Use of Contactless Integrated Circuits In Machine Readable Travel Documents

TECHNICAL REPORT

Prepared by Mike Ellis (Australia) WG3 for NTWG

Version 3.1, 16-April-2003

TABLE OF CONTENTS

DOCUMENTATION HISTORY

Date	**Revision**	**Action**
2-Dec-2002	1	Initial Draft
15-Dec-2002	2	Revision following NTWG NZ
15-Apr-2003	3	Revision during WG3 meeting 27, Helsinki
16-Apr-2003	3.1	Revision following WG3 meeting 27, Helsinki

1 Scope

The purpose of this Technical Report is to provide guidance and advice to States and to potential Suppliers regarding the application and use of Contactless Integrated Circuits (contactless ICs) in Machine Readable Travel Documents (MRTDs). This Report will cover each of the issues in relation to the deployment of these contactless ICs. This Report will form the basis of a presentation to ICAO TAG in May 2003 of recommendations for approval as standards in relation to contactless ICs and how these standards are to be incorporated into Document 9303.

In so doing, key considerations are:

- **Globally Interoperability –** the need for specifying how contactless ICs are to be used in a univerally interoperable manner
- **Technical Reliability –** the need for provision of guidelines and parameters to ensure member States deploy proven contactless IC technology; and that States reading data in contactless ICs encoded by other States can ensure accurate reading at their end
- **Practicality –** the need to ensure that recommended standards can be made operational and implemented by States without them having to introduce a plethora of disparate systems and equipment to ensure they meet all possible variations and interpretations of the standards
- **Durability –** that the systems introduced will last the maximum 10 year life of a travel document

2 Introduction

2.1 STRUCTURE OF THIS REPORT

This report contains two main parts. The first main part is a "Primer" (Section 3) which contains a general description of the technology of contactless ICs. It is not intended to be exhaustive or too complex, and has been intentionally restricted to the contactless ICs to be recommended for use in MRTDs.

The second main part of the Report discusses the Application of contactless ICs to MRTDs (Section 4).

2.2 CONTACTLESS ICS TO BE USED IN MRTDS

For reasons outlined below, contactless ICs to be used in MRTDs are to be those that conform to one of the following ISO Standards:

- ISO/IEC 14443 (proximity)
- ISO/IEC 15693 (vicinity)

2.3 REASONS FOR SELECTING STANDARDS ISO/IEC 14443 AND ISO/IEC 15693

2.3.1 Global Interoperability

Contactless ICs operate at Radio Frequencies (RF). There are many different RF bands used, however the RF band defined in ISO/IEC 14443 and ISO/IEC 15693 is available worldwide. The use of ISO standards also avoids proprietary issues.

2.3.2 Different Border Inspection Methods

It is evident that there are requirements for two different border inspection methods. "Staffed" inspection requires the holder to surrender the MRTD to a border official for inspection and processing. "Proximity" cards specified in ISO/IEC 14443 meet this application. "Self-service" inspection requires the holder to simply carry the MRTD through a gate where the contactless IC will be interogated for data, leading to automated permission or denial of entry or exit. "Proximity" cards can meet this application, or "vicinity" cards as specified in ISO/IEC 15693, depending upon the design of the application.

2.3.3 The Machine (RF) Reader of Contactless ICs

There are becoming available machine (RF) readers that will read contactless ICs conforming to ISO/IEC 14443 and ISO/IEC 15693. Thus a state or issuing organization may issue an MRTD containing a contactless IC conforming to ISO/IEC 14443 and only install machine (RF) readers to read the same. Alternatively, they may install machine (RF) readers to read all contactless ICs conforming to ISO/IEC 14443 and ISO/IEC 15693 to achieve global interoperability.

2.3.4 Durability

There are now estimated to be in excess of 100 million contactless ICs in circulation which conform to the ISO standards. The inherent durability of the contactless ICs specified here is not in question. However durability in the MRTD application needs to be investigated in terms of embossing, flexing or stamping the MRTD.

2.3.5 Reading of Multiple Documents

The ISO standards contain anti-collision procedures that under normal circumstances will overcome problems associated with reading multiple documents within the active range of the machine (RF) reader. Physical interference between the antenna of adjacent contactless ICs in an MRTD may occur, especially if the antenna is the same size and spatial matched. In this case the booklet (if the MRTD is an MRP) must be opened to the page where the contactless IC is placed in order to eliminate the interference and facilitate reading.

2.3.6 Logical Data Structure

Contactless ICs conforming to ISO/IEC 14443 and ISO/IEC 15693 have sufficient data storage to encode the Logical Data Structure (LDS). The LDS should be encoded by the random-access method.

2.3.7 Biometrics

Contactless ICs conforming to ISO/IEC 14443 have sufficient data storage to encode biometric images and templates within the LDS. Contactless ICs conforming to ISO/IEC 15693 may not have sufficient data storage to encode biometric images and templates within the LDS, nor may the transmission speed be high enough to transfer these images and templates in a reasonable time. However, contactless ICs conforming to ISO/IEC 15693 are useful for MRVs, and may access an external biometric database.

