

MACHINE READABLE TRAVEL DOCUMENTS

(Logo)

Guide to Interfacing e-MRTDs and Inspection Systems

Version – **1.0**

Date - February 14, 2005

Published by authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Guide to Interfacing e-MRTDs and Inspection Systems

Release : 1.0

Date : February 14, 2005

Release Control

Release	Date	Description
0.1	17-12-2004	First draft
0.2	05-01-2005	German comments incorporated; draft for Berlin meeting
0.3	11-01-2005	Discussion Berlin meeting
0.4	17-01-2005	Results Berlin meeting & additional contributions incorporated
0.5	31-01-2005	Input, comments from email and Essen group incorporated
0.6	08-02-2005	Final draft, additions Michael Hegenbarth to be accepted, section 5 first part to be rephrased
1.0	14-02-2005	Issue 1.0 of the Guide

Guide to Interfacing e-MRTDs and Inspection Systems

Release : 1.0

Date : February 14, 2005

Table of contents

1. INTRODUCTION	4
1.1 PRE-REQUISITES.....	4
1.1.1 <i>e-MRTD Interoperability Test Tools</i>	5
1.1.2 <i>Reader Interoperability Test Tools</i>	5
1.1.3 <i>Technical Testing</i>	5
1.1.4 <i>Scenario and Operational Testing</i>	5
1.2 TERMINOLOGY.....	5
1.2.1 <i>Report terminology</i>	5
1.2.2 <i>Abbreviations</i>	6
1.3 REFERENCE DOCUMENTATION	6
2. KEY FUNCTIONAL SPECIFICATIONS TABLE.....	7
3. E-MRTD KEY FUNCTIONALITIES	8
3.1 FUNCTIONALITIES	8
3.2 E-MRTD TEST FACILITY	10
3.2.1 <i>Reference Reader Hardware (Informative)</i>	10
3.2.2 <i>Reference Software Tool</i>	10
4. INSPECTION SYSTEM KEY FUNCTIONALITIES	13
4.1 FUNCTIONALITIES	13
4.2 E-MRTD REFERENCE SET	16
5. TECHNICAL TESTING	17
6. SCENARIO AND OPERATIONAL TESTING	18

Guide to Interfacing e-MRTDs and Inspection Systems

Release : 1.0

Date : February 14, 2005

1. Introduction

In 2004, three Technical Reports, concerning the global interoperable implementation of biometrics in Machine Readable Travel Documents have been endorsed by ICAO:

[R1], *Technical Report: Development of a Logical Data Structure – LDS for optional capacity expansion technologies, Version 1.7, May 18 2004.*

[R2], *Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, October 01 2004.*

[R3], *Technical Report: Biometrics Deployment for Machine Readable Travel Documents, Version 2 (draft 2), May 5 2004.*

Interoperability tests carried out in Canberra (AUS), Morgantown (USA) and Sidney (AUS), and the Mock Port of Entry test conducted in Baltimore-Washington International Airport (BWI) were held to confirm the progress of the reader manufacturers towards achieving global interoperability for reading of e-MRTDs, based on the specifications set out in the published Technical Reports.

The results of these tests were considered at the ICAO TAG-NTWG meeting in Auckland in December 2004. NTWG concluded that global interoperability for reading of e-MRTDs has not yet been achieved, especially the necessary functionalities of inspection (border clearance) systems, in order to support the variety of options that can occur in e-MRTDs, proved to be implemented insufficiently.

NTWG decided that an elaboration of the specifications in the form of a Guide would accelerate the realization of global interoperability for reading of e-MRTDs. This Guide would clarify the specifications contained in the existing Technical Reports to,

- Allow Issuing Authorities to better determine how well their prototype e-MRTDs meet the defined specifications;
- Allow reader manufacturers to independently confirm that their readers meet all mandatory specifications; *and*
- Allow Inspection (Control) Authorities wishing to carry out scenario and/or operational tests to quickly identify those e-MRTDs and Inspection Systems that meet the minimum functional specifications and can be included in the tests.

This Guide reflects the document envisaged by NTWG and as such, describes the approach, supporting minimum functional specifications and tools created to allow Issuing Authorities, reader manufacturers and Inspection Authorities to accelerate the realization of global interoperability for reading of e-MRTDs.

1.1 Pre-requisites

This Guide SHALL be read in combination with the ICAO Technical Reports and Supplement—9303. Should the contents of this Guide contradict any specifications contained in the Technical Reports or the Supplement—9303 the Technical Reports, respectively the Supplement supersedes.

