For Publication on the ICAO Website

Roadmap for Implementation of New Specifications for MRTDs

DISCLAIMER: All reasonable precautions have been taken by the International Civil Aviation Organization to verify the information contained in this publication.
However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall the International Civil Aviation Organization be liable for damages arising from its use.
This publication contains the collective views of an international group of experts and does not necessarily represent the decision or the policies of the International Civil Aviation Organization.

Version: Release 1

April 2016

File: Roadmap for Implementation of New Specifications for MRTDs – Release 1 Final 2016.doc

Author: ISO/IEC JTC1 SC17 WG3/TF1 for the New Technologies Working Group (NTWG), Working group of the ICAO Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP).

Release Control

Release	Date	Description
Release 1	2016-04-01	Finalized for first public release

Table of contents

1 Introduction

Travel documents are constantly evolving. The effectiveness of these advancements is however directly tied to the application of existing or new security features and/or specifications. As such, it is critical that all pertinent stakeholders involved in the production, use and inspection of these documents are aware of and/or are configuring their systems to fully leverage any security and facilitation advantages offered by new or enhanced international specifications.

The introduction of new travel document technologies is a gradual learning process that requires adaptation from the organizations that issue these documents, as well as those that use them and supporting systems to effectively manage travellers at points of entry and departure. Ensuring that all affected systems and processes are effectively modernized is needed if States are to fully benefit from improved document functionality. More specifically, new reading systems, new storage media, and new measures that are required to protect privacy and ensure data integrity and interoperability must all be addressed.

Implementation practices that come within the scope of Doc 9303 and Technical Reports endorsed by the TAG/TRIP show that just the publication of new material is not always sufficient. More guidance is needed on the implementation strategy to be followed by implementers of both inspection systems and MRTDs.

1.1 Roadmap

This Roadmap has been developed to bring awareness to key advancements to travel document specifications, and ultimately support the introduction of new specifications. It should be envisaged that the roadmap does not impose additional specifications; it must be respected as guidance only.

The Roadmap will be published on a regular basis, and will be made available through a range of channels.

This Roadmap provides information on the implementation issues of new specifications. It consists of:

- (Backwards compatibility) consequences for MRTDs and systems;
- Additional pre-requisites to be met before implementation (such as test specifications);
- The path to be followed by States and implementers;
- Timetables (planning diagrams) for updating inspection systems, overlap period with respect to issuing new features in MRTDs, time period in which both ‘old’ and ‘new’ MRTDs will be in circulation, and timing when ‘old’ specifications become deprecated.

1.2 Communication

At a minimum, the following communication channels for the Roadmap are foreseen:

- ICAO website;
- ICAO TRIP Platform;
- The ICAO TRIP Magazine (formerly the ICAO MRTD Report);
- ICAO TRIP Symposia (formerly ICAO MRTD Symposia);
- ICAO Regional Seminars; and
- Meetings of the TAG/TRIP, NTWG, ICBWG, and PKD Board.

In addition to distribution through these channels, the ICAO Secretariat, with the support of ICAO TRIP working groups, will endeavour to bring greater attention to this roadmap through targeted outreach and communication to assist States with planning and transition to new travel document technologies and systems. Through these activities, key stakeholders will be better advised of international travel document specifications advancements, and will make the changes necessary to limit disruptions to air travel and customs/immigration processes.

1.3 Structure of the Roadmap

1.3.1 Roadmap composition

Apart from this introductory section each main section covers a specific set of specifications, published in Doc 9303 or an ICAO Technical Report.

The sub sections within a section describe the consequences for implementation in the areas of:

- Backwards compatibility;
- Implementation pre-requisites;
- Implementation strategy; and
- Implementation timetable.