2.3.8 Inclusion in MRTDs

Contactless ICs conforming to ISO/IEC 14443 and ISO/IEC 15693 are usually incorporated in ID-1 size documents. Thus there is no impediment to their use in TD-1 size MRTDs. These contactless ICs may also be produced in a variety of forms which are suitable for placement (by glue, lamination, encapsulation, etc) in other sizes of MRTDs such as MRPs and MRVs. It is recommended that the contactless ICs and antennas placed in MRPs conform in size to the ID-1 so that reading compatibility is preserved.

3 Primer

3.1 INTRODUCTION

The MRZ, with its OCR-B characters printed according to DOC 9303, is the basic storage medium of the MRTD. However with the demand for extra data such as biometrics and electronic visas, the MRZ has insufficient data capacity.

ICAO has moved to standardize the use of barcodes for optional capacity expansion, but barcodes unfortunately have relatively low storage capacity and cannot be reprogrammed.

The silicon chip offers the best technical solution and it is already widely used in contact IC cards for varied uses eg bank and telephone cards, commonly referred to as “smartcards”. The main disadvantage with contact smartcards is the mechanical contact used, which is sometimes impractical in MRTD applications and may suffer from failure due to dirt or moisture. Contact smartcards are impractical in the TD-2 and TD-3 sizes used for MRPs and MRVs. ICAO has moved to standardize the use of contact smartcards in MROTDs (TD-1 size).

ICAO has also standardized the use of optical cards. Optical cards also are impractical for the ID-2 and ID-3 sizes and in addition are usually relatively expensive, although they offer vast amounts of data capacity in comparison to the other technologies.

The silicon chip is also used in contactless IC cards that operate at radio frequencies (RF). The contactless IC offers a much more flexible operation with a contactless transfer of data between the smartcard and the machine (RF) reader, a reasonable amount of data capacity, and a relatively low cost. The contactless IC can also be produced in a flexible plastic sheet format, so it can be sandwiched or laminated into the cover or pages of an MRP, or incorporated into an MRV.

3.2 WHAT IS A CONTACTLESS IC SYSTEM?

Contactless IC systems as defined here operate at radio frequencies and are made up of two components:
The *Contactless IC*, which is located in the MRTD,
The *Machine (RF) Reader*, which communicates with the contactless IC, and which may have read or read/write capability. The machine (RF) reader will normally be connected to a computer system.

In the MRTD application the contactless IC is *passive*, that is, it contains no power source of its own (as an *active* contactless IC would). The reason for this is that power sources (batteries) would be unlikely to last for the expected 10-year life of the MRTD.

The machine (RF) reader both provides the power for, and communicates with, the contactless IC by means of radio waves.

The contactless IC consists of a chip and an attached antenna. This structure can take the form of the relatively inflexible construction as used in TD-1 sized cards (MROTDs) or can be printed on a flexible plastic base which can then be incorporated into TD-2 and TD-3 sized documents (MRPs and MRVs). The contactless IC can be initially programmed and then re-programmed which makes it suitable for use in the electronic visa application, and which also offers the facility to modify or cancel an MRTD.

The contactless IC does not need to come into contact with the machine (RF) reader. Contactless ICs can read in seconds in hot, dirty, damp, cold, foggy environments and through material that would be unsuitable for other technologies. It is thought that in the future, improvements in the mass production of contactless ICs will make contactless ICs comparable in price to barcode technology. However unlike bar coding systems contactless ICs can be scanned more than one item at a time which makes it a substantially faster and more convenient technology.

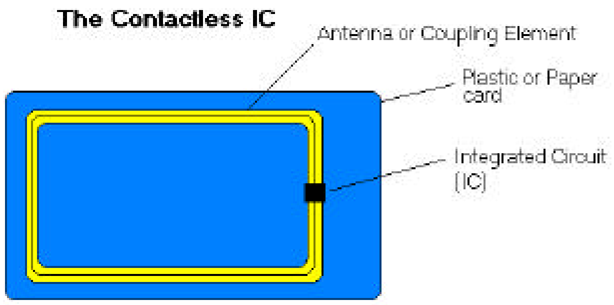
3.3 CONTACTLESS IC COMPONENTS AND BASIC OPERATION

The contactless IC, which is the actual *data carrying part*, normally consists of an *electronic IC* and an *antenna* or coupling element. When the contactless IC is not within the range of a machine (RF) reader it is not powered and so remains inactive. On coming into the range of a machine (RF) reader, the antenna of the contactless IC collects energy by means of *inductive coupling* and the IC becomes active. By means of switching a load resistance in its antenna, the contactless IC can transfer data to the machine (RF) reader by a process known as *load modulation*.

The machine (RF) reader contains a high frequency module for transmitting and receiving, a control module, and an antenna or coupling element to connect to the contactless IC. The machine (RF) reader will also usually have an interface (eg RS-232) to allow it to communicate with a computer system. The machine (RF) reader may be a read only or a read/write device.

3.3.1 The Contactless IC

The inductively coupled contactless IC consists of an electronic data carrying IC and a large area coil that functions as an antenna, also called a coupling element.