To assist the three stakeholders a **Set of Reference Tools** has been created based on the specifications set out in the Technical Reports. This Set of Reference Tools embodies the following five components:

1. A restatement of the minimum functional specifications defined for both the e-MRTD and the Inspection System that are critical to achieving global interoperability;

Guide to Interfacing e-MRTDs and Inspection Systems

Release : 1.0

Date : February 14, 2005

2. A standardized "test set of e-MRTDs with specially created ICAO compliant sample implementations" to allow the functionality required for Inspection Systems to be evaluated and confirmed. The intention is to create a version of the test set that could be acquired for independent testing any of the stakeholders.

In the near term access to the test set will be controlled given the security implications and the availability of test samples. It will be available at an e-MRTD and Reader Test Facility operated by the Japanese Ministry of Economy, Trade and Industry and at controlled tests organized by various Member States or groups of Member States.;

3. A set of readers to allow Issuing Authorities and Inspection Authorities to successfully evaluate and confirm the functionality required in the e-MRTD;
4. A Software Tool to allow Issuing Authorities and Inspection Authorities to evaluate and confirm successful global interoperability of both e-MRTDs and Readers; *and*
5. A Software Tool to allow reader manufacturers (with a PC/SC capability) to evaluate and confirm successful global interoperability of their Reader(s).

1.1.1 e-MRTD Interoperability Test Tools

Based on the table in Section 2, Section 3 of this Guide summarizes the key functional specifications set out in the Technical Reports that must be met by the e-MRTD to achieve global interoperability for reading details from the Contactless IC Chip. It further describes tools that have been created to allow Issuing Authorities and Inspection Authorities to evaluate and confirm proper operation of an e-MRTD; specifically reference hardware (the "Golden Reader" hardware) and reference software (the "Golden Reader Tool – GRT").

1.1.2 Reader Interoperability Test Tools

Based on the table in Section 2, Section 4 of this Guide summarizes the key functional specifications set out in the Technical Reports that must be met by the Inspection System to achieve global interoperability for reading e-MRTDs. It further describes two tools that have been created to allow Issuing Authorities, Inspection Authorities and reader vendors to evaluate and confirm proper operation of the Reader; specifically the "Representative e-MRTD Test Set" and the "Golden Reader Software".

1.1.3 Technical Testing

Section 5 of this Guide describes how the e-MRTD and Reader Test tools can be used by Issuing Authorities, reader manufacturers and Inspection Authorities to carry out detailed technical testing to assess and confirm compliance with the specifications set out in the Technical Reports.

1.1.4 Scenario and Operational Testing

Section 6 of this Guide describes how the e-MRTD and Reader Test tools can be used by Issuing Authorities to carry out scenario and/or operation testing. Special attention has been paid to supporting testing in which a collection of largely untested e-MRTDs and Inspection Systems are brought together to assess the operational considerations of using e-MRTDs and Inspection Systems within the border inspection process.

1.2 Terminology

1.2.1 Report terminology

- Where this Guide uses the term 'Inspection System' this refers to the combination of Hardware and Software, used to retrieve information from the e-MRTD. In this definition an Inspection System typically consists of Reader Hardware, Low Level (communications)

Guide to Interfacing e-MRTDs and Inspection Systems

Release : 1.0

Date : February 14, 2005

Software, High level (application) Software. The Inspection System takes care of powering the chip, communicating with the chip at 14443 as well as 7816 level, ICAO specified security features, retrieving LDS data groups. This Guide does not assume certain technical implementations of such an Inspection System (e.g. which functionality is covered in which system component).

- The key words "MUST", "SHALL", "REQUIRED", "SHOULD", "RECOMMENDED", and "MAY" in this Guide are to be interpreted as described in [R5], *RFC 2119, S. Bradner, "Key Words for use in RFCs to indicate Requirement Levels", BCP 14, March 1997.*

1.2.2 Abbreviations

Abbreviation	
APDU	Application Protocol Data Unit
BAC	Basic Access Control
BLOB	Binary Large Object
CA	Certification Authority
CRL	Certificate Revocation List
CSCA	Country Signing CA
DG	Data Group
DO	Data Object
DS	Document Signer
ECDSA	Elliptic Curve Digital Signature Algorithm
ICAO	International Civil Aviation Organization
ICC	Integrated Circuit Card
IFD	InterFace Device
LDS	Logical Data Structure
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
NTWG	New Technologies Working Group
PKD	Public Key Directory
PKI	Public Key Infrastructure
RF	Radio Frequency
SHA	Secure Hash Algorithm
SM	Secure Messaging
TAG	Technical Advisory Group

1.3 Reference documentation

The following documentation serves as reference in this Report and should be referenced for development of chip enabled MRTDs and Inspection System Applications:

