MACHINE READABLE TRAVEL DOCUMENTS

SUPPLEMENT
to
Doc 9303

Version: **Release 11**
Status: Final
Date – November 17, 2011

Published by authority of the Secretary General

ISO/IEC JTC1 SC17 WG3
for the
INTERNATIONAL CIVIL AVIATION ORGANIZATION

File	: Supplement to ICAO Doc 9303 - Release_11.doc
Author	: ISO/IEC JTC1 SC17 WG3/TF1 for ICAO-NTWG

Release Control

Release	Date	Description
2004-2	19-12-2004	First public release **(Release 1)**
2005-4 V3	12-06-2005	Second public release **(Release 2)**
Release 3	28-02-2006	Third public release
Release 4	30-06-2006	Fourth public release
Release 5	07-02-2007	Fifth public release
Release 6	21-09-2007	Sixth public release
Release 7	19-11-2008	Seventh public release
Release 8	19-03-2010	Eighth public release
Release 9	09-03-2011	Ninth public release
Release 10	20-05-2011	Tenth public release
Release 11	17-11-2011	Eleventh public release

Release Note:
Ten releases of the Supplement have been published before this release. The latest public release is Release 11, published on November 17, 2011.

This release (Release 11) is the eleventh public dissemination of material associated with ICAO Doc9303 specifications.
Releases 1-5 of the Supplement have been limited to ICAO's Doc 9303 - part 1. Starting with Release 6 the Supplement covers all three parts of Doc 9303. Starting with Release 9 the Supplement also covers published Technical Reports.

In some cases one issue might be relevant for more than one part of Doc 9303. For reasons of readability such an issue is repeated in each Supplement section to which it is relevant. Cross references are provided with these issues.

Table 1 shows the changes that have been made to release 10 of the Supplement, resulting in this release 11.

Supplement to Doc 9303	
Release 10	**Release 11**
General	
Technical Reports	
	R11-TR_Testspec_0001 reference to supplement R4 in TR test specifications
	R11-TR_SAC_0003 Worked examples PACE V2
Part 1	
	R11-p1_v1_sIV_0007 Error in three letter codes
	R11-p1_v1_sIV_0008 New three letter codes
	R11-p1_v1_sIV_0009 Transliterations
	R11-p1_v2_sIII_0061 Unknown date of birth encoding in DG11
	R11-p1_v2_sIV_0063 CRL signing
Part 2	
	R11-p2_v-_sIII_0005 New three letter codes
	R11-p2_v-_sIII_0006 Transliterations
Part 3	
	R11-p3_v1_sIV_0005 New three letter codes
	R11-p3_v1_sIV_0006 Transliterations
	R11-p3_v2_sIII_0015 Unknown date of birth encoding in DG11
	R11-p3_v2_sIV_0016 CRL signing

Table 1

Table of contents

1 Introduction

This Supplement to Doc 9303 is intended to serve several purposes. First and foremost, the purpose of the Supplement is periodic and regular issuance of travel document guidance, advice, update, clarification and amplification. The Supplement shall serve as a "bridge" between the formal drafting of Standards and Technical Reports and the needs of the travel document community to have timely and official direction on which to rely. The Supplement does not *replace* in any way the Technical Report process or the development of 9303. What the Supplement *does* accomplish is provide a systematic and continuing forum in which views can be captured and shared, issues raised and addressed, learnings can be communicated, clarifications and characterizations of standards matters can be memorialized and the myriad of matters that need to be codified and distributed on a time-urgency basis that cannot wait for a TR or 9303. The role of the Supplement is as a *maintenance* vehicle for 9303. Much of the contents of the Supplement shall eventually be incorporated into a Technical Report or 9303 or both and, in that manner, can serve to shape and form such ICAO documents.

1.1 Scope and purpose

To as great an extent as possible, the Supplement will address any issue that comes within the scope and purpose of the ICAO TAG, and in particular, the NTWG. The development of the Supplement and its content shall be a collegial undertaking, with Government officials working hand-in-hand with SC17 WG3 and other private sector entities. While the vehicle for developing revisions of the Supplement shall be the WG3 Task Force One, all members of the ICAO community are expected to contribute to substance and content. The Supplement shall only be authorized for issuance, or shall be issued directly, by the NTWG. The Supplement will be published on a regular schedule as well as on an as-needed basis.

1.2 Assumptions

The Supplement shall augment the traditional development of 9303, drafting Technical Reports, FAQ's and other media through which communication can be effected for the travel document community. The Supplement can serve as early-notice for matters that are pending within 9303 or TR's as well as material that is solely for the Supplement in and of itself. The content of the Supplement shall have the full force and effect of 9303 standards and as such may augment, clarify, elaborate, amplify or restate the content and interpretation of standards as well as practices.

