International Civil Aviation Organization

TAG/MRTD/21-WP/6
28/11/12
English Only

WORKING PAPER

TECHNICAL ADVISORY GROUP ON MACHINE READABLE TRAVEL DOCUMENTS (TAG/MRTD)

TWENTY-FIRST MEETING

Montréal, 10 to 12 December 2012

Agenda Item 2: Activities of the NTWG

REVISION OF THE LOGICAL DATA STRUCTURE TECHNICAL REPORT

(Presented by the New Technologies Working Group)

1. INTRODUCTION

1.1 Approval was given by the TAG-MRTD/20 to continue the on-going work of the NTWG for revision of the Logical Data Structure (LDS) and the development of a Technical Report for subsequent consideration and adoption.

1.2 This Technical Report is to be known as the LDS Version 2.0 Technical Report Draft.

1.3 This Working Paper describes the present status and requests endorsement to proceed.

2. BACKGROUND

2.1 Approval was given by the TAG-MRTD/19 in 2009 to continue the work of the NTWG for revision of the Logical Data Structure (LDS) and the development of a Technical Report Draft for subsequent consideration and adoption.

2.2 The LDS Sub-Working Group conducted several meetings to develop drafts and adjudicate comments from government and non-government participants. The draft report is a result of this iterative and exhaustive process.

2.3 The Technical Report Draft is informed by government policies and considerations surrounding current implementation, capabilities, and uses of electronic machine readable travel documents (eMRTD):

- The current LDS (known as LDS1) focuses on the electronification of the interoperable elements of the data page.
- The LDS Technical Report Draft reflects the adoption of the principle that LDS Version 2.0 (known as LDS2) will electronify visas and travel stamps and provide for additional biometrics. Accordingly, the use of LDS2 will require provision to allow writing to the chip after personalization.

2.4 LDS Version 2.0, which is optional for States to choose to use or not, will allow receiving States to add data to eMRTDs, furthering lawful, efficient, and secure travel while protecting the privacy of the traveling public. It also emphasizes protections against vulnerabilities such as counterfeiting, copying, and unauthorized reading.

3. PRESENT STATUS

3.1 The LDS Sub-Working Group recognizes that border, immigration, and passport-issuing authorities' budgets may limit the ability to fully exploit the potential of chip technology.

3.2 The LDS Sub-Working Group decided that this will be a new and optional LDS and that the current LDS remains intact. This means that the proposed Version 2.0 ensures backward compatibility with LDS Version 1.7.

3.3 A central concept for LDS2 is that it will be a new version that will allow for optional data to be implemented as separate and individual applications on the chip. The draft technical report is known as *LDS 2.0 – Optional Expanded Chip Functionality – Version 1.0*.

The LDS Sub-Working Group has agreed upon three applications for LDS Version 2.0 – visas, travel stamps, and additional biometrics. The new LDS2 applications are considered optional components of the eMRTD and can only be deployed under the direct policy control of the travel document issuing State. New LDS2 applications will focus on the writing or appending of data by the issuer and other States.

3.4 As a consequence, any State that wants to read or write data from or to the chip requires a certificate chain that starts with a certificate verifiable by the State that has issued the eMRTD. TF5 is working on a discussion paper to determine the trust model for public keys to be distributed to receiving countries.

3.5 The LDS Sub-Working Group considered the inclusion of the "Identification feature" data element of a visa. It was determined that this is a physical document security mechanism that is synonymous to an electronic authentication mechanism and does not imply the need for an added traveler biometric unless it proves to be a necessity due to national visa issuance policy. Inclusion of this data component may also prematurely exceed storage capacity as travelers add more visas.

3.6 The LDS Sub-Working Group presented updates to the NTWG in June 2012 in Montreal. The LDS Sub-Working Group sought and received NTWG concurrence to postpone the operational timeline completion date from early 2014 to late 2014.

3.7 The LDS Sub-Working Group met in July 2012 with Task Force 5 of ISO/IEC JTC1 SC17 WG3 (TF5) to address questions and clarify business requirements for the LDS2.0 applications. These clarifications included agreement that TF5 would develop a global certificate policy for the LDS 2.0 Public Key Infrastructure model. Further, the LDS Sub-Working Group agreed that certificate

exchange would be based on the EU's Single Point of Contact (SPOC) mechanism. The LDS Sub-Working Group charged TF5 with drafting the technical specifications for LDS2. TF5 will report results for discussion to the sub-group and NTWG. The LDS Sub-Working Group is revising the technical report and continues to address policy issues as they arise.

3.8 ISO / WG3 / TF5 met in October 2012 in New Orleans, Louisiana to discuss drafting of technical specifications in LDS2. TF5 discussed LDS2 data structures, security protocols for LDS2 applications, and public key infrastructure.

4. NEXT STEPS AND AVENUES FORWARD

4.1 The LDS Sub-Working Group will continue outreach to government entities to expand understanding of the optional additional applications and collaboration with TF5 to develop the policy and technical specifications that implement the applications defined in this report.

4.2 The LDS Sub-Working Group will hold the next meeting on January 29-30, 2013 in Washington, DC. TF5 will report on progress on the drafting of technical specifications. This meeting will be in advance of the NTWG which is scheduled for February 18-21, 2013 (location to be finalized).

4.3 The operational timeline for next steps as envisioned is:

- Solicit all comments, incorporate revisions and have final draft of policies / functionalities and preliminary draft of technical specifications ready for submission to TAG-MRTD/22; and
- Complete the Technical Report through to publication of final technical specifications in late 2014.

5. ACTION BY THE TAG/MRTD

The TAG/MRTD is invited to approve and endorse the continued work on this Technical Report.

— END —

APPENDIX A

MACHINE READABLE TRAVEL DOCUMENTS

TECHNICAL REPORT

LOGICAL DATA STRUCTURE 2.0 – Optional Expanded Chip Functionality

DRAFT VERSION 0.8 (Note: Version 1.0 after TAG approval)

Updated on July 28, 2011

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Logical Data Structure (LDS) Version 2.0

Release : 0.8
Date : July 28, 2011

Release Control

Release	Date	Description
0.2	2010-10-07	Initial Release
0.3	2011-01-07	Modifications based on comments from NTWG meeting in Tokyo
0.4	2011-01-25	Modifications based on comments following LDS2 Meeting in Tokyo
0.5	2011-02-25	Modifications based on comments from LDS2 Meeting in Washington
0.6	2011-04-25	Modifications based on comments received after LDS2 Meeting in Washington and TF5 Meeting in Singapore
0.7	2011-07-20	Modifications based on comments received at and after NTWG in Bern, Switzerland in May 2011.
0.8	2011-07-28	Modifications based on comments and discussions at LDS Sub-Working Group meeting in Washington, DC on July 20-21, 2011.

Table of Contents

FOREWORD

The International Civil Aviation Organization (ICAO) published the specifications for electronic passports in 2006 in the Sixth Edition of Doc 9303, Part 1, Machine Readable Passports, Volume 2, Specifications for Electronically Enabled Passports with Biometric Identification Capability. In 2008, the ICAO published the specifications for electronically enabled official travel documents in the Third Edition of Doc 9303 Part 3, Machine Readable Official Travel Documents, Volume 2, Specifications for Electronically Enabled MRTDs with Biometric Identification Capability. The Logical Data Structure (LDS) is a fundamental and foundational component of the technical underpinnings of electronic Machine Readable Travel Documents (eMRTD). The LDS describes how data are to be written to and formatted in the contactless integrated circuit chip of the eMRTD. The most recent version of the LDS, known as 1.7 (hereafter referred to as LDS1), has been codified into the current edition of Doc 9303.

LDS1 defines the specifications for the standardized organization of data for the recording of biometric, biographic and associated information in an eMRTD chip (or Contactless Integrated Circuit capacity expansion technology of the eMRTD) at the discretion of an issuing State so that the data is accessible by receiving States. The current version of the LDS1 supports recording of data only by an issuing State. The capability for receiving States to write to the LDS is not supported in the current version. This report explores the option for issuing and receiving States to write to the LDS for electronic travel history, visas, and automated border clearance applications. This is known as LDS2 for purposes of this report.

Where LDS1 can be seen as an electronic representation of the data page, the principle for LDS2 is the "electronification" of the remainder of the eMRTD (specifically to the passport-booklet, i.e., visa and entry-/exit-stamps) as well as further refinement/support of the verification process. The evolution of chip technologies combined with expanding use of eMRTDs and requests from stakeholders to use the documents to their fullest extent, combined with the latest and most secure privacy measures, is the impetus for addressing these additional functionalities in LDS2.

By developing LDS2 and allowing receiving States to add data to eMRTDs, ICAO seeks to promote lawful, efficient, and secure travel while protecting the privacy of the traveling public. Given the attention that the use and storage of biometrics and other personal data attract, privacy and data protection are vitally important for maintaining clarity of purpose concerning the use of eMRTDs for border control purposes. Thus, data integrity and respect for individual privacy should be part of the border and immigration planning and implementation processes and must be taken into account.