- [R1] *Technical Report: Development of a Logical Data Structure – LDS for optional capacity expansion technologies, Version 1.7, May 18 2004*
- [R2] *Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, October 01 2004*
- [R3] *Technical Report: Biometrics Deployment for Machine Readable Travel Documents, Version 2 (draft 2), May 5 2004*
- [R4] *Supplement—9303, Version 2004-2, December 19 2004*
- [R5] *RFC 2119, S. Bradner, "Key Words for use in RFCs to indicate Requirement Levels", BCP 14, March 1997.*
- [R6] *REF_EPassportAPI Design, Version 1.0*

Guide to Interfacing e-MRTDs and Inspection Systems

Release : 1.0

Date : February 14, 2005

2. Key Functional Specifications Table

The ICAO specifications provide various options for Issuing Authorities. As a consequence a variety of MRTD styles will be offered to Inspection Systems. The table below lists these varieties. The table serves as a reference in the following sections on e-MRTD Key Functionalities (see Section 3) and Inspection System Key Functionalities (see Section 4).

ICAO specifications for Machine Readable Travel Documents												
Mandatory								Options				
Power ²	14443 ¹	7816-4 ⁹	EF / DGs ³	Image ⁴	Auth ⁵	Alg ⁶	SHA ⁷	7816-4 ⁹	DGs ³	Auth ⁵	Access ⁸	
1,5 – 7,5 A/m	A	SELECT	DG1 EF_COM									
		READ BINARY	DG2	JPEG								
				JPEG2K								
									EXTERNAL AUTHENTICATE	DG15	Active	
									INTERNAL AUTHENTICATE			
									GET CHALLENGE			
									MUTUAL AUTHENTICATE			BAC
										DG3-16		
								RSA	1			
									256			
						ECDSA	1					
					Passive		224					
						(DSA)	(384)					
							(512)					
1,5 – 7,5 A/m	B	SELECT	DG1 EF_COM									
		READ BINARY	DG2	JPEG								
				JPEG2K								
									EXTERNAL AUTHENTICATE	DG15	Active	
									INTERNAL AUTHENTICATE			
									GET CHALLENGE			
									MUTUAL AUTHENTICATE			BAC
										DG3-16		
								RSA	1			
									256			
						ECDSA	1					
					Passive		224					
						(DSA)	(384)					
							(512)					

3. e-MRTD Key Functionalities

3.1 Functionalities

General functional requirements, derived from the Technical Reports and to be supported by e-MRTDs, are:

Memory.

- Issuer accessible memory SHALL be secure (factory lockable and issuer lockable), programmable and non-volatile.
- The offered IC SHALL have a minimum of 32 KiloBytes (KB) of memory available for Government discretionary use.
- The memory SHALL support random access data retrieval of data elements of LDS. IC supports independent selection of EFs.

Logical Data Structure.

- IC/Operating System MUST support writing of an ICAO standard LDS to the IC.
- IC/Operating System MUST support reading back and verifying an ICAO standard LDS.

Security.

- The IC/Operating System SHALL provide means against unauthorized writing.
- It is RECOMMENDED to use ICs/OS that are successfully certified/validated to a suitable Common Criteria Protection Profile with EAL 4+ SOF-High.
- An eventual e-MRTD shielding SHALL NOT prevent simultaneous reading of data page and IC chip on an integrated reader.

Speed.

IC/antenna assembly MUST support 106 kbps (to be compatible with ISO 14443) but SHALL also support the higher bit rate of 424 kbps (in compliance with ISO/IEC 14443-2/Amendment 2 and ISO/IEC 14443-3/Amendment 1). Support of even higher rates such as 848 kbps is highly desirable.

The required functionalities below refer to the corresponding columns in the table in Section 2.

¹ *Communication protocols.*

Ref: [R3], *Technical Report: Biometrics Deployment for Machine Readable Travel Documents, Version 2 (draft 2), May 5 2004, Annex I, Section 2.3.3.*

The e-MRTD chip SHALL support either the ISO/IEC 14443-A or the ISO/IEC 14443-B protocol.

IC SHALL respond to commands via ISO/IEC 14443-4 Section 7 “Half-duplex block transmission protocol” and “ANNEX B(Informative) Protocol scenarios”.

The IC/antenna assembly, when integrated, SHALL meet the tolerance limits for exposure to the various electromagnetic, physical, mechanical effects, etc., as described in ISO/IEC 14443-1.

As eMRTDs are required to be in compliance with ISO/IEC 14443, they are consequentially required to be in compliance with ISO/IEC 14443-3/Amendment 3 and ISO/IEC 14443-4/Amendment 1. As a further consequence they shall pass those test methods which are strictly related to the complete series of ISO/IEC 14443, laid down in ISO/IEC 10373-6 plus associated amendments 1 through 5.