1.3 Structure of the Supplement

1.3.1 Supplement composition

Section 1 contains the introduction and general supporting information.
Section 2 covers issues related to Doc 9303, part 1 (sixth edition) - Machine Readable Passports. This section reflects the division of part 1 into Volumes and Sections.
Section 3 is related to Doc 9303, part 2 (third edition) - Machine Readable Visas.
Section 4 covers issues related to Doc 9303, part 3 (third edition) - Machine Readable Official Travel Documents. This section reflects the division of part 3 into Volumes and Sections. Issues in this section are seen as not being relevant to incorporate into the new edition of Doc 9303, part 3 but do provide relevant clarifications.
Appendices provide additional specifying information.

1.3.2 Issue numbering

Each issue in the Supplement is identified by a unique number. This number has the following format:

Rm-pn_vx_sy_zzzz

in which

Rm	=	First Supplement **R**elease in which the issue was raised.
pn	=	**P**art of 9303 (p1, p2, p3) or **T**echnical **R**eport.
vx	=	**V**olume in Part (v1, v2) or Technical Report name abbreviation.
sy	=	**S**ection in Volume (sI, sII, sIII, sIV, sV), 'g' for General (not present in case of TR).
zzzz	=	Sequence number.

1.3.3 Supplement terminology

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

1.3.4 Abbreviations

Abbreviation	
AID	Application Identifier
APDU	Application Protocol Data Unit
BAC	Basic Access Control
BLOB	Binary Large Object
CA	Certification Authority
CRL	Certificate Revocation List
DES	Data encryption standard.
DO	Data Object
DSA	Digital signature algorithm.
DSS	Digital signature scheme.
EAL	Evaluation Assurance Level:
EAC	Extended Access Control
FAR	False Acceptance Rate
FRR	False Rejection Rate
EEPROM	Electrically erasable programmable read only memory. A non-volatile memory technology where data can be electrically erased and rewritten.
eMRTD	An MRTD (Passport, Visa or Card) that has a contactless IC imbedded in it and the capability of being used for biometric identification of the MRTD holder in accordance with the standards specified in the relevant Part of ICAO Doc 9303.
eMRtd	A Machine Readable Official Travel Document that has a contactless IC imbedded in it and the capability of being used for biometric identification of the MRtd holder in accordance with the standards specified in this Volume of ICAO Doc 9303 Part 3.
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
ICC	Integrated Circuit Card
IFD	Interface Device
JPEG	A Standard for the data compression of images, used particularly in the storage of facial images.
JPEG 2000	An updated version of the JPEG standard

Abbreviation	
LDS	Logical Data Structure
MAC	Message authentication code.
MRTD	Machine Readable Travel Document conforming to ICAO Doc 9303 Part1, 2 or 3
MRZ	Machine Readable Zone
NTWG	New Technologies Working Group
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Card
PID	Creator of Biometric Reference Data
PKD	Public Key Directory
PKI	Public Key Infrastructure
RAM	Random access memory.
RSA	Asymmetric algorithm invented by Ron Rivest, Adi Shamir, and Len Adleman. It is used in public-key cryptography and is based on the fact that it is easy to multiply two large prime numbers together, but hard to factor them out of the product.
ROM	Read Only Memory
SHA	Secure hash algorithm.
SM	Secure Messaging
TAG	Technical Advisory Group
WSQ	Wavelet Scalar Quantization
X.509	ITU-T digital certificate. The internationally recognised electronic document used to prove identity and public key ownership over a communication network. It contains the issuer's name, user's identifying information, and issuer's digital signature.

1.4 Reference documentation

The following documentation served as reference for Doc 9303, the Technical Reports and this Supplement:

ANSI X9.62:2005, *"Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", 7 January 1999.*

FIPS 180-2, *Federal Information Processing Standards Publication (FIPS PUB) 180-2, Secure Hash Standard, August 2002*.

FIPS 186-2 or 186-3, *Federal Information Processing Standards Publication (FIPS PUB) 186-2 (+ Change Notice), Digital Signature Standard, 27 January 2000 (Supersedes FIPS PUB 186-1 dated 15 December 1998)*).

ISO 1073-2: 1976, *Alphanumeric character sets for optical recognition — Part 2: Character set OCR-B — Shapes and dimensions of the printed image*

ISO 1831: 1980, *Printing specifications for optical character recognition*

ISO 3166-1: 2006, *Codes for the representation of names of countries and their subdivisions — Part 1: Country codes*

ISO 3166-2: 2007, *Codes for representation of names of countries and their subdivisions — Part 2: Country subdivision code*

ISO/IEC 7810: 1995, *Identification cards — Physical characteristics*

ISO/IEC 7816-2: 2007, *Identification cards - Integrated circuit cards - Part 2: Cards with contacts - Dimensions and location of the contacts.*

ISO/IEC 7816-4: 2005, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

ISO/IEC 7816-5: 2004, *Identification cards — Integrated circuit cards — Part 5: Registration of application providers*

ISO/IEC 7816-6: 2004, *Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange (Defect report included)*

