuer_ID	Binary, 4 bytes	The MCD Issuer Id, assigned by a KMA
Key_Certificate	Binary, variable	An actual MULTOS enablement, load or delete certificate
MCD_ID	Binary, 6 bytes	The identifier for an MCD, assigned during MCD manufacture
MCD_Issuer_Product_ID	Binary, 1 byte	The product ID to be assigned to this set of MCDs, denoting the subclass of the Issuer's card base
MCD_Issuer_Product_ IDs	Binary, 32 bytes	A 256 bit field of flags corresponding to each of the possible 256 *MCD_Issuer_Product_ID* values
MCD_Number	Binary, 8 bytes	Unique reference for a card assigned by KMA in enablement data
MKD_Cert_Method_ID	Binary, 2 bytes	Used to match a TKCK against an MCD when generating encrypted ALUs
MKD_PK_C	Binary, variable	Card public key certificate. Sent with MSM data
Modulus	Binary, variable	An RSA modulus used with an exponent (either specified explicitly or implicitly assumed to be of value 3 depending on context) used to sign or encrypt data
Padding	Binary, variable	Optional padding of zero or more bytes of a fixed value of 0x55
Random_Seed	Binary, 8 bytes	Used to implement a history list within the card
ROM_Identifier	Binary, 2 bytes	An identifier for a ROM mask
Session_Data_Size	Binary, 2 bytes	The amount of session data space an application needs on a MULTOS chip, as detailed in the Application Load Certificate
Time	Binary, 3 bytes hour (1 byte, 0..23) + minute (1 byte, 0..59) + second (1 byte, 0..59)	Note that values are stored in binary, so 42 seconds past half ten in the evening would be 22:30:42 on a 24 hour clock and would be coded as **16 1E 2A**

 © 2017 MAOSCO Limited.

MULTOS is a registered trademark of MULTOS Limited.

Type	Definition	Description
Verify_Certificate_Flag	Binary, 1 byte	Flag used to denote whether an ALU signature is present or not Set to 0x4E for not present Set to 0x50 for present
Verify_KTU_Flag	Binary, 1 byte	Flag used to denote whether an ALU KTU is present or not Set to 0x4E for not present Set to 0x50 for present

--end of document--

MULTOS is registered trademark of MULTOS Limited.