² *Field strength*

Ref: [R3], *Technical Report: Biometrics Deployment for Machine Readable Travel Documents, Version 2 (draft 2), May 5 2004, Annex K, Issue K.03.*

The e-MRTD chip SHALL operate within field strengths from 1,5 A/m – 7,5 A/m.

At the present prototype stage, some MRTDs will contain chips that require a minimum of 4 A/m to execute the required functions. This does in no way express any intention to loosen the burden on

Guide to Interfacing e-MRTDs and Inspection Systems

Release : 1.0

Date : February 14, 2005

chip manufacturers to meet the requirements set by the standards. States SHALL ensure that all MRTDs issued to their population will conform to the standards in any respect.

The IC chip SHALL be capable of being read within a range of 0 cm – 2 cm from the reader casing.

³ **Data Groups**

Ref: [R1], *Technical Report: Development of a Logical Data Structure – LDS for optional capacity expansion technologies, Version 1.7, May 18 2004*, Section V.

The use of Data Groups 1 (MRZ) and 2 (Encoded Face) is MANDATORY for MRTDs.

Data Groups 3-16 are OPTIONAL.

Requirements for using these Data Groups depend on the demands of Issuing States.

The presence of EF.COM is MANDATORY.

⁴ **Image Format**

Ref: [R3], *Technical Report: Biometrics Deployment for Machine Readable Travel Documents, Version 2 (draft 2), May 5 2004*, Annex D, Section 5.1.

The facial image SHALL be stored either in JPEG or in JPEG2000 format. The way these image formats MUST be stored in DG2 is specified in Ref: [R1], *Technical Report: Development of a Logical Data Structure – LDS for optional capacity expansion technologies, Version 1.7, May 18 2004*.

The Face biometric data interchange image recorded in DG2 SHALL be derived from the passport photo used to create the Displayed Portrait printed on the Data Page of the eMRP; and SHALL be encoded either according to type 2 (full frontal image) or type 3 (token image) formats set out in the latest version of ISO CD 19794-5. DG2 SHALL contain either a type 2 or type 3 face biometric data interchange format image or both as determined at the discretion of the Issuing State. Where a type 2 image is included, the eye positions MAY also be included along with type 2 image using an optional feature point data block set out in ISO CD 19794-5.

⁵ **Data Authentication**

Ref: [R2], *Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, October 01 2004*, Section 2.6.

Passive Authentication is MANDATORY. This means that the Document Security Object (EF.SOD) MUST be present in the e-MRTD. OPTIONALLY the SO_D contains the Document Signer Certificate (C_{DS}).

Active Authentication is OPTIONAL. The support of this option on the e-MRTD depends on the demands of Issuing State(s).

⁶ **Crypto algorithms**

Ref: [R2], *Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, October 01 2004*, Section 3.3.

These three algorithms are allowed. Since DSA does not allow keys >1024 bit, at this moment the use of DSA is not feasible.

RFC 3447 specifies two signature mechanisms, RSASSA-PSS and RSASSA-PKCS1_v15. It is RECOMMENDED to generate signatures according to RSASSA-PSS, but receiving States MUST also be prepared to verify signatures according to RSASSA-PKCS1_v15.

Those Issuing States implementing the ECDSA algorithm for signature generation or verification SHALL use ANSI X 9.62.

[R4], *Supplement—9303, Version 2004-2, December 19 2004, Issue S1.0-20041220-PKI0013* states: "States MUST use the same algorithms for use in their CSCA, DS Keys and where applicable Active Authentication Key Pairs."

⁷ **Hashing algorithms**

Ref: [R2], *Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, October 01 2004*, Section 3.3.

These hashing algorithms are permitted in MRTDs. At present no hashing algorithms above 256 bits hash length are feasible.

Guide to Interfacing e-MRTDs and Inspection Systems

Release : 1.0

Date : February 14, 2005

⁸ Access Methods

Ref: [R2], *Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, October 01 2004*, Section 2.6.

Basic Access Control is OPTIONAL for MRTDs, its use is at the discretion of the Issuing State.

⁹ ISO/IEC 7816-4

The command parameters that are mandatory and optional are specified in Appendix 2 to Annex A of [R1], *Technical Report: Development of a Logical Data Structure – LDS for optional capacity expansion technologies, Version 1.7, May 18 2004*. All commands, formats, and their return codes are defined in ISO/IEC 7816-4. Please refer to normative Appendix 2 to this Annex for examples of use of these commands.