ISO/IEC 7816-11: 2004, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

ISO 8601:2000, *Data elements and interchange formats — Information interchange — Representation of dates and times*

ISO/IEC 8825-1:2002, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO/IEC 9796-2: 2002, *Information Technology — Security Techniques — Digital Signature Schemes giving message recovery — Part 2: Integer factorization based mechanisms.*

ISO/IEC 9797-1:1999, *Information technology —Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher.*

ISO/IEC 10373-6:2011, *Identification cards – Test methods – Part 6: Proximity cards*

ISO/IEC 10373-6:2001/Amd 7:2010, *Identification cards – Test methods – Part 6: Proximity cards – Test methods for ePassports and ePassport Readers*

ISO/IEC 10646:2003, *Information technology — Universal Multiple-Octet Coded Character Set (UCS).*

ISO/IEC 10918, *Information technology — Digital compression and coding of continuous-tone still images.*

ISO 11568-2:2005, *Banking — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle.*

ISO/IEC 11770-2:1996, *Information technology Security techniques Key management Part 2: Mechanisms using symmetric techniques.*

ISO/IEC 14443-1:2008, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 1: Physical Characteristics*

ISO/IEC 14443-2:2010, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 2: Radio Frequency Power and Signal Interface*

ISO/IEC 14443-3:2011, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and Anticollision*

ISO/IEC 14443-4:2008, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol*

ISO/IEC 15444, *Information Technology - JPEG 2000 image coding system*

ISO/IEC 15946: 2002, *Information technology Security techniques Cryptographic techniques based on elliptic curves.*

ISO/IEC 19794-4, *Information technology — Biometric data interchange formats — Part 4: Finger image data*

ISO/IEC 19794-5, *Information technology — Biometric data interchange formats — Part 5: Facial image data*

ISO/IEC 19794-6, *Information technology — Biometric data interchange formats — Part 6: Iris image data*

RFC 2119, *S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, March 1997.*

RFC 3279, *W. Polk, R. Housley, L. Bassham, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002.*

RFC 3280, *R. Housley, W. Polk, W. Ford, D. Solo, "X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002.*

RFC 5280, *D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", May 2008.*

RFC 3369, *R. Housley, Cryptographic Message Syntax (CMS), August 2002.*

RFC 3447, *J. Jonsson, B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", February 2003.*

TR-03111, *Bundesamt für Sicherheit in der Informationstechnik, „Technical Guideline - Elliptic Curve Cryptography - Version 1.11", April 2009.*

Unicode 4.0.0, *The Unicode Consortium. The Unicode Standard, Version 4.0.0, defined by: The Unicode Standard, Version 4.0 (Boston, MA, Addison-Wesley, 2003. ISBN 0-321-18578-1) (Consistent with ISO/IEC 10646-1)*

1.5 Object Identifiers

This paragraph lists the actual ICAO Object Identifiers:

```
-- ICAO security framework, see ICAO Doc 9303-Volume 2-Section IV-A3.2
id-icao OBJECT IDENTIFIER ::= {2.23.136}

id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}

id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
```

```
-- LDS security object, see ICAO Doc 9303-Volume 2-Section IV-A3.2
id-icao-mrtd-security-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-
mrtd-security 1}

-- CSCA master list, see TR "CSCA Countersigning and Master List issuance"
id-icao-mrtd-security-cscaMasterList OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 2}

id-icao-mrtd-security-cscaMasterListSigningKey OBJECT IDENTIFIER ::= {id-icao-
mrtd-security 3}

-- document type list, see TR "LDS and PKI Maintenance"
id-icao-mrtd-security-documentTypeList OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 4}

-- Active Authentication protocol, see "TR LDS and PKI Maintenance"
id-icao-mrtd-security-aaProtocolObject OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 5}

-- CSCA name change, see TR "LDS and PKI Maintenance"
id-icao-mrtd-security-extensions OBJECT IDENTIFIER ::= {id-icao-mrtd-security 6}

id-icao-mrtd-security-extensions-nameChange OBJECT IDENTIFIER
::= {id-icao-mrtd-security-extensions 1}

-- DS document type, see TR "LDS and PKI Maintenance"
id-icao-mrtd-security-extensions-documentTypeList OBJECT IDENTIFIER ::= {id-
icao-mrtd-security-extensions 2}
```

2 Technical Reports

2.1 TR - Supplemental Access Control for Machine Readable Travel Documents

R9-TR_SAC_0001

Reference:
ICAO Technical Report: Supplemental Access Control for Machine Readable Travel Documents – V1.01, section 4.3.

Issue:
1.
For the integrated mapping the order of the nonces *s* and *t* input to the function ***R***() is incorrect. The current specification uses *s* as key and *t* as input to the initial encryption step, producing the output *o*=**E**(*s*,*t*). As the key *s* of the cipher is already known when the input *t* is chosen, *t* can be selected as *t*=**D**(*s*,*o*) for any *predetermined* output *o*, and therefore the output of the random function **R**() can be chosen to be independent of the nonce *s*.