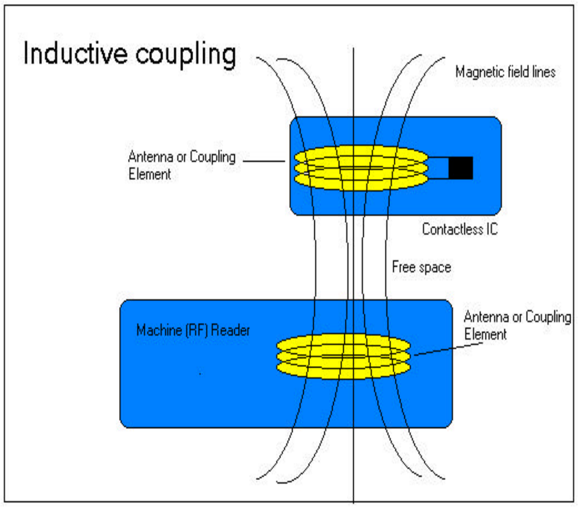


The main part of the contactless IC is a low-power IC that controls the communication with the machine (RF) reader. The IC also contains memory of some type to hold data. There are three types of operation: *Memory*, which is a simple memory device; *Wired Logic*, which contains memory and some simple logic functions such as password protection; and *Microcontroller,* which has memory and more advanced functions for encryption and data partition.

The antenna consists of a few turns of conductive material, typically less than 10. The simplicity of the antenna contributes to the low cost.

3.3.2 Inductive Coupling

The machine (RF) reader provides an inductively coupled contactless IC with energy for its operation. To do this, the machine (RF) reader generates a strong radio frequency electromagnetic field in its antenna. The frequency used for ISO/IEC 14443 and ISO/IEC 15693 devices is 13.56MHz and the corresponding wavelength is 22.1m. This is several times the distance between the machine (RF) reader and the contactless IC (usually less than 1m). Thus in this close region the electromagnetic field can be regarded as a simple magnetic alternating field, as found in transformers. The strength of the electromagnetic field decreases quickly with the distance between the machine (RF) reader and the contactless IC. As the maximum strength of the electromagnetic field generated by the machine (RF) reader is set by regulations, taking into account safety considerations, reading distances of over 1m are not practical.



A part of the electromagnetic field generated by the machine (RF) reader covers the antenna of the contactless IC and induces an AC voltage across it. This AC voltage is converted into DC and is used to charge a capacitor. The charge on the capacitor is used to power the IC.

Connected across the antenna is another capacitor. The value of this capacitance is chosen so that it works with the inductance of the contactless IC antenna to form a parallel resonant circuit. The resonant frequency of this circuit corresponds to the transmitted frequency of the electromagnetic field, and this gives the maximum voltage at the contactless IC.

Data can be transmitted from the machine (RF) reader to the contactless IC by changing one parameter of the transmitted electromagnetic field ie amplitude, frequency or phase.

3.3.3 Load Modulation

The parallel resonant circuit of the contactless IC draws energy from the electromagnetic field generated by the machine (RF) reader. This energy being drawn can be measured at the machine (RF) reader's antenna by monitoring the current being supplied. The contactless IC can switch a load resistor at its antenna which will have the effect of increasing or decreasing the energy being supplied by the machine (RF) reader. This change in energy can be measured by monitoring the current to the machine (RF) reader antenna. If the switching of the contactless IC load resistor represents data, then by this means the contactless IC can transmit data to the machine (RF) reader. This method of transmission is known as *load modulation*.

The contactless IC must switch its load resistor at a lower frequency than that being generated by the machine (RF) reader. This new frequency is called a *subcarrier*. The subcarrier can be modulated to communicate the data by a variety of methods eg ASK, FSK or BPSK.

Both ISO/IEC 14443 and ISO/IEC 15693 compliant contactless ICs use the same inductive coupling method at the same base carrier frequency of 13.56MHz.

3.3.4 Collision Avoidance

It is possible to place more than one contactless IC into the electromagnetic field generated by the machine (RF) reader. In this situation the contactless ICs will be powered together and the response subcarriers generated by them will interfere. To avoid this, collision avoidance schemes are used to ensure that the contactless ICs will respond separately.

3.3.5 Differences between ISO/IEC 14443 Type A and Type B contactless ICs

Type A contactless ICs are generally memory only ICs. The machine (RF) reader uses 100% amplitude modulation of the electromagnetic field for communication from the reader to the IC. That is, to communicate 1's and 0's the electromagnetic field is either on or off. During the time that the field is off, the IC must store enough energy in its internal capacitors to continue functioning.

Type B contactless ICs are generally equipped with a processor IC. The processor consumes more power than a memory IC. Thus 100% amplitude modulation of the electromagnetic field for communication is not practical. Type B uses 10% amplitude modulation so the energy flow is not disrupted. Thus, to communicate 1's and 0's the electromagnetic field switches from 100% to 90% amplitude.

Type A and Type B contactless ICs also have other operating differences, including different collision avoidance schemes. These differences are listed in the tables below (see paragraph 3.8).

3.4 LIMITATIONS ON OPERATION

Water or human tissue does not absorb radio waves at 13.56MHz. Therefore the presence of one or more human beings or parts such as hands, or moisture, in the region between the contactless IC and the machine (RF) reader will have no adverse impact on the operation.

However, the radio waves are sensitive to the presence of metal parts. Encasing the contactless IC in a metal jacket eg aluminium foil, will prevent reading. Care must be taken in the placement of the machine (RF) reader relative to adjacent metal parts.

Because inductive coupling decreases with the sixth order of distance, adjacent systems or other external noise sources are unlikely to adversely affect the reading operation.