The minimum command set, to be supported by e-MRTDs, consists of:

SELECT

READ BINARY

Appendix 2 also describes the command option for accessing files with length greater than 32,767 bytes.

Ref: [R2], *Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, October 01 2004*

In support of the specified options Basic Access Control and Active Authentication the following additional commands are OPTIONAL:

EXTERNAL AUTHENTICATE

INTERNAL AUTHENTICATE

GET CHALLENGE

MUTUAL AUTHENTICATE

3.2 e-MRTD Test Facility

To enable producers of e-MRTDs as well as Inspection System vendors to effectively develop and test, an e-MRTD test facility has been defined. This test facility serves as a reference to establish if e-MRTDs comply to the functionalities, described in section 3.1.

The test set consists of Reference Reader Hardware and a Reference Software Tool.

3.2.1 Reference Reader Hardware (Informative)

The reference reader serves as reference for compliance with ISO/IEC 14443 Type A and B. It is suitable to test on the hardware and lower layer software level. Since the reference readers not always guarantee the full range of compliancy on 14443/10373-6, it should be regarded as a tool for checking e-MRTD application which on certain subsets of 14443.

Type A.

The ISO/IEC 14443 Type A reference reader is the Philips Pegoda MF RD 700.

Type B.

The ISO/IEC 14443 Type B reference reader is the NMDA Tx-PR-400 ('x' stands for 'S', 'M' or 'L', indicating different antenna sizes).

There is a standard implementation guideline on lower software level such as "Proximity Communication Interface Implementation Specifications For e-Passports Version1.0" which is provided by NMDA for the Type B reference reader.

In the future, contact points to obtain NMDA 'Reference Reader Hardware' will be listed.

3.2.2 Reference Software Tool

The Golden Reader software Tool (GRT) serves as reference interoperability test tool for compliance with the ICAO specifications, described in [R1], *Technical Report: Development of a Logical Data Structure – LDS for optional capacity expansion technologies, Version 1.7, May 18 2004* and [R2], *Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access*,

Guide to Interfacing e-MRTDs and Inspection Systems

Release : 1.0

Date : February 14, 2005

Version 1.1, October 01 2004. It is suitable to test on the higher layer software (application) level. An e-MRTD, read and accepted by the golden reader software can be considered to be compliant to these standards.

An e-MRTD, read and accepted by the golden reader software, can be considered to be compliant to these standards.

The GRT is a collaborative effort, established by the “Essen Group“ and maintained by the Federal Office for Information Security (BSI) of Germany in co-operation with Secunet Security Networks AG¹.

The GRT **Reading Test** of sample passports includes:

- Reading of ICAO compliant e-Passports according to ICAO LDS TR v1.7 and PKI TR v1.1
- Reading all mandatory data groups (EF.COM, EF.DG1, EF.DG2 and EF.SOD)
- Support of the following security features:
 - Passive Authentication (mandatory) based on RSA and ECDSA signatures as mentioned in the PKI TR v1.1
 - Basic Access Control (optional) as in PKI TR v1.1
- Additional functionality for testing
 - Time measurement
 - Extended logging
 - Display of UID, ATR and ATS
- Binary LDS files can be imported or exported to test their ICAO compliance

Supported readers

The GRT supports three categories of RF Readers:

- PC/SC-Readers (PC/SC Version 1.1), for instance
 - SCM SCR 331-DI (Type A+B)
 - ACG RFID (Type A+B)
 - Inside Contactless (Type A+B)
 - other PC/SC readers
- Specially integrated readers (native integration into GRT)
 - Philips PEGODA (Type A)
 - Integrated Engineering SmartID (Type A+B)
 - NMDA Tx-PR-400 (Type B only)
- Readers with an ePassportAPI V1.0 compliant interface

ePassportAPI

An essential part of NTWG and ISO/WG3 activities to assist globally interoperable implementations of Inspection Systems and ePassports is the development of an ePassportAPI.

This ePassport-API features:

- Hierarchical respective layered software architecture
- well defined functional modules (Soft- and/or Hardware)
- Detailed technical requirements can be specified for each functional module
- Each module can be mapped to components of a real world system
- Well defined communication interfaces
- allows for easy exchange of functional modules (e.g. top-level application, crypto library, SmartCard reader etc.) as well as for future conformance testing of separate components

The reader layer of the ePassport API will allow reader hardware manufacturers, which are not already PC/SC compatible or which are not specially integrated as the Pegoda or NMDA-reference reader, to connect to the GRT testing software for high level testing.

¹ The GRT can be obtained for non-commercial use only from markus.ernst@bsi.bund.de .