2.
For the integrated mapping the sizes of the constants c_0 and c_1 used in the function ***R***() are incorrect for AES-192.

Conclusion:
See corrections described in the clarification below.

Clarification:
1.
Change the order of the inputs and adapt the input sizes to reflect the corresponding key and block size. Note that this also changes the size of the nonce *s* for the generic mapping when AES-192 is used.
With respect to the Technical Report ”Supplemental Access Control for Machine Readable Travel Documents – V1.01” the following corrections apply:
Section 4.3:

- Replace 1st sentence by ”The MRTD chip SHALL randomly and uniformly select the nonce *s* as a binary bit string of length *l*, where *l* is a multiple of the block size in bits of the respective block cipher **E**() chosen by the MRTD chip”.
- Replace 3rd bullet by ”For the Integrated Mapping the additional nonce *t* SHALL be selected randomly and uniformly as a binary bit string of length *k* and sent in clear. In this case *k* is the key size in bits of the respective block cipher **E**() and *l* SHALL be the smallest multiple of the block size of **E**() such that *l*>=*k*”.

Figure 4.1:

- Swap *s* and *t*.
- Change the five occurrences of “AES” into “CBC”.
- Replace the title by “*Figure 4.1: The function R(s,t) using the block cipher E() in CBC mode*”.

2.
Use the constants with the appropriate multiple of the block size instead of the key size.
For 3DES and AES-128 the 128-bit constants SHALL be used.
For AES-192 and AES-256 the 256-bit constants SHALL be used.
With respect to the Technical Report ”Supplemental Access Control for Machine Readable Travel Documents – V1.01” the following corrections apply:

Section 4.3.3:

- Replace the last sentence of the first paragraph by ”Where required, the output k_i MUST be truncated to key size *k*. The value *n* SHALL be selected as smallest number, such that $n*l >= \log_2 p + 64$”.
- Replace the note by “*Note: The truncation is only necessary for AES-192: Use octets 1 to 24 of k_i; additional octets are not used. In case of DES, k is considered to be equal to 128 bits, and the output of R(s,t) shall be 128 bits.*”
- Remove the second bullet specifying the constants c_0 and c_1 for AES-192.
- Replace the first sentence of the last bullet by “For AES-192 and AES-256 (l=256):”

R10-TR_SAC_0002

Reference:
ICAO Technical Report: Supplemental Access Control for Machine Readable Travel Documents – V1.01, section 4.3.3 and 4.5.

Issue:
1.
With respect to the bit lengths of octet strings *s* and *t* the first sentence in paragraph 4.3.3 is not in line with the clarification (1) in the Supplement, issue R9-TR_SAC_0001).
2.
In paragraph 4.5 it seems a clear description of the public key data object is missing as the template for this D.O. is missing. According to ISO/IEC 7816-6, we propose to use ‘7F49’

Conclusion:
Accepted, see the clarifications below.

Clarification:
1.
The first sentence in paragraph 4.3.3 should be read as follows:
“The function Rp(s,t) is a function that maps octet strings s (of bit length l) and t (of bit length k) to an element …”.

2.
The first sentence in paragraph 4.5 should be read as follows:

- “A public key data object is a constructed BER TLV structure containing an object identifier and several context specific data objects nested within the template ‘7F49’ “.

R10-TR_SAC_0003

Reference:
ICAO Technical Report: Supplemental Access Control for Machine Readable Travel Documents – V1.01.

Issue:
It would be helpful if Worked Examples with respect to the PACE V2 protocols were published.

Conclusion:
Accepted.

Clarification:
Appendix G to this Supplement provides PACE V2 Worked Examples.

2.2 TR - CSCA Countersigning and Master List Issuance

R10-TR_ML_0001

Reference:
ICAO Technical Report: Countersigning and CSCA Master List issuance – Version 1.0, June 23, 2009 section 3.1

Issue:
The intent for Master List syntax was to use the basic CMS object (based on PKCS7) containing the SignedData type. However, the wording in the TR implies that only that small component of the CMS object (i.e., the SignedData type) is used. Also, the reference to IETF RFC 3852 should be updated with a reference to RFC 5652 as RFC 3852 is no obsolete and replaced with RFC 5652.

Conclusion:
Accepted.