1.3.2 Abbreviations

Abbreviation	
BAC	Basic Access Control
CA	Chip Authentication
ICAO	International Civil Aviation Organization
ICBWG	Implementation and Capacity Building Working Group
MRTD	Machine Readable Travel Document conforming to ICAO Doc 9303.
NTWG	New Technologies Working Group
PACE	Password Authenticated Connection Establishment
PKD	Public Key Directory
TAG/TRIP (ex-TAG/MRTD)	Technical Advisory Group on the Traveller Identification Programme
SAC	Supplemental Access Control
TRIP	Traveller Identification Programme

1.4 Reference documentation

The following documentation served as reference for this Roadmap:

[R1] ICAO Technical Report “Supplemental Access Control for Machine Readable Travel Documents”, V1.01, November 2010
[R2] ICAO Technical Report “Supplemental Access Control for Machine Readable Travel Documents”, V1.1, April 2014
[R3] ICAO Technical Report “RF protocol and application test standard for eMRTD – part 3”, V2.07, October 2014
[R4] ICAO Technical Report “LDS and PKI Maintenance”, V1.0, May 2011
[R5] ICAO Technical Report “LDS and PKI Maintenance”, V2.0, April 2014

2 Supplemental Access Control

2.1 Introduction

Two subsequent versions of a Technical Report on Supplemental Access Control have been published.

2.1.1 Technical Report V1.01 – 2010

[R1] ICAO Technical Report "Supplemental Access Control for Machine Readable Travel Documents", V1.01, November 2010 was endorsed by the TAG at its 19th meeting in December 2009 (emphasizing the final version to incorporate the result of a patent discussion). It specifies the PACE protocol containing two variants of mappings, the generic mapping and the integrated mapping.

2.1.2 Technical Report V1.1 – 2014

[R2] ICAO Technical Report "Supplemental Access Control for Machine Readable Travel Documents", V1.1, April 2014 was endorsed by the TAG at its 22nd meeting in May 2014. This is an update of the 2010 version in the sense that an optional additional mapping for the PACE protocol, the Chip Authentication mapping, has been added.

The V1.1 version of the Technical Report has been incorporated into the Seventh Edition of Doc 9303.

2.2 Backwards compatibility

The PACE protocol for chip access and communications encryption is different from the BAC protocol, which is in use in eMRTDs since 2004. The technical report specifies the use of PACE in addition to BAC instead of the use of only PACE, because inspection systems may not all support PACE yet. PACE is a recommended addition (SAC=BAC+PACE). To allow for inspection systems to implement support for the PACE protocol a conversion period has been defined by the NTWG (see 2.4 Implementation strategy).

2.3 Implementation pre-requisites

The specification of Supplemental Access Control has implications for the test framework in the RF and Protocol Tests Part 3 (Tests for Application Protocol and Data Structure). The test specifications have been extended to accommodate the new protocols in the updated [R3] ICAO Technical Report "RF protocol and application test standard for eMRTD – part 3", V2.07, October 2014.

2.4 Implementation strategy

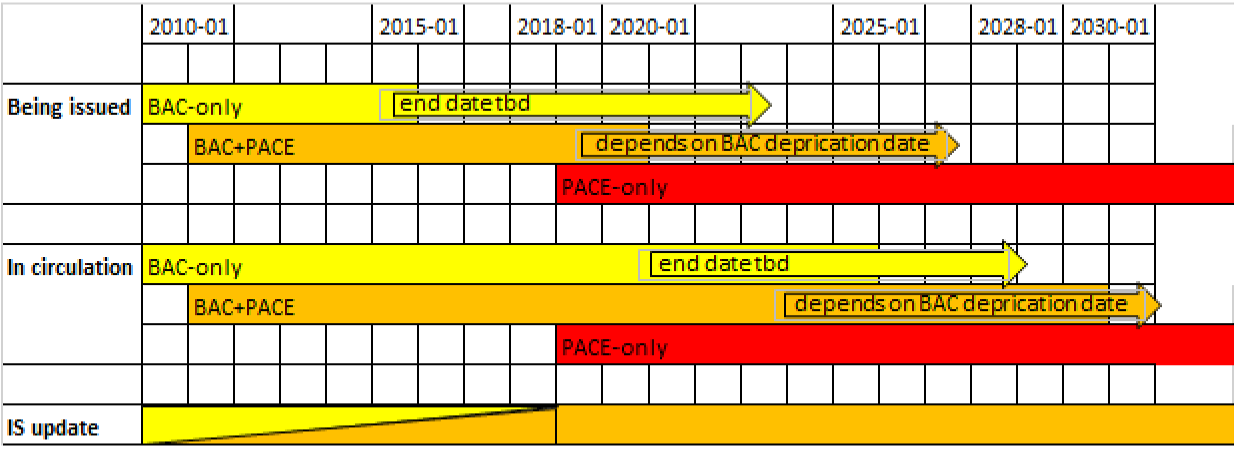
According to the outcomes of the 19th meeting of the TAG/TRIP, SAC should be implemented in eMRTDs "within a period of 5 years", which was approximately by 01 January 2015.