Guide to Interfacing e-MRTDs and Inspection Systems

Release : 1.0

Date : February 14, 2005

For an overview, see [R6], *REF_EPassportAPI Design, Version 1.0*. The complete framework is published in the ePassportAPI SDK available from 9 February 2005. The SDK will contain additional detailed documentation, example source codes and workspaces for Visual Studio.NET 2003 to allow development of ePassportAPI compliant modules.



Screenshot of the GRTV2.0, based on the ePassportAPI V1.0 (available Feb 9th, 2005)

4. Inspection System Key Functionalities

4.1 Functionalities

Inspection System functionalities are listed below. Some of these functionalities are directly derived from the specifications in the Technical Reports. With respect to the obligation to support these functionalities the appropriate terminology IN CAPITALS (see [R5], *RFC 2119*, S. Bradner, “Key Words for use in RFCs to indicate Requirement Levels”, BCP 14, March 1997.) is used.

More general recommendations for Inspection System Design are also listed, without using the formal terminology in capitals.

Physical

- The reader SHALL be capable of accepting ICAO 9303 TD-3 size documents.
- The reader SHALL be capable of accepting ICAO 9303 TD-1 and TG-2 size documents.
- The reader should be capable of accepting oversize passports (page size 9 cm. x 14 cm).
- The reader solution SHALL be capable of reading the OCRB-MRZ on both new e-Passports and e-visas and existing passports and other MRTDs.
- It is recommended that the reader design enables correct placement of the e-Passport to read the ISO 14443 contactless chip without requiring re-positioning of the e-Passport in both open and closed book configurations to accommodate eMRP design.
- Use of the reader should not require knowledge of reader antenna location.
- The reader should be able to read the properly placed open passport without manual intervention by the operator.
- It is recommended that the reader provides visible indication of power and status (e.g., off-line, ready, processing).
- The integrated reader must have the capability to export both the biographic data retrieved from the OCR-B MRZ and the biographic data retrieved from the contactless IC chip on the e-Passport.

Security

- The reader should be designed to inhibit eavesdropping of communications between the reader and the contactless IC chip from a distance greater than 1 meter from the reader.
- The reader should be designed to inhibit jamming of reader operations from a distance of 30 centimeters from the reader.

Machine Readable Zone

- The Inspection System should be able to retrieve the MRZ and re-initiate a failed contactless chip messaging session without a separate action to re-read the MRZ.
- The integrated reader² shall have the capability to export the MRZ for comparison and correction when a failure is encountered opening an e-Passport with BAC.
- The reader shall support the capability to correct the MRZ, when a failure is encountered opening an e-passport with BAC.
- The reader shall support the capability to open the e-Passport chip once the MRZ data has been corrected for BAC-protected e-Passports.

Speed

- The reader SHALL operate within the maximum following target times:
 - Reader initialization < 2 seconds.
 - Retrieval of data from chip in < 2.5 seconds for 32k of data < 5 seconds for 64k of data.
 - Recycle time: < 3 seconds.
 - Polling/Interaction response < 2 seconds from placement of chip on reader.

² The term “integrated reader” refers to peripheral devices capable of capturing both MRZ data and IC chip data using the same device.

Guide to Interfacing e-MRTDs and Inspection Systems

Release : 1.0

Date : February 14, 2005

The required functionalities below refer to the corresponding columns in the table in Section 2.

¹ **Communication protocols.**

Ref: [R3], *Technical Report: Biometrics Deployment for Machine Readable Travel Documents, Version 2 (draft 2), May 5 2004, Annex I, Section 2.3.3.*

Both communication protocols ISO/IEC 14443-A and ISO/IEC 14443-B MUST be supported by the Inspection System.

The reader SHALL be capable of reading ISO 14443 contactless chips regardless of chip location or orientation to the data page in e-Passports.

The reader SHOULD conform to the (Draft) PC/SC standard for contactless chips.

The reader SHALL support anti collision processes identified in ISO 14443.

² **Field strength**

Ref: [R3], *Technical Report: Biometrics Deployment for Machine Readable Travel Documents, Version 2 (draft 2), May 5 2004, Annex K, Issue K.03.*

The e-MRTD chip SHALL operate into field with field strengths from 1,5 A/m – 7,5 A/m.

Reader manufacturers need to be aware that, at the present prototype stage, some MRTDs will contain chips that require a minimum of 4 A/m to execute the required functions. Therefore it is expected that readers submitted for testing will be able to cope with such limitations. This does in no way express any intention to loosen the burden on chip manufacturers to meet the requirements set by the standards.

The reader's antenna(s) SHOULD be designed to prevent interference with other electronic devices within 30 centimeters.