Clarification:

- In section 3.1 replace the first sentence:
  "The CSCA Master List is implemented as a SignedData Type, as specified in [R3], RFC 3852 - Cryptographic Message Syntax - July 2004."
  with the following:
  "The CSCA Master List is implemented as a ContentInfo Type as specified in [R3], RFC 5652 - Cryptographic Message Syntax - September 2009. The ContentInfo MUST contain a single instance of the SignedData Type as profiled in 3.1.1 below. No other data types are included in the ContentInfo. "
- In section 3.1.1, replace the first sentence:
  "The processing rules in RFC3852 apply"
  with the following:
  "The processing rules in RFC5652 apply"

In Annex A, replace the reference to RFC 3852:
"**[R3]** RFC 3852 - Cryptographic Message Syntax - July 2004"
with the following:
"**[R3]** RFC 5652 - Cryptographic Message Syntax - September 2009"

2.3 TR - RF protocol and application test standard for e-Passport - part 3

R11-TR_Testspec_0001

Reference:
ICAO Technical Report: RF protocol and application test standard for e-Passport - part 3: tests for application protocol and Logical data Structure – Version 1.01, February 20, 2007.

Issue:
The test specification ICAO part 3 RF protocol and Application for MRTD v1.0.1 Feb 20 2007 refers to the ICAO Supplement R4 (see paragraph 1.6). This can cause a formal problem for ISO 17025 certified laboratories having to base their verdicts on fails based on the reference to Supplement R4 even if the tested product is compliant to a later version of the Supplement that solves the issue.

Conclusion:
Accepted.

Clarification:
References to the Supplement in ICAO Doc9303 and related documents (such as Technical Reports) SHALL be interpreted as references to the latest Release of this Supplement.

3 Doc 9303 - Part 1 (sixth edition)

3.1 Volume 1

Issues, related to Doc 9303-part 1-sixth edition, Volume 1, are gathered in this section.

3.1.1 General

R4-p1_v1_g_0001

Reference:
Doc 9303-part 1-sixth edition: Volume 1

Issue:
Use of key words.
How to interpret key words, such as "MUST", "SHALL", "REQUIRED", "SHOULD", "RECOMMENDED", and "MAY"?

Conclusion:
See clarification.

Clarification:
To provide a clear understanding on the use and meaning of the words "MUST", "SHALL", "REQUIRED", "SHOULD", "RECOMMENDED", and "MAY" in standards a definition has been described in RFC 2119, *S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, March 1997.* This definition only applies if the words are written in CAPITALS; then these words are key words. If not written in capitals, they should be interpreted as normal writing language, not intended to have a strictly defined meaning.
It is RECOMMENDED to use key words in the way as described in RFC 2119 in future versions of ICAO Doc 9303 and ICAO Technical Reports and make a note on this use in the introduction section of these documents.
The Supplement to Doc 9303 uses key words in the way it is meant in RFC 2119 (see paragraph 1.3.1).
An abstract RFC 2119 is incorporated in Appendix B to this Supplement.

3.1.2 Section II - Technical specifications for machine readable passports - references and definitions

R7-p1_v1_sII_0001

Reference:
Doc9303, Part 1, Vol1, Section II, paragraph 3.

Issue:
In Doc9303, Part 1, Vol1 the list of reference documentation in Section II, paragraph 3 contains references to documents, which have been revised, as a result of which referenced dates have changed. An updated list of reference documentation is desirable.

Conclusion:
Accepted

Clarification:
In case of doubt the reader MAY use to the reference documentation listed in paragraph 1.4 of this Supplement as the reference documentation to be used in conjunction with Doc 9303. It SHOULD however be noted that these editorial addenda in no way affect, or interfere with, the specifications set out in Doc 9303 Part 1, Sixth edition.

3.1.3 Section III – Technical specifications for security of design, manufacture and issuance of machine readable passports

R7-p1_v1_sIII_0001

Reference:
Doc9303, Part 1, Volume 1, Section III, Appendix 1.
Also Supplement issues R7-p2_v-_sIII_0002 and R7-p3_v1_sIII_0001.

Issue:
The worldwide increase in the number of people travelling and the expected continuing growth, together with the growth in international crime, terrorism, and illegal immigration has led to increasing concerns over the security of travel documents and calls for recommendations on what may be done to help improve their resistance to attack or misuse.

Conclusion:
Accepted

Clarification:
To meet the need of increased document security, ICAO's technical advisors decided it would be desirable to publish a set of "recommended minimum security standards" as a guideline for all States issuing machine readable travel documents. This resulted in an updated Appendix 1 to Section III of Doc9303, part 1, sixth edition to replace the existing Appendix. States are RECOMMENDED to follow the updated Appendix 1, which has been incorporated into Appendix E of this Supplement.

3.1.4 Section IV - Technical specifications for machine readable passports

R3-p1_v1_sIV_0001

Reference:
Doc 9303-part 1-sixth edition: Volume 1, Section IV, 7.1.9.1

Issue:
DCFWG has expressed a view that the present text regarding the quality of a submitted portrait is a bit vague, and more guidance should be offered to issuing authorities.

Conclusion:
Noted.

Clarification:
Referred to NTWG for consideration

R6-p1_v1_sIV_0002

Reference:
Doc 9303-part 1-sixth edition: Volume 1, Section IV, 9.7.

Issue:
If the optional data field in the MRZ is not used (e.g. filled with '<' characters, should the optional data field check digit be a '<' character or character '0'?