A central concept for LDS2 is that it will be a new version that will allow for optional data to be implemented as separate and individual applications on the chip. ICAO initially established as a preeminent requirement the need for a single LDS for all eMRTDs. The new LDS2 will meet this requirement: it will retain the existing LDS1 application as well as the new use cases defined herein. The new LDS2 applications are considered optional components of the eMRTD and can only be deployed under the direct policy control of the travel document issuing State. New LDS2 applications will focus on the writing or appending of data by the issuer and other States. This provides additional optional capabilities beyond LDS1. For States who have adopted LDS1 issuance and inspection capabilities, they can be assured their efforts will not be made obsolete by LDS2. Documents designed to LDS2 capabilities shall behave like a document designed under LDS1 by systems designed solely to inspect LDS1 based travel documents.

The policy considerations and requirements regarding new use cases and post-issuance recording of data by receiving States or other approved receiving organizations are the subject of this report. The current version of this report is the direct result of joint group meetings of the Task Forces and the overall and general membership of the ICAO working groups. This report is a point-in-time snapshot; dialogue and outreach to key stakeholders is ongoing to understand current and future uses of

eMRTDs and make tangible the benefits represented by its expanded use to State authorities as well as the general public. Furthermore, expanded use of LDS functions will lead to enhanced understanding by immigration and inspection authorities while facilitating travel and heightening aviation security.

1. INTRODUCTION

ICAO Doc 9303 – Parts 1 and 3, Volume 2, Section III, standardizes the LDS to ensure efficient facilitation of the travel document holder, to protect data recorded in the chip, and to address the needs of issuing and receiving States as well as carrier organizations. As our collective business needs evolve, the current LDS standard must accommodate existing as well as emerging operational requirements.

The current LDS version (LDS1) is the standardized organization of data for the recording of biometric, biographic, and associated information in a chip. The current version meets the needs of receiving States to verify the authenticity and integrity of the information stored on the chip.

Evolving eMRTD chip technology offers new opportunities to implement additional functionality and use cases with respect to enhanced facilitation and security considerations. The LDS sub-working group of ICAO's NTWG was directed to review and recommend revisions to the current LDS version. The LDS sub-working group advocates the use of the electronic Machine Readable Travel Document (eMRTD) to support assisted and fully automated processes at the border and potentially throughout the travel continuum at the option of the issuing and receiving States.

The term LDS2 in this document describes a potential series of discrete new applications on the chip in addition to the existing LDS1 application. For example, an electronic visa is a different optional use case from an electronic travel stamp. The LDS Working Group understands that the explanation of how and when to use these options will be the subject of an additional technical specification.

Data protection and privacy are of paramount importance to the traveling public. Data protection and privacy legislation, including prohibition of passing personal data to third parties, using personal data for purposes other than that its stated purpose, varies in detail from country to country. Of particular concern is what happens to the data after the eMRTD has been read, who might have access to it, and for what purpose. Since the primary stakeholder is the travel document holder, full consideration should be given to factors such as ease of use and privacy protection.

Global interoperability is a major objective of the standardized specifications for placement of both visual and machine readable data in all MRTDs; the LDS2 continues this objective. In this context, the term is understood as the capability of inspection systems in different States throughout the world to exchange data, to process data recorded by other States, and to utilize that data in inspection operations in their respective States. Implementation of the optional LDS2 applications depends on the issuing State's policy decisions and internal specifications. Likewise, issuing States will determine who is allowed to write to the applications after issuance. If the LDS2 use cases are implemented, data that is currently visible in the document should, in general, remain viewable on the chip. However, access to additional biometrics should be restricted to authorized inspection systems. For transparency, it is recommended that issuing States make provisions for the document bearer to view all data written to the chip post issuance.

1.1 METHODOLOGY FOR DEVELOPMENT OF THE REPORT

At the meeting of Technical Advisory Group (TAG) 16 in 2005, the TAG approved the ongoing efforts of the NTWG to develop version 2.0 of the LDS, and endorsed a draft outline for this report. During the TAG 17 meeting in March 2007, the NWTG (1) asked the TAG to note that LDS 1.7 had been incorporated into Doc 9303; (2) acknowledged the need to revise the LDS Technical Report to address additional optional functionalities to be included; and (3) endorsed the revision as LDS Technical Report Version 2.0.

The NTWG formed an LDS sub-working group to review the current LDS and roadmap for the next version (LDS2). The sub-working group is initially focusing on policy considerations regarding

multiple applications on the chip and post issuance appending of data, while working closely with technical experts to progress the LDS2 project.

To assess border, immigration, and passport-issuing authorities' current use of the LDS, the LDS sub-working group created and distributed a survey and collected opinions from both Government and non-government organizations (see Annex C: Current and Future Use of Electronic Passports Questionnaire and Response Summary). These survey responses served as starting points for discussion of expanded LDS capabilities. As the NTWG and its Task Forces develop the technical specifications for LDS2, it is imperative to continue this outreach.

To provide full backward compatibility, the LDS sub-working group determined that the LDS1 will not be changed and shall not rely on the adoption of LDS2. The LDS2 will be a new version to allow for optional data to be implemented as separate and individual applications on the chip. These new LDS2 applications are therefore considered an optional component of the eMRTD under the direct policy control of the travel document issuing State. This report does not address issues regarding LDS1 addressed through the Doc 9303 Supplement.

States are developing next generation eMRTDs to include fingerprint and iris biometrics. There is also an increase in use of automated border clearance concepts to facilitate travel through use of eMRTDs. As the issuance and use of eMRTDs increases, it is important to understand and assess how border, immigration, and passport issuing authorities have reacted to eMRTDs. Immigration and inspection authorities, as well as the general public, may not be aware of the benefits of the eMRTD for facilitated travel and aviation security. Providing education and information to issuing and inspection authorities and the general public regarding the benefits of eMRTDs and LDS2 will continue to be a focus for ICAO and the NTWG.

1.2 REFERENCES

The following documents are referenced in this report:

[1] ICAO Doc 9303 Part 1, "Machine Readable Passports", Volume 2

[2] ICAO Doc 9303 Part 3, "Machine Readable Official Travel Documents", Volume 2

[3] ICAO Technical Report "CSCA countersigning and Master List issuance"

[4] ICAO Technical Report "Supplemental Access Control for Machine Readable Travel Documents"

[5] Supplement to Doc 9303 – Release 10

2. LDS1 BACKGROUND AND HISTORY

LDS1 defined the storage architecture for eMRTD data. It was made a requirement for global interoperability and does not include the option of adding data to the Contactless Integrated Circuit by any authority after the eMRTD has been issued. This requires the identification of all mandatory and optional data elements and a prescriptive ordering and/or grouping of data elements that must be followed to achieve global interoperability for reading of details recorded in the capacity expansion technology optionally included on an eMRTD. Given the global disparity in inspection systems and regimes, many receiving States are not in a position to read and or validate data from eMRTDs deploying LDS1. Consequently these receiving States are also not in a position to add data to an eMRTD deploying LDS2. Henceforth there is a clear need to maintain LDS1 as a foundation level for global interoperable reading of eMRTD data. Any incorporation of LDS2 into Doc 9303 should, thus, not affect States who choose to continue to solely use the LDS1 architecture.

ICAO has determined that the standardized LDS must meet a number of mandatory requirements[1]:

- Ensure efficient and optimum facilitation of the rightful bearer;
- Ensure protection of details recorded in the optional capacity expansion technology;
- Allow global interchange of capacity expanded data based on the use of a single LDS common to all eMRTDs;
- Address the diverse optional capacity expansion needs of issuing States and organizations;
- Provide expansion capacity as user needs and available technology evolve;
- Support a variety of data protection options;
- Support the updating of details by an issuing State or organization, if it so chooses; and,
- Support the addition of details by a receiving State or approved receiving organization while maintaining the authenticity and integrity of data created by the issuing State or organization.

The ordered groupings of Data Elements defined in LDS1 were grouped based on whether they have been recorded by (1) an issuing State or organization or (2) a receiving State or approved receiving organization. LDS1 defined the Issuer data application, consisting of two mandatory Data Groups (DG1, Details recorded in the Machine Readable Zone (MRZ), and DG2, Encoded face) and 14 optional DGs, and included a placeholder for the User application for recording of data by receiving States for the following potential capabilities: Automated Border Clearance, Electronic Visas, and Travel Records.

2.1 PRESENT LDS1 CAPABILITIES

LDS1 supports potential eMRTD functions beyond border inspection by governments and private entities. These functions, however, require the establishment of the necessary infrastructure and national policy for implementation. This includes facilitated travel using the electronic data on the travel document to perform biometric verification and automated customs clearance, allowing immigration and border management officials to focus on individuals who may require further inspection.