BAC being present on the eMRTD ensures that inspection systems that do not support PACE (yet) will still be able to access the MRTD's chip with access control. To access eMRTDs supporting only PACE, inspection systems will need to support PACE. For inspecting authorities and inspection system vendors to prepare their systems to support PACE a date has been established before which MRTDs supporting only PACE are not considered to be ICAO compliant. The chosen date should provide enough time for inspection system owners and vendors to implement the necessary modifications to their systems.

In its meeting of 19-21 February 2013 the NTWG concluded that as of the date 01 January 2018 eMRTDs supporting only PACE will be considered to be ICAO compliant.

A date for BAC to become deprecated has not been established yet. It would make sense to declare BAC deprecated once all inspection systems support PACE, which is planned to be in January 2018 according to the aforementioned conclusion of the NTWG.

2.4.1 Timetable



3 Logical Data Structure V1.8

3.1 Introduction

In its 20th meeting (September 2011) the TAG endorsed [R4] ICAO Technical Report “LDS and PKI Maintenance”, V1.0, May 2011. The Technical Report provides a revised specification for the versioning information in the LDS to be implemented in the LDS, revision V1.8.

3.2 Backwards compatibility

The change has an impact on inspection systems. These systems will need to be able to parse the SO_D V1 structure. When the EF.COM is not present, version information (both the LDS version as well as the SO_D version) can only be retrieved from the SO_D. Therefore in LDS V1.8 the change has been implemented in the SO_D whilst the EF.COM remains present.

3.3 Implementation prerequisites

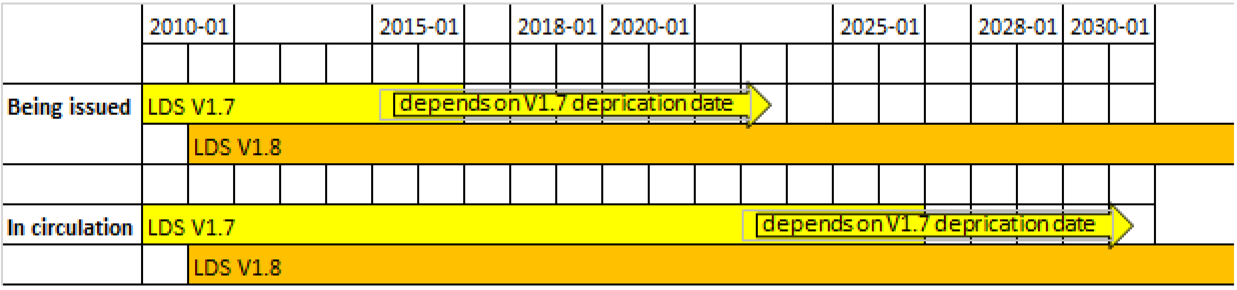
The test specifications have been extended to accommodate the LDS V1.8 specifications in the updated [R3] ICAO Technical Report “RF protocol and application test standard for eMRTD – part 3”, V2.07, October 2014.

3.4 Implementation strategy

With this change, all information present in the EF.COM has been duplicated in the SO_D. This means that the EF.COM will be removed from the specifications from the next LDS version after V1.8. Issuing States should implement this change in their MRTDs as soon as possible. Assumed is a period of 5 years from the endorsement date after which all Issuing States will have implemented LDS V1.8.