Conclusion:
See clarification.

Clarification:
Initially it was meant to be a '0'. But because the '<' character has the same weight in calculation of the composite check digit, it was decided that this is also allowed.
9303 states: "When the personal number field is not used and filler characters (<) are used in positions 29 to 42, the check digit may be ***zero or the filler character (<)*** at the option of the issuing State or organization."

R6-p1_v1_sIV_0003

Reference:
Doc 9303-part 1-sixth edition: Volume 1, Section IV, 4.1.
Also R6-p3_v1_sIV_0001.

Issue:
At TAG 17, Germany presented data from several e-passport issuing States in support of a request to relax some of the face image acquisition tolerances in the image quality guidelines. This same report had been submitted to ISO/IEC SC 37 for consideration and incorporation into a Technical Corrigendum with respect to the specifications of ISO/IEC 19794-5. The TAG directed that the next Supplement acknowledge this work and note the stage of progress at the time of Supplement publication.

Conclusion:
Accepted.

Clarification:
The drafting group of SC 37 circulated a draft that was discussed at the SC 37 meetings in Berlin in late June 2007. At the time of preparation of Supplement Release 6, as affirmatively voted, the Corrigendum called for relaxing the tolerance in head roll (tilt) to ±8° and for the following relaxations of tolerances in head size and position (where A is image width, B is image height, CC is head width, DD is head height, and M_x and M_y are the x and y coordinates of M, the center of the face, as measured from the upper left corner of the image).

Section	Definition	Requirements
8.3.1	General requirement	Head entirely visible in the image
8.3.2	Horizontal Position of Face	$0.45\ A \leq M_x \leq 0.55\ A$
8.3.3	Vertical Position of Face	$0.3\ B \leq M_y \leq 0.5\ B$
8.3.3	Vertical Position of Face (Children under the age of 11)	$0.3\ B \leq M_y \leq 0.6\ B$
8.3.4	Width of Head	$0.5\ A \leq CC \leq 0.75\ A$
8.3.5	Length of Head	$0.6\ B \leq DD \leq 0.9\ B$
8.3.5	Length of Head (Children under the age of 11)	$0.5\ B \leq DD \leq 0.9\ B$

The work of the SC 37 with respect to the final specifications affected by this Corrigendum are backward compatible with the earlier provisions of 19794-5 since only the normative requirements will be relaxed; best practice requirements remain unchanged and are strongly recommended for the application in the e-passport framework. This ensures that, e.g., issuing authorities and/or photographers do not have to change their already-published photo requirements which are based on the existing best practice requirements. Also, issuing authorities will now be able to accept more of the submitted photographs without degrading facial recognition performance. In its 18th meeting in May 2008 the TAG acknowledged the adjustments made by this Technical Corrigendum to ISO/IEC 19794-5 affecting the according reference of ICAO Doc 9303 for photographs, and approved the continuation of on-going awareness or research in this area.

See also **R6-p1_v2_sII_0002**

R7-p1_v1_sIV_0004

Reference:
Doc 9303-part 1-sixth edition: Volume 1, Section IV, Appendix 7.
Also R7-p2_v-_sIII_0001 and R7-p3_v1_sIV_0002.

Issue:
It should be noted that since 2002 the term “Dependant territories citizen - GBD*” has been changed into “British Overseas Territories Citizen - GBD*”.

Conclusion:
Accepted.

Clarification:
The description at the 3-lettercode GBD* has changed into “British Overseas Territories Citizen”.

R8-p1_v1_sIV_0005

Reference:
Doc 9303-part 1-sixth edition: Volume 1, Section IV, Appendix 7.
Also R8-p2_v-_sIII_0003 and R8-p3_v1_sIV_0003.

Issue:
It should be noted that in ISO 3166, where Doc 9303 refers to for three letter county codes, changes have been made.

Conclusion:
Accepted.

Clarification:
The following changes apply for the 3-lettercodes, as listed in Doc 9303-part 1-sixth edition: Volume 1, Section IV, Appendix 7:

- France, Metropolitan – FXX: deleted
- Montenegro – MNE: added
- Serbia – SRB: added

Serbia and Montenegro – SCG: deleted

R10-p1_v1_sIV_0006

Reference:
Doc 9303-part 1-sixth edition: Volume 1, Section IV, Appendix 7.
Also R10-p2_v-_sIII_0004 and R10-p3_v1_sIV_0004.

Issue:
It should be noted that in ISO 3166, where Doc 9303 refers to for three letter county codes, changes have been made.

Conclusion:
Accepted.

Clarification:
The following changes apply for the 3-lettercodes, as listed in Doc 9303-part 1-sixth edition: Volume 1, Section IV, Appendix 7:

- Bonaire, Saint Eustatius and Saba – BES: added
- Curaçao – CUW: added
- Saint-Barthélemy – BLM: added

- Saint-Martin (French part) – MAF: added

Sint Maarten (Dutch part) – SXM: added

R11-p1_v1_sIV_0007

Reference:
Doc 9303-part 1-sixth edition: Volume 1, Section IV, Appendix 7.