Machine Assisted Document Security Verification (MADV) encompasses the use of document printing technologies at the time of issuance to deter counterfeit and forgery attacks. This information is accommodated under LDS1 Data Groups 8 through 10 for data, structure, and substance. Support for self asserting MADV security mechanisms is achievable through the existing LDS1 structure. Considering annotations, comments, or modification of the e-Passport data page invalidates the document for further use, therefore, updates to MADV data page characteristics proves unnecessary.

[1] ICAO Doc 9303, Part 1, Volume 2, Section III 5.1.

The general principle of the current LDS1 means:

- Storage of the printed information in Data Groups (DG) on the eMRTD chip by the passport issuing authority at the time of issuance
- No writing to the Data Groups after issuance, likewise as writing to the data page after issuance is not possible
- Read access to the chip for everyone in possession of the passport, likewise as everyone in possession of the passport can read the physical data page
- Support of the verification of the identity of the holder via biometrics (traditionally by manual comparison of the displayed portrait with the holder, electronically by machine-assisted face/fingerprint/iris-biometric verification)

2.2 POTENTIAL LDS1 FUNCTIONS

Other potential functions for LDS1, which are applicable without modifying LDS1 structure, would be the use of the eMRTD data as a token to access databases. These use cases which may be subject to national regulations include both government and private industry uses such as:

- Access to travel records in databases to support immigration/admissibility determinations;
- Application for renewal of an expired/expiring passport at a kiosk based on verification of the applicant at the kiosk.
- Airline uses to speed and simplify check-in processing and boarding. The eMRTD data can be used to populate passenger information system data to reduce data entry errors or inaccurate OCR scans of the printed MRZ. Existing data on the eMRTD can also be used to issue airline boarding passes, luggage tags, or to permit traveler self check-in by reading the eMRTD data and using it to access data in airline systems.

2.3 LOGICAL NEXT STEPS

The next logical step is the electronification of the remainder of the travel document, i.e., providing electronic storage for visa and entry-/exit travel stamps as well as further refinement/support of the verification process. This means:

- Enabling the passport issuing authority to include globally interoperable applications on the chip to electronically record travel stamps or visas
- Allowing writing to the new applications after issuance as authorized by the issuing authorities, likewise as travel stamps and visas are added to the travel document after issuance
- Read access to the electronic travel stamp and visa data on the chip for those in possession of the passport which is consistent with current ability of those in possession of the passport to view the travel stamps or visas included in the passport booklet.2
- Reading of additional biometrics (fingerprints and iris) using strong access control features due to the sensitive nature of the data.

These are the principles of the proposed LDS2, described in the following.

[2] Discussion on open read access is currently ongoing.

3. LOGICAL DATA STRUCTURE VERSION 2.0

Based on the guiding principle of electronification of the entire passport-booklet, the LDS2 shall facilitate the following optional capabilities:

- Storage, evidence, and retrieval of visa3 information / approvals from States;
- Storage, evidence, and retrieval of entry / exit records (travel stamps) from States;
- Storage of additional biometrics for facilitated travel programs.

LDS2 is limited in scope to include information issued and approved by government entities only and does not accommodate third party or commercial interests at this time. With these added capabilities, new policies must be implemented to prevent misuse and damage to the travel document when dealing with electronic media where problems are not visibly evident upon casual inspection.

Currently, visa and travel records, if they are included at all, are placed in the passport as a stamp or a sticker only. This is a major obstacle for automated or machine-assisted border clearance. For example, many visas are issued as a sticker with a separate MRZ, which has to be scanned in addition to the MRZ of the passport. Also in manned border-inspection booths, automated retrieval of these information elements from the chip has the potential to speed up the processing.

Additionally, digitally signed storage of visa and travel stamps dramatically enhances the security of these elements against tampering. The current methods of placing stickers or stamping do not provide the same level of security as the data page of the passport, which is usually secured using enhanced physical security measures, let alone the security of the electronically stored data page.

Physically stamping the passport is vulnerable to misuse and can be difficult to detect. In the electronic world, misuse can include such items as filling up the finite resources of the chip by repeatedly writing data to it. Such misuse makes it more difficult to complete a border inspection and can cause great inconvenience to the holder of the passport. Therefore, writing visa and travel records must only be allowed to authorized parties.

3.1 BEARER CONTENT ACCESS

To address readability and bearer access issues, States may consider hosting eMRTD self-service kiosks at the vicinity of points of inspection to provide the bearer the ability to perform document maintenance. Some travel document bearers are obligated to keep certain travel information up to date during the life of the passport book. It is difficult to anticipate public interest in monitoring the contents of the eMRTD when treated as a static token but curiosity in what other States may be adding to it may prove to be a tipping point. Services should allow the display for the contents of all LDS data groups.

3.2 RECEIVING STATE ACCESS

Receiving States have read access to all travel history as is currently permitted through visual inspection. In order to be allowed to write to the chip, the receiving State must acquire write access from the issuing State.

In order to prevent storage denial attacks by unauthorized entities filling the eMRTD with spurious data, a mechanism is needed to limit write access to agreed formats. Worldwide distribution of credentials to limit write access may leverage the PKD once a formal governance policy is agreed upon to certify the authenticity of requestors. See Section 6. LDS2 Security and Privacy Architecture.

[3] The term visa is defined in Doc 9303, Part 2. When used in this document, the term electronic visa refers to an LDS2 application to record visa information to the eMRTD chip; it does not refer to a visa with a chip, which is prohibited under current ICAO specifications, nor does it refer to electronic travel authorizations that do not include writing data to the chip.

3.3 RELATIONSHIP BETWEEN PHYSICAL AND ELECTRONIC DOCUMENT

A basic principle of the LDS1 is the consistency between the physical and the electronic document. This means that the data stored on the chip is identical to the printed information (the exception being the [optional] secondary biometrics). There are mainly two reasons for this. First, an electronic document – regardless of whether the chip is functioning – is still valid as a physical document. Second, this principle enables the holder to know which data are stored on the chip without using technical equipment.

This principle is valid for both Doc 9303 Part 1-Documents [1] (i.e., passports) and Doc 9303 Part 3-Documents [2] (e.g., MRTD application on ID-cards). Both types of documents have essentially the same information printed on the data page.

Part 1-documents (passports) are the primary, globally interoperable travel documents. Therefore the mentioned basic principle of consistency between the physical and electronic document should not be abandoned for passports when employing LDS2. This means that only those travel-records and visas which are also placed physically into the booklet shall be stored electronically. In practice, this means that the electronically stored visa and travel-records may be only a subset of the physical recorded information, since not all countries / border-posts will be equipped with the necessary equipment to write to the chip.

The situation is different for Machine Readable Official Travel Document (ICAO Doc 9303, Part 3-Documents), such as identity cards. In general, Part 3-Documents are not globally accepted as international travel-documents, in part since physical recording of visa and travel-records is not possible. The electronic storage of this travel information using an LDS2 application can facilitate the usage of a Part 3-Document as an internationally accepted travel document.

3.4 MULTI-APPLICATION CHIPS

With the introduction of the LDS2, the chip on the passport will be a multi-application chip. This means that new LDS2 applications operate alongside the existing LDS1, and access control to the applications cannot be evaluated in isolation. The access control to all applications of the chip must be designed as an integrated whole while keeping full backward compatibility with the LDS1.

This becomes more involved for Doc 9303 – Part 3 documents which may contain additional national applications, e.g., a driving license-application or eID-/signature-applications in the case of ID-cards. For these documents further consideration may be needed to design and enforce access to the LDS1-application to appropriately protect the privacy of the card-holder. The key to multi-application chips resides in the policies that issuers clearly outline for the entitlement, use and verification of such documents.

3.5 CONSIDERATION OF RELATIVE COSTS AND BENEFITS

The implementation costs will vary among States. Each State will need to do a cost benefit analysis. As traffic volumes continue to grow and States focus on how they can automate some of their clearance processes with the employment of computerized databases, the eMRTD plays an important part in modern, enhanced border inspection systems. Equipment to read and validate the eMRTDs and access databases may entail a substantial investment, but this investment can be expected to be returned by improvements in security, clearance speed and accuracy of verification that such systems provide. Use of eMRTDs in automated border clearance systems may also make it possible for States to eliminate both the requirement for paper documents, such as passenger manifests and embarkation/disembarkation cards, and the administrative costs associated with the related manual procedures.

The current cost of developing eMRTDs is born exclusively by the issuing authority. Some border and immigration authorities may not be fully aware of the capabilities of the current eMRTD, nor of

the changes to process and infrastructure necessary to use the eMRTD to facilitate travel and enhance security. The cost for implementation of automated border gates and processing and inspection of eMRTDs is currently born by the receiving authority. It is important to recognize that border, immigration, and passport issuing authorities face budget short falls which may limit their ability to fully exploit the potential of a new LDS. Implementation and utilization of LDS2 capabilities will require additional expenditures for both issuing and receiving authorities. Any additional costs incurred will be a function of the range of options chosen by the issuing State and receiving State, as appropriate, in direct proportion to the functions deployed.