3.5 HUMAN SAFETY

Radio frequency waves have the capacity to inflict injury on human beings if the radiation level is too strong. There have been many medical studies into the physiological effects and safety limits have been established.

In testing the safety of the 13.56MHz radio frequency waves used by these systems, there are many standards in place eg

ANSI C95.1:	SAR = 1.6W/kg (averaging 1g mass)
ICNIRP:	SAR = 2.0W/kg (averaging 10g mass)

In these standards the worse case scenario is taken of exposure of the head and trunk of the general public. Manufacturers of contactless ICs complying to ISO/IEC 14443 and ISO/IEC 15693 have verified the basic restriction, the Specific Absorption Rate (SAR). Thus the use of these contactless ICs is safe.

3.6 LEGAL RADIATION LIMITS

Unlike many RF technologies that do not have harmonised international regulations, the 13.56MHz frequency used by contactless ICs complying with ISO/IEC 14443 and ISO/IEC 15693 has international acceptance.

Regulations are set in different countries to limit the strength of the radiation emitted by a machine (RF) reader. This is done to limit the interference between different users of a frequency band, or interference to users of neighbouring bands.

There are some differences between regulations in different countries. The following is a summary of regulations in the US, Japan and Europe:

Carrier:	± 7kHz
US (FCC):	10 000µV/m in 30m
Japan:	1W reader output power, antenna gain <= -30dBi
Europe:	42dBµA/m in 10m

Sidebands:

US(FCC):	30µV/m in 30m
Japan:	500µV/m in 3m
Europe:	9dBµA/m in 10m (carrier ±150kHz)

Both the US and Japanese regulations are more stringent than the European, however it is expected that both the US and Japanese regulations will be harmonized with the European regulations in the future.

3.7 PERFORMANCE

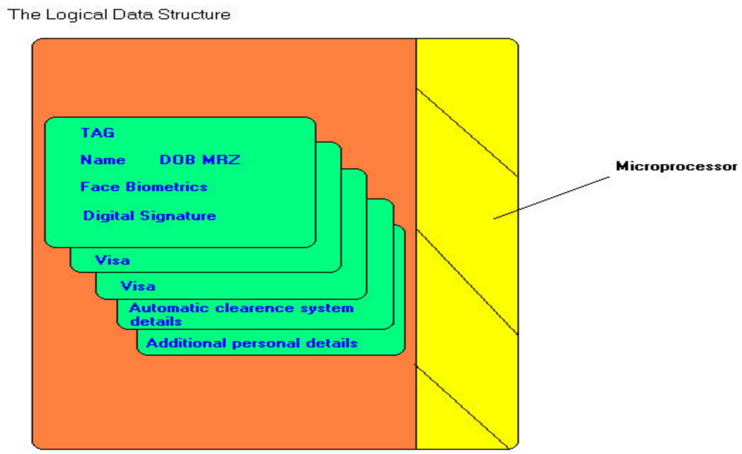
Performance on a RF system depends on many factors and is related to the application. However as applied to MRTDs, the two main performance indicators are functional (memory size, security) and operational (range, communication reliability and speed).

Contactless ICs complying with ISO/IEC 14443 and ISO/IEC 15693 are produced by a large number of silicon manufacturers, and there are also a large number of reader companies and system integrators. Based on 100 million contactless cards sold, this is a mature technology.

3.7.1 Memory Size

For use in MRTDs it is expected that at least 16K bytes will be required to store the biometric and the LDS overhead.

The memory capacity must be considered in relation to the communication speed and the expected read time of the data in the MRTD application.


The Logical Data Structure
TAG
Name DOB MRZ
Face Biometrics
Digital Signature
Visa
Visa
Automatic clearence system details
Additional personal details
Microprocessor

3.7.2 Security

Contactless ICs that are "memory" only have no inherent security protection. The MRTD application must provide the security in the form of the digital signature as specified in the LDS. Both "wired logic" and "microcontroller" devices provide a variety of security levels ranging from passwords to encryption. However as the LDS recommends open structure without any requirement for the encryption function inherent in these devices, their use in MRTDs is not required. However the issuing country may require some private area which is not subject to the LDS constraints, in which case the encryption function may be useful.

3.7.3 Range

Contactless ICs conforming to ISO/IEC 14443 have a reliable range of up to 10cm from the machine (RF) reader. Contactless ICs conforming to ISO/IEC 15693 have a reliable range of approximately 1m.

3.7.4 Communication Reliability

The reliability of the data communication is related to the signal to noise ratio in the RF system. As the contactless IC data signal is transmitted by the subcarrier that is outside the noisy base carrier band, the system performance can be very robust. The reliabilty can be enhanced by designing the machine (RF) reader to be selective and to process subcarriers independently.

3.7.5 Communication Speed

Because of the shorter operating distance and the greater power level available to the contactless IC, devices conforming to ISO/IEC 14443 have a data transfer rate of 106kbps. Faster data transfer rates, unsupported at the moment by the standard, of 847kbps or greater are possible. At the longer operating range ISO/IEC 15693 devices have a data transfer rate of up to 26.6 kbps.

Comparison of Data transfer speed for ISO/IEC 14443

	106kbps	212kbps	424kbps	847kbps	> 847kbps
Type-A	Yes	Proposed*1	Proposed*1	Proposed*1	Proposed*1
Type-B	Yes	Proposed*1	Proposed*1	Proposed*1	Proposed*1
(Read time @ 40kbyte)	3 sec.	1.5 sec.	0.75 sec.	0.4 sec.	