Issue:
The table with three letter country codes contains an error. The country codes of “Republic of Korea” and “Republic of Moldova” have been mixed up.

Conclusion:
Accepted.

Clarification:
The country codes for “Republic of Korea” and “Republic of Moldova” must be:
Republic of Korea - KOR
Republic of Moldova - MDA

R11-p1_v1_sIV_0008

Reference:
Doc 9303-part 1-sixth edition: Volume 1, Section IV, Appendix 7.
Also R11-p2_v-_sIII_0005 and R11-p3_v1_sIV_0005.

Issue:
A three letter code has been assigned to South Sudan.

Conclusion:
Accepted.

Clarification:
The country code for South Sudan is SSD.

R11-p1_v1_sIV_0009

Reference:
Doc 9303-part 1-sixth edition: Volume 1, Section IV, Appendix 9.
Also R11-p2_v-_sIII_0006 and R11-p3_v1_sIV_0006.

Issue:
A request has been received to accommodate the transliteration of Turkish characters.

Conclusion:
Accepted.

Clarification:
In the transliteration table the following transliterations apply for the characters mentioned below:
Ö can be transliterated by OE or O.
Ü can be transliterated by UE, UXX or U.
Ä can be transliterated by AE or A.
Å can be transliterated by AA or A.

3.2 Volume 2

Issues, related to Doc-9303-part 1-sixth edition, Volume 2, are gathered in this section.

3.2.1 General

R4-p1_v2_g_0001

Reference:
Doc 9303-part 1-sixth edition: Volume 2

Issue:
Use of key words.
How to interpret key words, such as "MUST", "SHALL", "REQUIRED", "SHOULD", "RECOMMENDED", and "MAY"?

Conclusion:
See clarification.

Clarification:
To provide a clear understanding on the use and meaning of the words "MUST", "SHALL", "REQUIRED", "SHOULD", "RECOMMENDED", and "MAY" in standards a definition has been described in RFC 2119, *S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, March 1997.* This definition only applies if the words are written in CAPITALS; then these words are key words. If not written in capitals, they should be interpreted as normal writing language, not intended to have a strictly defined meaning.
It is RECOMMENDED to use key words in the way as described in RFC 2119 in future versions of ICAO Doc 9303 and ICAO Technical Reports and make a note on this use in the introduction section of these documents.
The Supplement to Doc 9303 uses key words in the way it is meant in RFC 2119 (see paragraph 1.3.1).
An abstract RFC 2119 is incorporated in Appendix B to this Supplement.

3.2.2 Section II - The deployment of biometric identification and the electronic storage of data in machine readable passports

R3-p1_v2_sII_0001

Reference:

Issue:
In the Working Draft (WD) of the Sixth Edition Part 1 ICAO Doc 9303 there is no mention of a version of ISO 19794-5. The CD was subsequently revised and elevated to Final Draft International Standard (FDIS) status. The FDIS of 19794-5 published on 6th of January 2005 contains the following changes to the CD version:

DATA ITEM	As specified in CD of 19794-5	As specified in FDIS of 19794-5
CBEFF_BDB_format_type	0x0501	0x0008
Face Image Type – Basic	1	0x00
Face Image Type – Full Frontal	2	0x01
Face Image Type – Token Image	3	0x02

Several States have already started issuing ePassports. Given that previously posted versions of the Technical Reports, as well as, draft versions of the Sixth Edition of Part 1 of ICAO Doc 9303 indicated that States issuing ePassports should follow specifications set out in the referenced International Standard, the countries already issuing may have used the specifications set out in the CD of 19794-5 as versus those contained in the **Published ISO/IEC19794-5 Standard**, which are based on the FDIS of 19794-5.
The danger from the above are as follows:

- ePassports from a State already issuing may have prepared the LDS based on the specs set out in the CD of 19794-5 and when a Receiving State checks the CBEFF_BDB_format_type they will reject the ePassport as invalid (i.e. CBEFF_BDB_format_type = 0x0501 as versus 0x0008); and
- Failure of a Receiving State to check the CBEFF_BDB_format_type and confirm it is set to "0x0008" could result in incorrect interpretation of a Full Frontal Type Image as a Token Image (i.e. "2" interpreted as "0x02") or a Full Frontal Type Image as a Basic Image (i.e. "0x01" interpreted as "1"); or rejection of a legitimate Token Image as being invalid (i.e. "3" processed based on FDIS specifications) when CBEFF_BDB_format_type = "0x0501".

Conclusion:
Accepted.