3.6 SECURITY AND ACCESS CONTROL

The common technical basis for all described uses is the management of access control to the chip (reading and writing). Access to the LDS2-information shall be governed by the issuing State, to ensure protection of the passport against malicious writing as well as protection of the citizen's data against access by non-authorized parties.

The following table summarizes LDS1 and LDS2 accessibility. The technical requirements for access control management are described in the chapter “Security Architecture.”

Table 1. Access rights under LDS1

Data Group	Description	Read	Write	Update	Delete
DG 1	Details recorded in MRZ	All	eMRTD issuing State only during personalization	Disallowed	Disallowed
DG 2	Encoded Face	All	eMRTD issuing State only during personalization	Disallowed	Disallowed
DG 3	Encoded Fingerprint(s)	eMRTD issuing State authentication required	eMRTD issuing State only during personalization	Disallowed	Disallowed
DG 4	Encoded Eye(s)	eMRTD issuing State authentication required	eMRTD issuing State only during personalization	Disallowed	Disallowed
DG 5	Displayed Portrait	All	eMRTD issuing State only during personalization	Disallowed	Disallowed
DG 6	Reserved for Future Use	All	eMRTD issuing State only during personalization	Disallowed	Disallowed
DG 7	Displayed Signature	All	eMRTD issuing State only during personalization	Disallowed	Disallowed
DG 8	Data Feature(s)	All	eMRTD issuing State only during personalization	Disallowed	Disallowed
DG 9	Structure Feature(s)	All	eMRTD issuing State only during personalization	Disallowed	Disallowed
DG 10	Substance Feature(s)	All	eMRTD issuing State only during personalization	Disallowed	Disallowed
DG 11	Additional Personal Detail(s)	All	eMRTD issuing State only during personalization	Disallowed	Disallowed
DG 12	Additional Document Detail(s)	All	eMRTD issuing State only during personalization	Disallowed	Disallowed
DG 13	Optional Detail(s)	All	eMRTD issuing State only during personalization	Disallowed	Disallowed
DG 14	Security Options for Secondary Biometrics	All	eMRTD issuing State only during personalization	Disallowed	Disallowed
DG 15	Active Authentication Public Key Info	All	eMRTD issuing State only during personalization	Disallowed	Disallowed
DG 16	Person(s) to Notify	All	eMRTD issuing State only during personalization	Disallowed	Disallowed

Table 2. Access rights under LDS2

Description	Read	Write/Append	Update	Delete
Electronic Visas	All	eMRTD issuing State authentication required	eMRTD and Visa issuing State authentication required	Disallowed
Travel Stamps	All	eMRTD issuing State authentication required	Disallowed	Disallowed
Additional Biometrics	eMRTD issuing State authentication required	eMRTD issuing State authentication required	eMRTD issuing State authentication required	Disallowed

3.7 PUBLIC AWARENESS

It is important that the traveling public have full and complete knowledge of the effects brought about by LDS2, from both a procedural perspective as well as the benefits to be derived by its use. In this context, privacy and data protection are uppermost in eMRTD programs in general and LDS2 deployments specifically. It is important that the traveling public understand the purposes concerning eMRTDs for border management and the direct benefits to be derived from their use in the context of LDS2.

Each eMRTD holder needs to be aware of the purposes for which the data contained in the document will be used and, especially important, the mutual benefits derived for both the State as well as the traveler. For example, regarding the (optional) use of LDS2, travel stamps are already included in the traditional physical document, though not yet universally applied by all States. Since LDS2 allows electronic travel stamping of the travel history, implementing States can more readily process and analyze this information.

These public awareness initiatives and objectives must be directly and inherently incorporated into an LDS 2 program implementation. Also to this end, to further increase the transparency of the use of eMRTDs, ICAO recommends (1) allowing the document holder to view what is encoded on the chip (per ICAO Document 9303), and, (2) informing the public regarding what data are used, the entities with whom the data are shared, the entities that are allowed to read and write to the eMRTD, and for what purposes. All such communication should cover, among other factors, data retention, privacy protections, data integrity and access control.

4. POTENTIAL CAPABILITIES OF LDS2

Several potential eMRTD capabilities, including (1) electronic visas, (2) travel stamps, and (3) additional biometrics are available through advances in technology that allow for use of a separate eMRTD chip application. This means that governments load both the LDS1 application and one or more given LDS2 applications on the eMRTD chip at issuance. These new LDS2 applications require national policy decisions regarding: (1) whether the government's issuing authority will load the application that allows States to write data to the eMRTD; and (2) bilateral/multilateral Write Access Control agreements, data protection schemes, and distribution methods to secure the data (described in the Security Architecture section).

4.1 ELECTRONIC TRAVEL STAMPS

Travel stamps are used at border control to provide evidence that a person has legally entered a State, and in some cases, legally exited a State. Some States require that approval to enter be given in writing which must be readable by the holder. The travel stamp serves this purpose. A border control officer may examine stamps from other States to assess the risk presented by a holder, as evidence of where and when the holder has travelled, whether admission was granted, for how long and under what conditions. This information may also be used to test whether the person presenting the MRTD is the genuine holder. Non-border control bodies such as local government, health services, driving license issuers may also use the stamp to determine the holder's entitlement to services.

The inclusion of electronic travel stamps as an LDS2 application both mimics and extends the utility of traditional machine travel documents. Although travel history is readily visible in travel stamp form, there are notable shortcomings to the existing method curtailing widespread use. A casual inspection of travel stamps at points of entry reveals several interoperability challenges. These include:

- Varying fonts styles and sizes
- Unique art and layout
- Languages
- Inconsistent date formats: YYYYDDMM, MMM, DD YYYY, and DDMMMYYYY
- Differing anti-counterfeit prevention techniques
- Differing entry/exit information is implied through ink color and variations
- Placement is not always in chronological order
- Incomplete or illegible stamps

Even with standardization of the aforementioned characteristics, illegible and incomplete travel stamping of information makes the task of optical character recognition-based technology cumbersome. Border agents spend invaluable time sorting through pages to associate entry information with a visa, delaying inspection.

States will continue to use their stamps in the physical booklet, but the optional LDS2 application will standardize the content and data format for the electronic travel stamp. Protection of electronic travel stamp data through the use of cryptographic methods adds information assurance and increases the integrity of entry/exit records where use of physical travel stamping remains susceptible to counterfeit and forgery attacks.

4.1.1 Limitations

Participating States should not anticipate implementation of electronic travel stamps to supplant the need for existing border management systems or the practice of travel stamping border entry and exit. Considerations surrounding the use of the LDS2 to electronically record comprehensive travel history remain within the purview of issuing States and must be established through national policy. States should continue to physically travel stamp.

4.1.2 Comprehensiveness of Travel Records

Assuming existing border control, or travel document inspection policies and consular reciprocity agreements remain largely unchanged between States, electronic travel stamps may not necessarily contain a comprehensive list of every point of entry and exit (travelers may hold more than one type of travel document used for border crossing). For receiving States without an electronic travel stamp implementation, a physical travel stamp passage may exist without a corresponding electronic entry.
Most border control and immigration authorities already account for the entry and exit status of travelers across their borders through integrated border management systems. However, there are two important capabilities electronic travel stamps possess that are not easily resolved through existing means.

One capability pertains to disconnected operation. Should receiving States fail to properly maintain synchronization of their own border management system across all points of entry, the inspection agency would not have the information needed to validate prior entry or exit, creating confusion. A cryptographically authenticated electronic travel stamp provides States an alternate means of travel assurance assuming that the cryptographic authenticity of the electronic travel stamp can be verified during primary or secondary inspection. Even if a State is not willing to place greater trust in the electronic travel stamp than in the records in its own system, the additional information from the travel stamp can be used in a secondary inspection, which would also allow for a rigorous verification of the cryptographic authenticity of the electronic travel stamp, including online checks for the revocation status of the corresponding signature key.
A second capability is the ability to retrace and verify the authenticity of the complete travel history of the bearer on the travel document[4] across multiple States of travel at the time of inspection.

Thus, electronic travel stamps best serve to complement the integrity of existing entry and exit technologies and enhances the ability for inspecting agents to quickly verify prior travel. In cases where the bearer wishes to not disclose travel history to regions sensitive to a receiving State, one option that has been used remains the use of a separate passport issued by the bearer's issuing country or authority. This prevents unwanted association and allows travel history to be read without resorting to selective access to the travel history entries. While the use of multiple passports may provide some protection, electronically supplied data allows easier and quicker analysis than physical stamps. Such analysis could identify suspicious travel patterns from gaps in the record. This would be to the benefit of border control but not to a holder who legitimately travels in sensitive regions.

4.1.3 Collectability

A characteristic difficult to translate through electronic travel stamping is the ease of presentation and aesthetics of the travel stamped format. It is worthy to note that passport books often possess an indelible collection value to the bearer.

[4] Travel history is not necessarily comprehensive as it reflects only travel history associated with that specific travel document.