Proposed: New working item, now WD stage.
*1: Will be standardised in 2003.

3.7.6 Durability of Data

Contactless ICs store the data as electrical charge that has the possibility of leaking away and hence the data will be lost. Usually the electrical charge is refreshed through the use of the contactless IC; that is, the passive device is placed in an active field and the charge is refreshed. It has been found that contactless ICs will store their charge for at least ten years at 25ºC, and so will last for the maximum ten-year lifetime of an MRTD. Operating or storage temperatures very different from this may result in a shorter data retention time. Manufacturer’s specifications should be consulted for exact information on data retention.

3.8 SUMMARY OF ISO/IEC 14443 AND ISO/IEC 15693 PARAMETERS

3.8.1 Comparison of ISO/IEC 14443 and ISO/IEC 15693 Parameters

Features	ISO/IEC 14443	ISO/IEC 15693
Standards	ISO/IEC 14443 Type A/B	ISO/IEC 15693
Frequency	13.56MHz	13.56MHz
Read range	Up to 10 cm	Up to 1 m
Chip types supported (at present)	Memory Wired Logic Microcontroller	Memory Wired Logic
Encryption and authentication functions	MIFARE, DES/3DES, AES, RSA, ECC	Supplier specific, DES/3DES
Read/write ability	Read/write	Read/write
Data transfer rate	Up to 106kbps (ISO/IEC) Up to 847kbps (available)	Up to 26.6kbps
Anti-collision	Yes	Yes
Card-to-reader authentication	Challenge/Response	Challenge/Response
Hybrid card capability	Yes	Yes
Contact interface support	Yes	No

3.8.2 ISO/IEC 14443 - Type A - Proximity Contactless ICs

POWER SUPPLY:	13.56 MHz, inductive coupling Allowed field strength: 42 dBµA/m
Downlink	ASK 100%, modified Miller Code, 106kbps
Uplink	Load modulation with 847 kbps subcarrier ASK-modulated, Manchester Code, 106kbps Anticollision: Binary search tree

3.8.3 ISO/IEC 14443 Type B - Proximity Contactless ICs

POWER SUPPLY:	13.56 MHz, inductive coupling Allowed field strength: 42 dBµA/m

Downlink	Downlink: ASK 10%, NRZ Code, 106kbps
Uplink	Load modulation with 847 kbps subcarrier BPSK (bi-phase shift keying) modulated, NRZ Code, 106 kbps Anticollision: Slotted Aloha

3.8.4 ISO/IEC 15693 - Vicinity Contactless ICs

POWER SUPPLY:	13.56 MHz inductive coupling Allowed field strength: 42 dBµA/m
DOWNLINK	Modulation: 10% ASK, 100% ASK Baud rate: 1.65 kbps, 26.48 kbps
UPLINK	Modulation: Load modulation with subcarrier Bit coding: Manchester, the subcarrier is ASK (423 KHz) or FSK (423/485 KHz) modulated Baud rate: 6.62 kbps, 26.48 kbps (selected by reader)

4 Application of Contactless ICs to MRTDs

4.1 INTRODUCTION

ICAO has traditionally tracked technology changes with a view to recommending their adoption by the international community for use by States in issuing Machine Readable Travel Documents. Contactless ICs are already used in many applications where fast non-contact reading of the holder's data is required (eg toll booths, transportation systems, and ID verification for access). Many of these applications use credit-card sized ID-1 cards which are approximately similar to the TD-1 Machine Readable Official Travel Document as defined in Doc 9303. Contactless ICs have also been defined as an "Optional Capacity Expansion" technology in DOC 9303. As well, contactless ICs are seen as presenting a desirable combination of unit cost, data capacity, and the practicality of incorporation in existing paper-based applications such as Machine Readable Passports and Visas.

4.2 RESTRICTION OF CONTACTLESS ICS TO ISO STANDARDS

To both avoid proprietary issues and to ensure that the contactless ICs work in every part of the world, the choice of contactless ICs has been restricted to those for which an ISO Standard exists. In addition, contactless ICs that are considered obsolete or not well supported – even though an ISO Standard might exist pertaining to them – have been eliminated.

Thus two ISO Standards have been selected for use:

- Proximity (up to 10cm) – ISO/IEC 14443
- Vicinity (up to 1m) – ISO/IEC 15693

4.3 CONSTRUCTION FACTORS

The following factors should be taken into account when constructing an MRTD containing a contactless chip.

4.3.1 Capacity of Data Storage

The contactless IC should be chosen to have sufficient data storage capacity to meet the requirements of the LDS, and in particular the data storage required by the encoded biometric(s), if any.

4.3.2 Data Processing

The contactless IC may have data processing in order to meet the requirements of PKI and encryption. Note that the greater power requirement of extra data processing electronics results in a lower operating distance.

4.3.3 Placement of the Contactless IC

4.3.3.1 MROTD

For placement of the contactless IC in an MROTD (TD-1 size) the usual industry guidelines for ID-1 size cards are followed.