The reader SHOULD be designed to prevent the capture of IC chip data by the reader from a distance greater than 10 centimeters.

³ **Data Groups**

Ref: [R1], *Technical Report: Development of a Logical Data Structure – LDS for optional capacity expansion technologies, Version 1.7, May 18 2004, Section V.*

The use of Data Groups 1 (MRZ) and 2 (Encoded Face) is MANDATORY for MRTDs. The Inspection System MUST be able to retrieve these Data Groups.

Data Groups 3-16 are OPTIONAL. Requirements for Inspection Systems concerning these Data Groups depend on the demands of 'receiving' States.

⁴ **Image Format**

Ref: [R3], *Technical Report: Biometrics Deployment for Machine Readable Travel Documents, Version 2 (draft 2), May 5 2004, Annex D, Section 5.1.*

The facial image can be stored in JPEG or in JPEG2000 format. The Inspection System MUST be able to retrieve both JPEG and JPEG2000 images from DG2.

⁵ **Data Authentication**

Ref: [R2], *Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, October 01 2004, Section 2.6.*

Passive Authentication is MANDATORY. This means that the Inspection System MUST be able to verify the authenticity and integrity of the LDS, using the Document Security Object and its digital signature.

Active Authentication is OPTIONAL. Requirements for Inspection Systems concerning these Data Groups depend on the demands of 'receiving' States.

Guide to Interfacing e-MRTDs and Inspection Systems

Release : 1.0

Date : February 14, 2005

⁶ *Crypto algorithms*

Ref: [R2], *Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, October 01 2004*, Section 3.3.

These three algorithms are allowed. Since DSA does not allow keys >1024 bit, at this moment the use of DSA is not feasible. Therefore at present both RSA and ECDSA MUST be supported by the Inspection System.

RFC 3447 specifies two signature mechanisms, RSASSA-PSS and RSASSA-PKCS1_v15. It is RECOMMENDED to generate signatures according to RSASSA-PSS, but Receiving States MUST also be prepared to verify signatures according to RSASSA-PKCS1_v15.

[R4], *Supplement—9303, Version 2004-2, December 19 2004, Issue S1.0-20041220-PKI0013* states: "States MUST use the same algorithms for use in their CSCA, DS Keys and where applicable Active Authentication Key Pairs."

⁷ *Hashing algorithms*

Ref: [R2], *Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, October 01 2004*, Section 3.3.

These hashing algorithms are permitted in MRTDs. At present no hashing algorithms above 256 are feasible. Therefore at present hashing algorithms SHA_1, SHA_224 and SHA_256 MUST be supported by the Inspection System.

⁸ *Access Methods*

Ref: [R2], *Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, October 01 2004*, Section 2.6.

Basic Access Control is OPTIONAL for MRTDs, its use is at the discretion of the Issuing State.

However, Inspection Systems SHOULD support Basic Access Control to be able to obtain access to BAC equipped MRTDs. Requirements for Inspection Systems concerning Basic Access Control (such as MRZ reading and fall-back) depend on the demands of Receiving States.

⁹ *ISO/IEC 7816-4*

The command parameters that are mandatory and optional are specified in Appendix 2 to Annex A of [R1], *Technical Report: Development of a Logical Data Structure – LDS for optional capacity expansion technologies, Version 1.7, May 18 2004*. All commands, formats, and their return codes are defined in ISO/IEC 7816-4. Please refer to normative Appendix 2 to this Annex for examples of use of these commands.

The minimum command set, to be supported by e-MRTDs, consists of:

SELECT
READ BINARY

Appendix 2 also describes the command option for accessing files with length greater than 32,767 bytes.

Ref: [R2], *Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, October 01 2004*

In support of the specified options Basic Access Control and Active Authentication the following additional commands are OPTIONAL:

EXTERNAL AUTHENTICATE
INTERNAL AUTHENTICATE
GET CHALLENGE
MUTUAL AUTHENTICATE

Guide to Interfacing e-MRTDs and Inspection Systems

Release : 1.0

Date : February 14, 2005

4.2 e-MRTD reference set

Based on the above, a set of golden e-MRTDs should cover all the various combinations of mandatory and optional features. A useful set of e-MRTDs for this purpose at this moment consists of eight e-MRTDs. An Inspection System, being able to read, interpret and verify the complete golden e-MRTD set is considered to be compliant to the standards.