4.1.4 Electronic Travel Stamp Content

Travel stamps should follow a well-defined, structured digital format for interoperability and to deter the insertion of sophisticated virus, worm, denial of service, or other attacks against inspection systems. In addition, where large data blocks appear such as under biometric images or where variable length fields are permitted, safeguards must be taken by border management systems to identify characteristic patterns of executable code. At present, executable code is not defined by the LDS1 and should be blocked. For variable length fields, maximum allowed data lengths should be defined in the LDS2 application and enforced by the border management system's business logic.

The physical and electronic travel stamps should be as close in content as possible, including handwritten notation as applicable. The content of the electronic travel stamp may include, but is not limited to:

- Type of stamp (entry, exit, other)
- Visa approvals, refusals, and revocations as applicable (not all border crossings require visa)
- Destination State
- Travel date
- Inspection authority
- Inspection locale
- Inspector reference
- Authenticity token
- Result of inspection
- Mode of travel
- Duration of stay
- Conditions holder is required to observe whilst in issuing State

4.1.5 eMRTD Data Storage Considerations

Chip storage capacity limits the number of travel history entries that can be stored. Depending on whether entries are cryptographically authenticated by receiving States, the number of entries may fall short or exceed the number of booklet pages in the eMRTD. The vital difference is whether digital certificates to perform validation are contained in the LDS2 and how travel history shall be treated by issuing States during its use.

Ultimately, the issuing State of the travel document is responsible for establishing whether travel history is a dispensable attribute of the document and must communicate that as such to inspection terminals. At a minimum, if travel stamps are digitally signed, ICAO should expect inspection systems to only attest to their own activity, given foreign States do not possess the authority to vouch for the credibility of other States.

If travel history becomes a basis for future determination of immigration admissibility and future interoperability with trusted traveler programs, travel stamps should not be deleted. This requirement limits the number of travel stamps and visas that can be programmed to the chip. Unlike inserting new physical pages into the eMRTD for new visas and stamps, the chip at present does not support memory expansion.

A compromise mechanism exists for digitally signed entries by allotting a fixed pool of travel stamp validation certificates in the LDS. All travel entries will be retained with references to which certificate is to be used for validation. Newer certificates can be added indefinitely as older certificates get overwritten. The PKD can distribute travel stamp certificates between States. Primary or secondary inspection stations may access this list if they wish to further validate travel stamps if the referenced certificates are no longer in the LDS2.

Mechanisms for data compression should be further investigated, but such techniques provide marginal results when dealing with small data files.

4.2 ELECTRONIC VISAS

Electronic visas recorded in the LDS2 must comply with data element requirements defined in ICAO 9303 Part 2, Machine Readable Visas, to mimic current capability and functions. Currently, visa and travel records are placed in the passport as a travel stamp or a label. Many visas are issued as a label with a separate MRZ, which has to be scanned in addition to the MRZ of the travel document. Automated retrieval of this information from the chip has the potential to speed up the processing. Non-border control bodies such as local government, health services, driving license issuers may also use the visa to determine the holder's entitlement to services.

In instances where electronic visas are used, the content of the electronic visa may include, but is not limited to:

- Issuing State
- Document Type
- Place of issuance
- Valid from
- Valid until
- Number of entries
- Document number
- Type/class/category
- Additional information (endorsements: duration, limitations, and fees paid)
- Name (full name)
- Primary Identifier (surname)
- Secondary Identifier (given name)
- Passport number
- Sex
- Date of Birth
- Nationality

Given that multiple electronic visas from multiple States shall coexist in the LDS2; mechanisms for independently storing, indexing and authenticating them are necessary. The electronic visa must be stored in the LDS2 application for the duration of its validity period. Following visa expiration, the issuing State should rely on its own systems to reconcile prior visa issuance for re-application.

To prove the authenticity of electronic visas through the LDS2, the State's visa issuing authority should digitally sign electronic visas to allow the State's receiving authority to validate the authenticity of material issued by a consulate. A separate authentication mechanism should be established to prevent misuse of this information and to verify that the content was written by an approved or authorized entity.

Electronic visa pages should be written only once to the LDS2 and read many times. Access rights to add an electronic visa should be restricted to authorized systems for official use only. To support this, a form of Terminal Authentication is warranted to prevent storage denial attacks. Data protection methods should be used to prevent loss of data.

4.3 ADDITIONAL BIOMETRICS

The approach of LDS1 to aid the verification of the holder of a document is the use of (machine-assisted) biometrics. Therefore, the LDS1 stores as a primary biometric identifier a facial image of the holder and as secondary (optional) identifiers, such as fingerprints and / or irises. Since the secondary identifiers are optional, many countries chose not to implement them. Additionally, in some countries implementing secondary biometrics with the (mandatory) storage of secondary biometrics was and remains a contentious issue.

Meanwhile, advances in automated border clearance systems have allowed for additional biometric identifiers to be used in frequent / trusted traveler programs. Nationally sponsored trusted traveler programs seeking to integrate with the eMRTD presently treat the LDS1 as an identifying token. Currently a traveler must enroll in these programs separately and the biometrics are stored independently for each program, resulting in multiple copies of the biometrics outside the direct control of the traveler.

An alternative to this scheme is the option to store (additional) biometrics on the passport after issuance. This enables states to issue passports without (potentially contentious) secondary biometrics, while at the same time offering the benefits of faster border clearance supported by biometrics, if the holder chooses to enroll. Compared to separate enrollment at each border, storage of the biometrics on the passport benefits privacy (data only in the possession of the passport holder) and offers better convenience since enrollment is only necessary once.

With the storage of additional biometrics on the eMRTD, it becomes possible to enroll and verify at one station and use them at another border station. Since the biometric identifiers can be stored at the request of the holder and remain on the chip in the control of the holder, this approach might prove less contentious than the mandatory storage of secondary biometrics for all document holders. Writing to the chip post issuance and reading additional biometrics (which is considered to be sensitive information) must be access controlled.

Although States may choose to independently issue supplemental travel documents, this approach as a whole works in contradiction to ICAO eMRTD goals. Travelers are inconvenienced because they must organize, store, and present separate travel documents for each State of travel increasing risk of document loss or theft. Expedited inspections are hampered as inspection agents may need to handle multiple documents for some travelers.

The goal of interoperability is set to:

- Enable inspection systems to quickly verify the authenticity of the passport.
- Enable inspection systems to verify the identity of the bearer.

The second goal is usually accomplished using biometrics, either “manual” biometrics, i.e., comparing the imprinted displayed portrait by the inspection officer, or by automated biometric verification. The primary interoperable biometric feature of the eMRTD is the digitally stored facial image.

In some use cases, such as automated border gates or trusted traveler programs, it is desirable to have other biometric features available, e.g., fingerprints. The current LDS1 acknowledged this by offering data groups for storage of fingerprints and iris. Biometrics other than facial images are often considered intrusive for privacy reasons. The drawback of LDS1 is that the holder or the issuer of an eMRTD has to decide at time of application to a new travel document whether to store secondary biometrics.

The purpose of the LDS2-application is to enable the eMRTD holder to allow loading of additional biometrics onto the document post issuance to facilitate faster and more convenient border crossing. Thus, the decision about secondary biometrics is moved from the issuing State to the holder, which is

advantageous in the public discussion about the privacy aspects of secondary biometrics. This option should lead to increased use of machine-assisted biometric verification, especially of frequent/trusted travelers, leading to expedited border clearance for travelers.

4.3.1 Content Governance

The adoption of additional biometrics content to a LDS2 use case should not be interpreted as an effort by ICAO to consolidate data requirements between trusted traveler programs or other systems using additional biometrics. In the context of the specification of LDS2 interoperable data formats have to be defined. This includes unique descriptive headers as well as storage formats for the biometrics itself.

Read and write access to additional biometrics must be granted only to trusted inspection systems, since biometrics are considered sensitive data. Issuing countries must be able to grant and revoke access to additional biometrics by receiving States, globally and individually for each State. It must be possible to grant access on a "per-biometric-basis," i.e., access to additional biometric identifier 1 does not automatically imply access to biometric identifier 2. This allows the issuing State to decide who has access to a biometric which the holder has chosen to put on the eMRTD.

4.3.2 Security of Additional Biometrics

Access to additional biometrics beyond those standardized for global interoperability, i.e., facial image, should be granted only to authorized terminals. This is analogous to the necessity for enhanced access control mechanisms for eMRTD. A security mechanism analogous to that described in 4.2. Electronic Visas must be devised and implemented to prove authenticity of additional biometric data elements

5. PLATFORM CONSTRAINTS

Chip platforms today are capable of nearly infinite configuration variations, applications and use cases in the context of a portable low cost electronic vault. Equally, there exists a limitation of platform resources in terms of execution speed, storage, and security policy set at the time of issuance. In determining any new functionality associated with the LDS2, the following platform constraints need to be considered.