4.3.3.2 MRP

For MRPs the contactless IC may be placed in the endleaf or an internal page, either by glueing, laminating, or encapsulating. Note that there may be advantages in separating the contactless IC from the data page eg reconciliation of data, tamperers having to change two areas. However tampering with the IC in the data page is likely to damage the data page too; and some issuance authorities may not wish for legal or procedural reasons separate the data page and the IC, especially if the data page is regarded as the official and legal identification.

Regardless of where the contactless IC is placed in the MRP, some notation must be included to warn visa issuance authorities not to apply a MRV with a contactless IC on the same leaf (either side) as this may interfere with the operation of the MRP contactless IC.

In the case of the MRP TD-1 sized card, the usual procedures for incorporating a contactless IC in an ID-1 size apply.

4.3.3.3 MRV

The MRV may be programmed into the contactless IC of the MRP, if available, and if there is sufficient data space in the MRP contactless IC to permit this. The specifications of the LDS must be followed.

Alternatively, the contactless IC may be implemented in an MRV-A or MRV-B sized label and placed into an MRP. It is strongly advised not to place MRV labels containing contactless ICs back-to-back on the same page (leaf) as it is then impossible to separate them if reading interference occurs. Moreover, in no circumstances should the MRV label be placed on either side of the page or cover containing the MRP contactless IC.

4.3.4 Antenna

The contactless IC should have an antenna that complies with either ISO/IEC 14443 or ISO/IEC 15693. It is recommended that for TD-2 and TD-3 size MRTDs the antenna conforms to the TD-1 size for compatibility.

4.3.5 Protection against Flexing

Flexing causes a significant failure mechanism in contactless ICs when placed in MRPs or MRVs. This flexing commonly breaks the electrical connection between the IC and the antenna, or it may fracture the IC itself. It is advised that the region of the IC and IC-antenna connection should be stiffened by means of a non-metallic surface to prevent this flexing.

4.3.6 Protection against Stamping

In normal use MRPs and MRVs are sometimes stamped with ink stamps. The contactless IC may be damaged by this action. It should be noted that even though the page containing the contactless IC might not be the subject of stamping, however the force may be transmitted through several pages and damage the IC. It is advised that a non-metallic “donut” or similar support assembly should be used to protect the contactless IC from the force of stamping.

4.3.7 Embossing and Heat Treatment

If the contactless IC is placed in the cover of a MRP, then care must be taken not to damage it if the cover is to be subsequently embossed with a coat-of-arms or similar. Also if the MRP is to be hot-laminated care must be taken that the heat does not damage the contactless IC.

4.4 ISSUANCE FACTORS

The following factors must be taken into account when issuing an MRTD containing a contactless IC.

4.4.1 Other ICAO Standards and Technical Reports

The MRTD containing the contactless IC must be issued in conformance with ICAO DOC 9303 Parts 1, 2 and 3. The data must be placed into the contactless IC in conformance with ICAO Technical Report: Development of Logical Data Structure (LDS) for Optional Capacity Expansion Technologies. Any biometric data must further conform to ICAO Technical Report: Selection of a Globally Interoperable Biometric for M-A Identity Confirmation with MRTDs. Finally the data in the contactless IC must be secured in conformance with ICAO Technical Report: PKI and Encryption.

4.4.2 Secure Programming

The original issuing authority must take care that the data is loaded securely. Methods for accomplishing this have been established but the details are beyond the scope of this document. There should be evidence of the issuing authority, and evidence that the data placed by the issuing authority has not been modified.

4.4.3 Biometric

While a biometric is not mandatory for contactless IC applications, it is advisable to include a biometric within the LDS structure if possible.

4.4.4 Quality Assurance

After personalization of the contactless IC, and completion of all the manufacturing procedures on the MRTD (eg embossing, laminating), the contactless IC should be read by a machine (RF) reader to make sure it is operational. Many failures of the contactless IC occur before it is issued to the holder and can be eliminated at this stage by proper quality assurance.

4.5 BORDER INSPECTION FACTORS

The following factors must be taken into account when inspecting an MRTD containing a contactless IC. The contactless IC will contain data pertaining to the holder of the MRTD.

4.5.1 Machine (RF) Reader

According to existing standards machine (RF) readers can read contactless ICs conforming to ISO/IEC 14443 Type A and Type B, and contactless ICs conforming to ISO/IEC 15693. For global interoperability it is advisable to use a machine reader which will read all types.

The machine reader may be configured to read the standard OCR-B MRZ. In this case, if reading of the contactless IC is desired at the same time, the antenna of the machine (RF) reader should be aligned for maximum coupling with the antenna of the contactless IC.

If an MRP containing a contactless IC also contains one or more MRV contactless ICs, the pages of the MRP may need to be physically separated to enable the RF reading process; otherwise RF interference may occur.

4.5.2 Reconciliation of Data

On reading the contactless IC the data contained therein should be reconciled with the data read from the data page (MRZ). If the contactless IC contains a biometric in the form that is similar to a displayed feature (ie-facial image), then it is advisable to check the data from the contactless IC with that shown in the displayed feature.

4.5.3 Border Inspection Methods

There are broadly two different border inspection methods. *"Staffed"* inspection requires the holder to surrender the MRTD to a border official for inspection and processing. *"Self-service"* inspection requires the holder to simply carry the MRTD through a gate where the contactless IC will be interogated for data identifying the holder. There is a third method of inspection, *"Walk-through"*, where the holder is inspected remotely without any specific action being required of the holder; however, for the purposes of this Technical Report "Walk-through" is regarded as "Self-service".