Inspection systems that rely on the EF.COM need to be modified to use the SO_D instead as soon as possible, realizing that in the next version of the LDS after V1.8 the EF.COM will be removed from the specifications and systems from then on rely on the SO_D for obtaining version information.

3.4.1 Timetable



4 Updated Certificate Profiles

4.1 Introduction

In its 22nd meeting (May 2014) the TAG endorsed [R5] ICAO Technical Report “LDS and PKI Maintenance”, V2.0, April 2014. The certificate and CRL profiles in this edition of the Technical Report integrate the inherited detailed technical requirements from RFC 5280 directly. This approach should provide an increased support to implementers as all the requirements are presented together. This version of the Technical Report has been incorporated into the Seventh Edition of Doc 9303.

4.2 Backwards compatibility

The profiles use the following terminology for presence requirements of each of the components/extensions certificates:

m mandatory - the field MUST be present
x do not use - the field MUST NOT be populated
o optional - the field MAY be present

The profile uses the following terminology for criticality requirements of extensions that may/must be included in certificates:

c critical - the extension is marked critical, receiving applications MUST be able to process this extension.
nc non-critical - receiving applications that do not understand this extension may ignore it.

The indication non-critical is an addition to the previous certificate profiles specifications.

These certificate profiles impose new requirements to the certificate issuers. From an interoperability point of view relying parties SHOULD be capable of accepting certificates that conform to the previous profile as well as the profiles specified in this Technical Report.

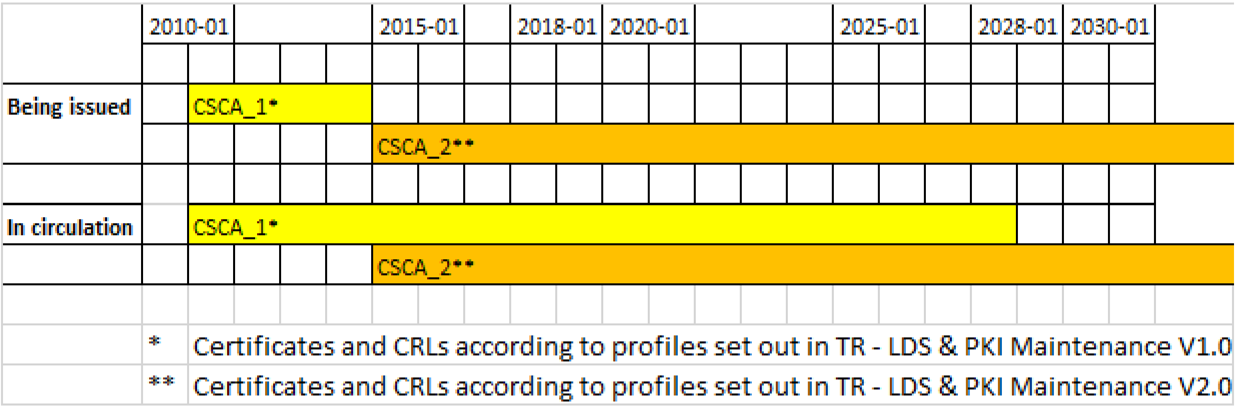
4.3 Implementation prerequisites

n/a

4.4 Implementation strategy

Issuers are RECOMMENDED to start issuing certificates conforming to this new profile starting at their next CSCA roll-over. It is assumed that for each CSCA the next roll-over will occur within 5 years from the publication date of the Technical Report.

4.4.1 Timetable



	2010-01					2015-01			2018-01		2020-01					2025-01			2028-01		2030-01		
Being issued		CSCA_1*	🟨	🟨	🟨																		
						CSCA_2**	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧
In circulation		CSCA_1*	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨				
						CSCA_2**	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧

* Certificates and CRLs according to profiles set out in TR - LDS & PKI Maintenance V1.0

** Certificates and CRLs according to profiles set out in TR - LDS & PKI Maintenance V2.0