5.1 DATA STRUCTURE AND RETRIEVAL

The size of data files being created and appended over the lifetime of the travel document requires careful consideration. Chip storage capability is finite and data to be recorded to the chip over a lifetime needs to be manageable. A practical approach to memory management should be considered when determining new functionality. In particular, the determination of whether the data to be stored are of time limited value or lifetime value can play a role in implementing a linear file structure.

5.2 EXECUTION TIMES

The setting of security conditions in a given transaction is not considered to significantly affect execution times. The size of the data in the transaction, however, plays a significant role in any given read or write transaction time. This is of particular importance where data written to the chip must be digitally signed after each transaction. Careful consideration to minimizing data volume transaction times should be taken when implementing any new use cases. Digitally signing individual transactions for subsequently writing to the chip platform will be more efficient than digitally signing the entire file structure to be appended with a given transaction.

5.3 OTHER PLATFORM CONSTRAINTS

The chip platform by design is a passive device. This means that the chip will only react once an outside influence initiates a transaction. The chip platform can never actively start a transaction without an external request.

As a passive device, the chip platform has no internal time base (real time clock). Therefore, time stamping integrity of a given application must be maintained by the host system, and then only after an authorized authentication with the chip platform.

6. SECURITY AND PRIVACY ARCHITECTURE

6.1 APPLICATION-SPECIFIC SECURITY CONTEXT

As the chip provides multiple applications, the security context must be established in the Master File. Support for **Supplemental Access Control (SAC)** as specified in [4] is mandatory. The access control mechanism for any new LDS2 application shall be based on a public key infrastructure. The details for the access control mechanism are specified in cooperation with NTWG as approved by the TAG.

6.1.1 LDS1 Backward Compatibility

Basic Access Control must be supported for backward compatibility as long as BAC remains part of the standard for LDS1 documents.

6.1.2 LDS1 Use Cases

Data groups 1-16 stored in LDS1 are defined as elementary files according to Doc 9303. The signed Document Security Object contains the hash values of all data groups stored on the chip. As a consequence these data groups are static, i.e., they are written at the time of personalization and must not be changed afterward.

Read access to all data groups is protected by SAC (as noted above, consequent to full backward compatibility, for the transitional period Basic Access Control may also be used). Data groups 3 (Fingerprints) and 4 (Iris) are considered sensitive and should be additionally protected against unauthorized read access. This additional access control mechanism should be based on a public key infrastructure.

6.1.3 New LDS2 Use Cases

The LDS2 will store rewritable and/or appendable data; the exact content and format of the data are specified in cooperation with NTWG as approved by the TAG.

Writing data to an LDS2 application implies signing the data to guarantee its authenticity and integrity. Furthermore, the chip itself should verify that the signature is valid before writing the data to the file.

Both read and write access to the chip are protected, so that only authorized inspection systems can access data within the application. See Table 2 Access Rights under LDS2.

6.1.4 Access Conditions

It is required that all personal data of the travel document be protected to the current Document 9303 levels or greater. The policy for various access scenarios must be controlled and maintained by the issuing country. Access conditions for Read only, Read/Write, or Append (update) files can serve to differentiate between the issuing State, the receiving State, and non-governmental organizations (airlines, airport security, etc).

6.1.5 eMRTD Life Cycle considerations

It is anticipated that the issuing States determine exact configuration of the eMRTD (i.e., loading of LDS2 applications) at time of issuance; post issuance loading of applications is not recommended. It

is expected that any subsequent addition of a State-specific application or functionality[5] separate from LDS2 would require a re-issuance of the travel document to maintain integrity.

6.1.6 Separation of Chip Applications

The existing LDS1 application must clearly be separated from any other new functionality or application associated with LDS2. The LDS1 version should be considered as a separate chip application (AID) from any new LDS2 applications to maintain backwards compatibility and interoperability to existing standards and infrastructure.

6.2 PUBLIC KEY INFRASTRUCTURE

A separate public key infrastructure (PKI) is required for access control to and authentication of any LDS2 data groups. The existing PKI for the verification of LDS1 data, consisting of a single Country Signing Certification Authority (CSCA) and one or more Document Signers per country, remains unchanged.

This additional PKI will consist of three levels:

Country Verification Certificate Authority (CVCA) is the national root CA of each country

- At least one Document Verifier (DV) per country that operates the inspection systems
- Sufficient 9303-compliant systems at the border to read/write eMRTDs

The public key of the national CVCA must be stored on the chip of the eMRTD and may be updated. Every inspection system or every group of inspection systems is required to store its own private keys and certificates to access data in a given LDS2 application of a received eMRTD. The chip then performs the verification of the certificate chain provided by the inspection system based on the stored public key of the national CVCA. As a consequence any State that wants to read or write data from or to the chip requires a certificate chain that starts with a certificate verifiable by the State that has issued the eMRTD. The ICAO Public Key Directory will provide a broker service (as described below in 6.3.1) to simplify the certificate application procedure.

The private key of the inspection system is not only used for access control to data stored in a given LDS2 application, it is also used for authenticating data written to the LDS2 application of the chip.

6.2.1 Access Control

The certificate issued to an inspection system shall describe the read/write access rights of that terminal to the data stored in the LDS2 application, but may also describe read access to sensitive data (e.g., fingerprints and iris) in the LDS1 application.

6.2.2 Data Authentication

All data written to the LDS2 application must be signed by the inspection or visa issuance system storing the data on the chip. This allows verification of the authenticity of the data and prevents storing invalid data.

6.2.3 Card Verifiable Certificates

Access control and signature verification have to be performed by the chip, therefore, the public key certificates have to be validated by the chip itself. Due to the computational restrictions of those chips, a simplified certificate format is used instead of X.509 certificates, i.e., card verifiable certificates.

[5] ICAO Doc 9303 Part 1 Vol 2 Section III, Appendix A.10.3

6.3 ICAO PUBLIC KEY DIRECTORY

The ICAO public key directory serves as a repository for Document Signer Keys and Master Lists [3]. Participation in the PKD (for LDS1) is strongly recommended.

However, to make use of an LDS2 application, participation in the PKD is required as the additional Broker Service and CV Certificate publication cannot be replaced by a non-automated mechanism such as diplomatic means.

6.3.1 Broker Service

Any State that wants to read biometric data or write any data to an LDS2 application must apply for a certificate at the issuing State of the eMRTD according to the access rights contained in Table 2 Access Rights Under LDS2. To support the certificate application procedure, the PKD provides a broker service that interconnects the CVCA of eMRTD issuing States with the DVs of eMRTD reading States.

While the broker service is not a requirement from a technical perspective, it has a number of process and border management advantages. The broker service not only simplifies the discovery of CVCAs and DVs, it also monitors the whole certificate application procedure and checks the format of received requests and resulting certificates according to standardized criteria.

6.3.2 Publication of CV Certificates

For the verification of signed data written to an LDS2 application of the chip, the certificate chain starting at the public key of the national CVCA of the eMRTD issuing State and ending at the certificate of the inspection system is required. While this certificate chain is already provided by the inspection system to the eMRTD chip as part of access control, it is not stored on the chip to save resources on the chip. For an external verification of the (signed) data written by the inspection system to the chip, the certificate chain must be retrieved from a directory.

As the certificate application and issuing procedure is performed by the broker service of the ICAO PKD, storing and retrieving the certificate chain corresponding to data written by a certain inspection system is straightforward.

6.3.3 Revocation of CV Certificates

The concept of invalidating certificates after issuance by revocation is usually not employed for CV certificates as the chip itself would have to perform this verification. Instead CV certificates may be issued with short validity periods.

In contrast, the validation of long term signed data stored in an LDS2 application of the eMRTD chip requires the availability of the status of published CV certificates. The ICAO PKD will therefore also provide corresponding revocation information.

7. CONCLUSION

The LDS Sub-Working Group of the New Technologies Working Group affirmed that the current LDS1 should not be modified. Rather, the identified "bug fixes" and clarifications should be incorporated and maintained. Changes with any new LDS2 use cases will focus on the writing or appending of data by other States. Such updates would occur after issuance. New LDS2 use cases will be separate and individual chip applications and will not impact the existing LDS1 application.

Post issuance loading of any LDS2 applications is not foreseen. It is anticipated that the issuing countries determine exact configuration of the electronic passport at time of issuance, and that that any subsequent addition of an LDS application or functionality would require a re-issuance of the travel document to maintain integrity. The policy for various access scenarios to update data to the chip must be controlled and maintained by the issuing country.

ANNEX A: TERMS AND DEFINITIONS

Within this document, the reader may encounter various terms and abbreviations with which they may not be familiar. A list of abbreviations is offered below for clarification. The following terms are defined with respect to MRTDs and were obtained from ICAO references.

Active Authentication – Explicit authentication of the chip requiring processing capabilities of the MRTD's chip. The active authentication mechanism ensures that the chip has not been substituted, by means of a challenge-response protocol between the inspection system and the MRTD's chip.

AID - The chip Application Identifier

Advance Passenger Information (API) – Involves the capture of a passenger's travel document data and other flight details such as name of the carrier, arrival and departure points. This data is transmitted by electronic means to public authorities for risk management purposes prior to arrival in order to expedite clearance. API can also act as a decision making tool that Border Control Agencies can employ before a passenger is permitted to board an aircraft.