4.5.3.1 Staffed Border Inspection

In the staffed border inspection method, the MRTD is presented to an official who processes the application to enter the State, and may at the same time check the validity of the document and the right of the holder to present it. If the MRTD contains a contactless IC, then can be read by a machine (RF) reader. The official choses which data to use, the primary MRTD data or the contactless IC data.

Any possibility of security breaches can be avoided by making the machine (RF) reader relatively insensitive, that is, the reading range can be restricted to a few centimetres or even require physical contact. This will avoid the possibility of inadvertently (or for fraudulent purposes) reading another contactless IC concealed by the holder or held by another person.

The contactless IC can be incorporated into an existing primary MRTD (MRP, MRV or MROTD) in order to provide extended data capacity. In this case the primary MRTD will provide the link to the holder by means of the standard facial image or other biometric (if included). As a security aid, the data included in the contactless IC should be compared with the data contained in the primary MRTD. Note that if a biometric is contained within the LDS, then the constraints of data capacity and data transmission time mean that typically a contactless IC conforming to ISO/IEC 14443 will be used.

4.5.3.2 Self-service Border Inspection

The use of a contactless IC in an MRTD lends itself to the self-service processing application. In this application it is essential that the MRTD be linked to the holder by means of a biometric. This means that optimally the contactless IC should contain a biometric that can be read by the self-service processing system and compared with the holder. The type and implementation (ie full image, template) of the biometric is discussed in another Technical Report. Note that if a biometric is contained within the LDS, then the constraints of data capacity (typically 16K bytes) and data transmission time (typically less than 3 seconds) mean that typically a contactless IC conforming to ISO/IEC 14443 will be used. In this case the holder must place the MRTD containing the contactless IC in close proximity to the machine (RF) reader to activate the self-service system.

However, it may be desirable to read the MRTD containing the contactless IC at a distance in which case a vicinity contactless IC conforming to ISO/IEC 15693 may be used. In using a vicinity contactless IC, the data capacity is small (typically 2K bytes) and the data transfer rate is slow, governed by the power limitations at the greater distance. Therefore it is unlikely that the contactless IC will contain a biometric. Accordingly it is essential that in this self-service application the contactless IC access a biometric to be linked to the holder by means of an external biometric database. Therefore it is recognised that vicinity contactless ICs might not be able to be used fully in a globally interoperable manner for self-service border inspection unless there is shared access to the external biometric database.

4.5.4 Reading of Multiple Documents

ISO/IEC 14443 and ISO/IEC 15693 have collision avoidance schemes. In cases of reading multiple documents, for example, several MRPs brought into the reading range of the machine (RF) reader, or several MRV's in the same document, then the machine (RF) reader will read all of these documents in quick succession. It is then the function of the host computer system to manually or automatically select which MRPs or MRVs are relevant and valid.

In the case of multiple MRVs each containing a contactless IC, in an MRP which also may contain a contactless IC, there may be interference between the antenna, especially if these are spatially matched. In this case generally one or none of the contactless ICs will be read, but not all. To achieve reading of the desired contactless IC, the page containing the contactless IC should be held open and apart from the other pages of the MRP, and placed in the range of the machine (RF) reader. It should be noted again that MRVs containing contactless ICs should not be placed back-to-back on the same page (leaf), as it is then impossible to separate them for reading if interference occurs.

4.6 PRIVACY AND UNAUTHORIZED READING

ISO/IEC 14443 and ISO/IEC 15693 specify maximum reading distances for machine (RF) readers that conform. As the available power for the contactless ICs decreases proportional to the sixth power of the distance between the machine (RF) reader and the IC, it is unlikely that unauthorized reading will occur. However, this can not completely ruled out. There are methods of preventing unauthorized reading. One such method is that a state (or other organization) wishing to issue contactless IC may consider giving holders the advice to keep their MRTD in a metal jacket when not in use. This will completely prevent unauthorized reading. The MRTD must be removed from the metal jacket for authorized reading.

With MRPs another option if privacy is of paramount concern is to place a metal surface on an adjacent page. Under this scheme the contactless IC will not be readable while the MRP is closed. To read the contactless IC the MRP must be opened causing the antenna of contactless IC to be moved away from the metal surface.

At borders, the reading states may need to ensure that the sub-carrier of the contactless IC (returning data to the machine (RF) reader) is not detectable at any appreciable distance from the machine (RF) reader.

4.7 SECURITY ISSUES

The MRTD containing the contactless IC should be resistant to physical tampering, and alteration of the data in the IC. Methods for accomplishing this have been established but the details are beyond the scope of this document. See also other Technical Reports.

4.8 INTEROPERABILITY ISSUES

4.8.1 Interoperability of Contactless ICs Conforming to ISO/IEC 14443

The following is taken from the Appendix 3 to Annex C of the Technical Report on the Logical Data Structure.

This appendix defines the minimum requirements for interoperability of proximity (ISO/IEC 14443) contactless IC based MRTDs:

- ISO/IEC 14443 Parts 1-4 and ISO/IEC 10373-6 compliant considering amendments to both standard series
- Type A or Type B signal interface (readers must be capable of reading both)
- Support for a file structure as defined by ISO/IEC 7816-4 for variable length records
- Support for one or more applications and appropriate commands as defined by ISO/IEC 7816-4,5.