Constitution of the golden e-MRTD set:

GeP_A1: 14443 type A. DG1, DG2, DG15. DG2 - JPEG RSA with SHA_1 Active Authentication	GeP_B1: 14443 type B. DG1, DG2, DG15. DG2 - JPEG RSA-PSS with SHA_1 Active Authentication
GeP_A2: 14443 type A. DG1, DG2. DG2 - JPEG RSA with SHA_256	GeP_B2: 14443 type B. DG1, DG2. DG2 - JPEG RSA-PSS with SHA_256 Basic Access Control
GeP_A3: 14443 type A. DG1, DG2. DG2 – JPEG ECDSA with SHA_1 Basic Access Control	GeP_B3: 14443 type B. DG1, DG2. DG2 – JPEG ECDSA with SHA_1
GeP_A4: 14443 type A. DG1, DG2, DG15. DG2 – JPEG2000 RSA with SHA_1 Active Authentication Basic Access Control	GeP_B4: 14443 type B. DG1, DG2, DG15. DG2 – JPEG2000 RSA with SHA_1 Active Authentication Basic Access Control

The Document Signer Certificates in all reference documents are stored on the chip

5. Technical Testing

The **Global Interoperability Test Kit** enables the need for immediate and detailed technical testing of both e-MRTDs and Inspection Systems by Issuing and Inspection Authorities.

It equally provides a means for reader vendors to carry out the critical independent testing to ensure that they can provide devices that meet the required specifications to Authorities conducting scenario and operational testing.

Detailed technical testing is supported in two ways,

For the period through the end on 2006 Issuing Authorities, reader manufacturers and Inspection Authorities can take advantage of the e-MRTD and Reader Test Facility operated by the Japanese Ministry of Economy, Trade and Industry in Tokyo. Controlled access to the standardized Representative Test Set of e-MRTDs is provided for a fee as well as temporary access to facilities in which to conduct individual technical tests. Details on how to arrange technical testing at the Japanese Ministry of Economy, Trade and Industry can be found at <http://www.epassport-test.org/>.

In the future a representative Test Set of e-MRTDs can be acquired by any stakeholder wishing to carry out independent detailed technical tests.

6. Scenario and Operational Testing

The **Global Interoperability Test Kit** has been conceived recognizing the urgent need of Inspection Authorities to carry out scenario and full operational testing of e-MRTDs and Inspection Systems, not to mention machine assisted identity confirmation, within the border inspection process.

The e-MRTD and Reader Interoperability Test Tools described in Sections 2 and 3 respectively and the high level approach defined in Section 4 ensure Issuing Authorities can carry out detailed technical assessments of both e-MRTDs and Inspection Systems if they wish or derive detailed insight from separate tests before they embark on scenario and/or full operational testing of an e-MRTD Inspection System.

The Test Tools equally provide a means of quickly testing a collection of largely untested e-MRTDs and Inspection Systems to assess their compliance with the specifications set out in the Technical Reports and their fitness for supporting tests designed to evaluate operational considerations of a border inspection process enhanced through the use of the e-MRTD, Inspection Systems and machine assisted identity confirmation technology.

Using the e-MRTD and Reader test tools, inspecting organizations will be able to develop scenario and operational tests validating the following key e-MRTD Inspection System functionalities:

- Feedback on success or failure results of passive and active authentication.
- Passive authentication if the document's public key is not stored on the chip.
- Passive authentication using the public key if it is stored on the chip.
- Access external sources, e.g., the ICAO public key directory, to retrieve public key(s) and verify the e-Passport chip data.
- Verify the authenticity of the Document Signer Certificate using the Country Signing CA Public Key.
- Validate the ICAO Object Identifier (OID) in the certificate stored on the chip is OID component value 136.
- Provide selectable options to activate or de-activate the Active Authentication or Extended Access Control process.
- Parse the data retrieved from the MRZ.
- Correct an MRZ with external input (e.g., from a keyboard).
- Validate OCR-B font, character spacing of MRZ text, line spacing between MRZ lines, skew of MRZ lines, margins of MRZ lines, and check digits.
- Initiate sequential chip access that automatically performs the BAC protocol on the e-Passport chip if open access fails.
- Parse the second line of the MRZ to generate a key to unlock the e-Passport contactless chip for BAC.

Guide to Interfacing e-MRTDs and Inspection Systems

Release : 1.0

Date : February 14, 2005

- Retrieve the MRZ and re-initiate a failed contactless chip messaging session without a separate action to re-read the MRZ.
- Provide notification of failure to open the chip using BAC.
- Attempt to re-establish a session with an ISO 14443 contactless chip if the transaction has not successfully completed. Once a transaction has completed, the Inspection System attempt further read transactions until the chip has been removed from the field and re-presented.
- Provide an indication that a read transaction has completed and the passport may be removed from the reader.
- Provide an operational indicator of a failure to access the chip.
- Provide the capability to cancel a transaction that fails to read an e-Passport chip and initiate a new session with a new chip.