Application – Under ISO/IEC 7816-4 on Identification Cards and Integrated Circuit Cards, an application gives structure, data elements, and program modules needed for performing a specific functionality.

Authorized Receiving Organization: Organization authorized to process an official travel document (e.g., an air carrier) and as such, allowed to record details in the optional capacity expansion technology.

Automated Border Control system – An automated system which authenticates the eMRTD, establishes that the passenger is the rightful holder of the document, queries border control records, then automatically determines eligibility for border crossing according to pre defined rules.

Basic Access Control (BAC) – Challenge-response protocol where a machine (RF) reader must create a symmetric key in order to read the CONTACTLESS chip by hashing the data scanned from the MRZ.

Biometric – A measurable physical characteristic or personal trait used to determine the identity, or verify the claimed identity, of an enrolled individual.

Biometric Data – The information extracted from the biometric sample and used either to build a reference template (template data) or to compare against a previously created reference template (comparison data).

Biometric Sample – Raw data captured as a discrete unambiguous, unique, and linguistically neutral value representing a biometric characteristic of an enrollee as captured by a biometric system (for example, biometric samples can include the image of a fingerprint as well as its derivative for authentication purposes).

Certificate Revocation List (CRL) – List issued by ICAO member States to revoke any of its certificates or to signify that no such revocations exist for any of their certificates.

Common Biometric Exchange Formats Framework (CBEFF) – Defines a basic structure for standardized biometric information records.

Capture – The process of taking a biometric sample from the user.

Contactless Integrated Circuit – the data carrying unit incorporated into the MRTD, consisting of an integrated circuit or microchip and an antenna.

Country Signing Certificate Authority (CSCA) – The Certificate Authority for a Participant that is responsible for managing the Country Signing CA Certificate (CCSCA) used to sign all State Document Signer Certificates (CDS). The CSCA is the highest trust authority for the Participant in the context of the ICAO PKD.

Country Verifying Certification Authority (CVCA) – Determines the access rights to its MRTD chips for all DVs (i.e., its own DVs as well as the DVs of other States) by issuing certificates for DVs entitled to access some sensitive data.

Data Group (DG) – A series of related Data Elements group together with the Logical Data Structure.

Doc 9303 – The ICAO standards publication that defines specifications for MRTDs which allow compatibility and global interchange using both visual (eye readable) and machine readable means.

Document Signer (DS) – A body which issues a biometric document and certifies that the data stored on the document is genuine in a way which will enable detection of fraudulent alteration.

Document Verifier (DV) – An organizational unit that manages inspection systems belonging together (e.g., inspection systems operated by a State's border police) by issuing Inspection System Certificates. The DV is a CA, authorized by the national CVCA to issue certificates for national inspection systems.

Electronic Identity Document (eID) – Official electronic proof of one's identity issued by a State.

Electronic Visa – An LDS2 application that allows recording of visa information to the eMRTD chip; it does not refer to a visa with a chip, which is prohibited under current ICAO specifications, nor does it refer to electronic travel authorizations that do not include writing data to the chip.

Electronification – Providing option for electronic storage of visa and entry-/exit travel stamps on the eMRTD chip as well as further refinement/support of the verification process.

Extended Access Control – EAC – Protection mechanism for additional biometrics included in the MRTD. The mechanism will include State's internal specifications or the bilateral agreed specifications between States, sharing this information.

Enrollment – The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's physical being.

Enrollee – A human being assigned an MRTD by an Issuing State.

Electronic Passport (ePassport) – An MRTD passport that has a contactless integrated circuit chip embedded in it, in accordance with ICAO standards.

eMRTD – An MRTD with an contactless IC (chip) embedded which is designed and the mandatory data stored, according to ICAO standards, in order to facilitate identity verification via either a manual or automated process

eMRTD Assisted Border Clearance – A system which assists the border control officer to authenticate the eMRTD via the use of a suitable document reader, establish that the passenger is the rightful holder of the document and query border control records. The officer himself determines eligibility for border crossing"

Functionality – Under ISO/IEC 9126, functionality is a set of attributes that bear on the existence of a set of functions and their specified properties.

Global Interoperability – the capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye readable and machine readable data in all MRTDs.

Hash – A number generated from a string of text using a formula to ensure that a message has not been tampered with. The sender generates a hash of the message, encrypts it, and sends it with the message itself. The recipient then decrypts both the message and the hash, produces another hash from the received message, and compares the two hashes.

Holder – A person possessing an MRTD, submitting a biometric sample for verification or identification whilst claiming a legitimate or false identity. A person who interacts with a biometric system to enroll or have his/her identity checked.

Identifier – A unique data string used as a key in the biometric system to name a person's ***identity*** and its associated attributes. An example of an ***identifier*** would be a passport number.

Identity – The common sense notion of personal identity. A person's name, personality, physical body, and history, including such attributes as nationality, educational achievements, employer, security clearances, financial and credit history, etc. In a biometric system, ***identity*** is typically established when the person is ***registered*** in the system through the use of so-called "breeder documents" such as birth certificate and citizenship certificate.

Identification/Identify – The one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the MRTD holder whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity. Contrast with 'Verification'.

Integrated border management system – This represents the interoperability between multiple systems to allow for the facilitation and security of the border process.

Image – The digital representation of a biometric as typically captured via a camera or scanning device.

Inspection – The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity.

Issuer Data Block – A series of Data Groups that are written to the optional capacity expansion technology by the issuing State or organization.

Issuing State – The country issuing the MRTD and writing the biometric to enable a Receiving State (which could also be itself) to verify it.

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 the MRTD).

Machine Assisted Document Security Verification (MADV) – Use of the RF chip in the eMRTD to provide machine authentication of the travel document. ICAO Doc 9303 currently distinguishes three main categories of machine-verifiable security features: structure features, substance features, and data features.

MRTD – Machine Readable Travel Document (e.g., passport, visa). 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.

MRZ – Machine readable zone. The area on a passport containing two lines of data (three lines on a visa) that are printed using a standard format and font.

MRV – Machine Readable Visa

Passive Authentication – Verification mechanism that does not require processing capabilities of the chip in the MRTD. Passive authentication proves that the contents of the Document Security Object (SOD) and LDS are authentic and not changed. It does not prevent exact copying of the chip content or chip substitution.

Passenger Name Record (PNR) – A record in a computer reservation system database used in the travel industry that contains all the relevant information related to the passenger's journey. The amount and nature of the information held may vary between industry members. A PNR may contain details such as passenger name, address, telephone numbers, ticketing information, and travel itinerary.

Password Authenticated Connection Establishment (PACE) – An asymmetric cryptography protocol created by the German Federal Office for Information Security. It comprises four steps: (1) the chip randomly chooses a random number, encrypts it with a password-derived key and sends the encrypted random number to the terminal, where it is recovered; (2) both the chip and the terminal use a mapping function to map the random number to parameters for asymmetric cryptography; (3) the chip and the terminal perform a Diffie-Hellman protocol based on the parameters generated during step 2; (4) the chip and terminal derive session keys, which are confirmed by exchanging and checking the authentication tokens.

Public Key Directory (PKD) – The ICAO PKD is the central platform to manage the world wide exchange of certificates and certificate revocation lists. Those certificates and certificate revocation lists are used to validate the electronic signature of data contained in the RFID chip of e-Passports and other eMRTD. The PKD content is pre-validated and can be downloaded for free.

Public Key Infrastructure (PKI) – Data encryption trust hierarchy that helps to ensure data privacy, security, and integrity.

Receiver Data Block – A series of Data Groups that are written to the optional capacity expansion technology by a receiving State or authorized receiving organization.

Receiving State – The country to which the MRTD holder is applying for entry.

RFID – Radio-frequency identification

Secure Signature Creation Device (SSCD) – Secure hardware device for signature generation.

SOD – (Document Security Object) on the chip, containing a hash representation of the LDS contents to ensure data integrity.

State – A country that issues MRTD, and/or inspects MRTDs at its border.

Supplemental Access Control (SAC) – An optional access control mechanism, based on Password Authenticated Connection Establishment, which is supplementary to Basic Access Control.

Template / Reference Template – Usually condensed and vendor-specific data, which represents the biometric measurement of an enrollee, used by a biometric system for comparison against subsequently submitted biometric samples.

Travel Continuum – Encounters that occur between travelers and border, immigration and passport issuing authorities. The continuum begins with issuance of a travel document and continues through the visa application process, inspection at the port of entry, adjudication of immigration benefits, issuance of immigration documents, enforcement of immigration law, and departure. Not all travelers participate in each phase. However, biometric and biographic information should be accessible to decision-makers during encounters along continuum to support the fundamental functions of reliable identity verification of legitimate travelers and screening for persons of interest against watch lists and other biometric repositories.