Example of sequence of operation:

- Document enters operating field of Proximity Coupling Device (PCD)
- IC responds to Request for Command-Type A (REQA) or Request for Command-Type B (REQB) with Answer to Request-Type A (ATQA) or Answer to Request-Type B (ATQB) as appropriate.
- The PCD shall detect and resolve any collision that may occur if multiple documents are within the operating field.
    - ICAO AFI = *tbd*
- Compliance with 7816 commands shall be indicated by
    - Type A: SAK (Select Acknowledge) bit 6 = 1, bit 3 = 0
    - Type B: Protocol_Type = "0001"
- The ICAO MRTD Application shall be selected using the following sequence

  <u>Example of application selection for the issuer application</u>
  The issuer application shall be selected by use of the following parameters for the APDU.

CLA	*'00'*
INS	*'A4'*
P1	*'04' – (select by DF name – the AID)*
P2	*'00'*
L_c	*'06' – (length of AID)*
Data field	*'A0 00 xx xx xx 01' – (the issuer AID)*

L_e	*'00' – return the application label if present*

The response data field contains the application label. The label shall be 'MRTD'

- The common data file EF.COM (Short File ID = 30) containing Application Identifier, Version levels and tag list will be read using the Read Record command

CLA	'00'
INS	'B2'
P1	'1E' - specifies record number thirty
P2	'0C' - read by record number from SFI '1E'
L_c	Empty
Data field	Empty
L_e	0 - specifies to read the entire record

- The tag list in EF.COM will list the Data Groups (Elementary Files) encoded within this document.

- The Machine Readable Zone (MRZ) is read using the Short File designator, '01' or record identifier '61.'

<u>Example using short file designator</u>

CLA	'00'
INS	'B2'
P1	'01' - specifies record number one
P2	'0C' - read by record number from SFI '01'
L_c	Empty
Data field	Empty
L_e	0 - specifies to read the entire record

<u>Example using record identifier</u>

CLA	'00'
INS	'B2'
P1	'61' - specifies the record identifier
P2	'0A' - read next record by record identifier from SFI '01'
L_c	Empty
Data field	Empty

L_e	0 - specifies to read the entire record

- Other Data Groups are read as needed

- If the IC supports "Get Data," this command can be used to retrieve a specific data object.

  This example gets the data object with tag ’5C’ from the current DF. (This data object contains the list of data groups present in the application.) The APDU parameters for this action are shown below.

CLA	‘00’
INS	‘CA’
P1	‘00’ - indicates a simple-BER-TLV tag
P2	‘5C’ - data object tag’
L_c	Empty
Data field	Empty
L_e	0 - specifies to read the entire data object

The response data field contains the data object

4.8.2 Interoperability of Contactless ICs Conforming to ISO/IEC 15693

[to be added]

5. Glossary

Machine readable travel document (MRTD): Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity). The MRTD contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read.

Global Interoperability: An MRTD conforming to Doc 9303 issued by one country must be readable by any receiving country.

Logical Data Structure (LDS): standardized data format common to optional capacity expansion technologies of MRTDs to enable global interoperability for recorded details (travel document data) used during inspection of person and their MRTD.

Biometric: encoded physical characteristic which identifies the holder of an MRTD.

Machine readable zone (MRZ): Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods.

Contactless IC: the data carrying unit incorporated into the MRTD, consisting of an integrated circuit or microchip and an antenna. Also known as *tag, RF device, chip.*

Machine (RF) reader: the radio frequency reader which provides the power to the contactless IC and reads and writes to the contactless IC by means of radio waves.

Passive: the contactless IC contains no power source of its own and must be powered by the machine (RF) reader. Opposite: *active*, where the contactless IC is powered by an internal battery.

Durability, physical: the contactless IC is prone to physical damage due to stamping or heat, and flexing may damage the IC and/or the connection to the antenna. In general, the larger the data capacity of the IC, the larger the IC and greater the risk of damage.

Durability, data: the data contained in the contactless IC is held as electrical charges which may leak away in time if not refreshed by actual use in the electromagnetic field of the machine (RF) reader. The time taken for the charge to leak away (without use) is generally more than ten years.

Proximity: the contactless IC operates at a close distance to the machine (RF) reader, generally at 10cm or less. ISO/IEC 14443 refers.

Vicinity: the contactless IC operates at a further distance from the machine (RF) reader, generally at 1m or less. ISO/IEC 15693 refers.

Staffed Border Inspection: an authorized official carries out inspection of the MRTD, the holder surrenders the document to the official.

Self-service Border Inspection: the holder facilitates border inspection by placing the MRTD near, or inserting the MRTD into, a kiosk, booth or gate machine reader.

Walk-through Border Inspection: the holder is subjected to border inspection remotely, possibly being unaware of the operation.

Collision avoidance: a procedure that enables a machine (RF) reader that has encountered more than one contactless IC at the same time to distinguish between the ICs and effectively communicate with them individually.

Downlink: refers to communication from the machine (RF) reader to the contactless IC.

Uplink: refers to communication from the contactless IC to the machine (RF) reader.

Quality Assurance: the contactless IC is inspected after production to ensure its correct operation.