Trusted Traveler Program – A program that allows pre-assessed low-risk travellers expedited passage through an automated border control system following successful background checks and the recording of biometric data. Such programs provide expedited travel through dedicated lanes and kiosks.

Verification/Verify – The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. Contrast with 'Identification'.

Visual Inspection Zone (VIZ) – Those portions of the MRTD (data page in the case of MRP), i.e., front and back (where applicable), not defined as the MRZ.

ANNEX B: CASE STUDIES

ELECTRONIC TRAVEL STAMPS

- **PROs**:
  - Extended automation of eMRTD inspection during (automated) border control to be coupled with a local risk assessment devised from Advance Passenger Information/ Passenger Name Record (API/PNR) data.
  - Improved security offered by a signed electronic record over an ink stamp.
  - Security is enhanced by presence of a signed electronic record.
  - Having access to electronic travel records may prove useful when adjudicating a visa application.
  - Having access to electronic travel records may prove useful when determining admissibility.
- **CONs:**
  - Traditional travel stamping is commonly carried out during the process of interviewing travelers at border control; in those cases, electronic travel stamping may not offer improvements on transit times.
  - There are legislative and civil liberty challenges as this gives States a relatively easy means of monitoring people's travel across other States' borders.
  - Storage space is required for electronic travel stamp on the chip.
- **RATIONALE:** In principle, all of today's travel stamps could also be photocopied with no traveler recourse, obviating the previous objection.
- **EMPOWERMENT:** Need to define the size of each entry; usage will not be universal or fail proof, unless e-stamping becomes the standard.

ELECTRONIC VISAS

- **PROs:**
  - Supports the use of e-gates and automated border clearance systems for visitors requiring visas and allows visas to be checked offline.
  - Security is enhanced by presence of a signed electronic record.
  - Offers opportunity for remote renewal or re-issue of a visa where the holder and passport are already known to the issuing State.
  - Having access to electronic travel records may prove useful when adjudicating a visa application.
- **CONs:**
  - Does not withstand complexity or exception handling, and may be superseded by electronic data base driven e-visas solutions (e.g., via secure Internet, APP in Australia).
  - Storage space is required for visas on the chip.

- **RATIONALE:** Biometric visa procedures including ten fingerprint and face collection have been implemented in a few States. Thus, database records are already in place, involving (1:1) verification during border crossing to avoid last minute ID substitution of visa holder (e.g., look-alike), as well as possibly additional last minute (1:many) search for most recent threat assessment.

- **EMPOWERMENT:** See previous case.

ADDITIONAL BIOMETRICS

Additional biometrics would be added to the LDS2 application after issuance of the eMRTD either by a third party (trusted traveler program) or by the issuing country after issuance of the eMRTD and before expiry.

- **PROs:**
  - Integrate additional, secondary biometrics for trusted traveler programs which could be used by different installations provided that the enrollment procedure is trusted.

- **CONs:**
  - Relies on third party to secure the biometric data.
  - Storage space is required for additional biometrics on the chip.

- **RATIONALE:** Where a State does not have a mandatory secondary biometric, this provides the means for storage of such at the holder's discretion.

- **EMPOWERMENT:** Need to define the size of each entry; due to the size of biometrics stored as images as required by ICAO only a few additional biometrics might be stored on the chip.

ANNEX C: CURRENT AND FUTURE USE OF ELECTRONIC PASSPORTS QUESTIONNAIRE AND RESPONSE SUMMARY

Current and Future Use of Electronic Passports Questionnaire

SECTION 1: FOR GOVERNMENT USE

Organization:

Contact Person Name and email:

1. Is your country currently issuing ICAO-compliant ePassports? Yes / No

2. Indicate your current use of ePassports?
   _____ Manned border clearance
   _____ Automated border clearance
   _____ Other (Please explain)

3. What is your anticipated use of ePassports?
   _____ Manned border clearance
   _____ Automated border clearance
   _____ Issuance or verification of electronic visas
   _____ Record travel information
   _____ Other or None (Please explain)

Below is the current list of the LDS data groups. Some are currently active, and others are reserved for future use.

DG 1 - Details recorded in MRZ	DG 11 - Additional personal details
DG 2 - Encoded face	DG 12 - Additional document details
DG 3 - Encoded finger(s)	DG 13 - Optional details
DG 4 - Encoded eye(s)	DG 14 - Security options for secondary biometrics
DG 5 - Displayed portrait	DG 15 - Active authentication public key information
DG 6 - Reserved for future use	DG 16 - Person to notify
DG 7 - Displayed signature, mark	DG 17 - Automated border clearance
DG 8 - Data features	DG 18 - Electronic visa(s) - for future use
DG 9 - Structure features	DG 19 - Travel record(s) - for future use
DG 10 - Substance features	

4. Of those that are currently active, which are you not currently using? (Please explain)

5. Of the data groups that you are not currently using, which would you eliminate? (Please explain)

6. Which data groups do you envision using in the future? (Please explain)

7. As an issuing country, would you consider allowing another country to write to your ePassport chip for the following purposes:
   _____ Manned border clearance
   _____ Automated border clearance
   _____ Issuance or verification of electronic visas
   _____ Record travel information
   _____ Other circumstances (Please explain)

Current and Future Use of Electronic Passports Questionnaire

SECTION 1: FOR GOVERNMENT USE (continued)

8. If yes, what security controls would you consider requiring? (Please explain)

9. If you would not consider allowing another country to write to your ePassport, please explain why.

10. As a receiving country, would you consider writing to an issuing country's ePassport chip for the following purposes:
    _____ Manned border clearance
    _____ Automated border clearance
    _____ Issuance or verification of electronic visas
    _____ Record travel information
    _____ Other circumstances (Please explain)

11. If yes, what security controls would you consider requiring? (Please explain)

12. If you would not consider allowing another country to write to your ePassport, please explain why.

Current and Future Use of Electronic Passports Questionnaire

SECTION 2: FOR NON-GOVERNMENT USE

Organization:

Contact Person Name and email:

While you do not need to answer the Government Use questions above, reading them may help you to think about your answers to the questions below.

1. How do you currently use features of the ePassport?

2. What features would you be particularly interested in developing for your use or the holder's use?

3. How would you use them?

4. What would be the benefit to:
    a) Your organisation
    b) Holder of the passport
    c) Others

Summary of Responses

Nine government entities completed the questionnaire; plus one partial response. Three non-government entities submitted responses. A summary of responses follows.

Government Responses:

Issuance and Use of ePassports: All countries that responded are issuing ICAO-compliant ePassports. The ePassports are currently used for both manned (six countries) and automated border clearance (ABC). Seven countries responded that their ePassports are used for ABC – this includes use with the issuing country's ABC gates as well as with other countries' ABC gates. Two additional countries anticipate use for ABC; three countries indicated they would consider recording visa information in ePassports; two may record travel information.

Use of LDS Data Groups: Only the mandatory data groups (DG1 and DG2) are used by all respondents; DG4 (iris), DG6 (reserved for future use) and DG17-19 are not used by any respondents. For future use, several respondents indicated they may use DG3 and DG4 to record additional biometrics, DG14 to protect the additional biometric data, DG7 for displayed signature, and DG18 and 19. One country would consider recording of health vaccination information of the bearer and registered/ trusted traveler enrollment information.[6] Outside of the questionnaire, some NTWG participating States have considered recording information on blood type, marital status, tax status, religion, and parental data for children traveling alone.

LDS version 2.0 – Allow other countries write access to issuing country's ePassport: One country would consider allowing other countries to write to its ePassports; with chip partitioning to protect original data. Other respondents would not allow writing, but identified controls including virus protection, write-only access (no update/modify), and terminal authentication using secured access module (SAM).

LDS version 2.0 – Write to another country's ePassport: Three countries would not consider writing to another ePassport for any reason; three countries would consider recording border clearance data (DG 17); one would write visa information to the chip (DG18) or record travel information (DG18). One country's ePassport issuing authority indicated it have discussed a "limited write" model, which would involve authorizing its country's border control officials to write arrival/departure information to the ePassport and allowing other countries to read that information protected via Basic Access Control/Password Authenticated Connection Establishment.

Non-Government Responses:

Use of ePassports: Qantas Airways plans to issue smart card to frequent flyers to serve as a boarding pass and permanent luggage tag. Respondent encouraged the NTWG to look at what airlines are doing to facilitate travel and maximize use of ePassport for commercial operators and border control. Passports are used for travel and authentication of the holder both within and outside the Schengen area. Future uses identified include: automated border clearance; renewal of expired ePassport with self-service kiosk; use at hotels for identity verification; watch list checks; and ensure one passport/one person through use of automated fingerprint identification systems to detect duplicate and fraudulent applications.

Additional features respondents would be interested in developing: Check-in for airline boarding pass; airport lounge and purchase of goods at airport, self-service check in at hotel.

---

[6] Some States require traveler to present a valid Yellow Fever Vaccination Certificate to immigration inspector in cases where the traveler has been or passed through any country where yellow fever is endemic.