Clarification:
The RECOMMENDED solution is as follows:

1. Receiving States MUST check the CBEFF_BDB_format_type to confirm it is set to "0x0008". If not, they SHOULD then check to see if is set to "0x0501" before rejecting the ePassport as invalid. In the event that a Receiving State finds CBEFF_BDB_format_type is set to "0x0501", they SHOULD ensure that interpretation of the Face Image Type – Full Frontal, Face Image Type – Token Image and Face Image Type – Basic Image are as defined in the CD of 19794-5.
2. All States not yet issuing their ePassport SHALL follow the specifications set out in the published ISO/IEC19794-5 Standard, which are based on the FDIS of 19794-5.

R6-p1_v2_sII_0002

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section II, 13.4.2.
Also R6-p3_v2_sII_0001.

Issue:
At TAG 17, Germany presented data from several e-passport issuing States in support of a request to relax some of the face image acquisition tolerances in the image quality guidelines. This same report had been submitted to ISO/IEC SC 37 for consideration and incorporation into a Technical Corrigendum with respect to the specifications of ISO/IEC 19794-5. The TAG directed that the next Supplement acknowledge this work and note the stage of progress at the time of Supplement publication.

Conclusion:
Accepted.

Clarification:
The drafting group of SC 37 circulated a draft that was discussed at the SC 37 meetings in Berlin in late June 2007. At the time of preparation of Supplement Release 6, as affirmatively voted, the Corrigendum called for relaxing the tolerance in head roll (tilt) to ±8° and for the following relaxations of tolerances in head size and position (where A is image width, B is image height, CC is head width, DD is head height, and M_x and M_y are the x and y coordinates of M, the center of the face, as measured from the upper left corner of the image).

Section	Definition	Requirements
8.3.1	General requirement	Head entirely visible in the image
8.3.2	Horizontal Position of Face	$0.45\ A \leq M_x \leq 0.55\ A$
8.3.3	Vertical Position of Face	$0.3\ B \leq M_y \leq 0.5\ B$

8.3.3	Vertical Position of Face (Children under the age of 11)	$0.3\ B \leq M_y \leq 0.6\ B$
8.3.4	Width of Head	$0.5\ A \leq CC \leq 0.75\ A$
8.3.5	Length of Head	$0.6\ B \leq DD \leq 0.9\ B$
8.3.5	Length of Head (Children under the age of 11)	$0.5\ B \leq DD \leq 0.9\ B$

The work of the SC 37 with respect to the final specifications affected by this Corrigendum are backward compatible with the earlier provisions of 19794-5 since only the normative requirements will be relaxed; best practice requirements remain unchanged and are strongly recommended for the application in the e-passport framework. This ensures that, e.g., issuing authorities and/or photographers do not have to change their already-published photo requirements which are based on the existing best practice requirements. Also, issuing authorities will now be able to accept more of the submitted photographs without degrading facial recognition performance. In its 18th meeting in May 2008 the TAG acknowledged the adjustments made by this Technical Corrigendum to ISO/IEC 19794-5 affecting the according reference of ICAO Doc 9303 for photographs, and approved the continuation of on-going awareness or research in this area..
See also **R6-p1_v1_sIV_0003.**

3.2.3 Section III - A Logical Data Structure for contactless integrated circuit data storage technology

R1-p1_v2_sIII_0018

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section III, Appendix 1, A.11.1

Issue:
Resolve ambiguity of File Select Command (7816-4 Short EFID)

Conclusion:
Accepted.

Clarification:
Doc 9303-part 1-sixth edition: Volume 2, Section III, Appendix 1, A 12 should be interpreted as follows:

The first 7816 instruction is “select application”, with the code 00A4 04 0C 07 A0 00 00 02 47 10 01. Every machine-readable travel document (MRTD) application supports the select command. Reference ISO 7816-4 (table 5, section 5.1.3) for complete return codes.

SELECT:
The MRTD supports both methods (Select File and Short EFID). Readers support at least one of the two methods. The file identifier and Short EFID is mandatory for the [card] operating system, but optional for reader.

READ BINARY:
Le must be one byte, and must be encoded per 7816-4.

Other:
The clause “*by the reader*” is understood as implied in the LDS anywhere that 'Select File' is stated as optional.

R1-p1_v2_sIII_0019

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section III, Appendix 1, A.19.2.
Also Supplement issue R6-p3_v2_sIII_0001.

Issue:
Silver Data set references LDS Ver 1.6.
The editorial syntax is misleading. The correct syntax is either '00' 'A4' '00' '0C' Empty Empty Empty
or,
'00' 'A4' '00' '0C' Empty Empty MaxRet

Conclusion:
Noted.

Clarification:
The difference between the commands is: The first one just returns 0x9000 in case of success, the second one returns the File Control Parameters of the selected file (see LDS 1.x, x<5)

The MF on the MRTD's chip is OPTIONAL, and therefore might not be present.

If SELECT MF is used, then, in compliance with other SELECT functions, '00' 'A4' '00' '0C' Empty Empty Empty MUST be used.

R1-p1_v2_sIII_0021

Reference:

Issue:
Separate Type–A description and Type-B description.

Conclusion:
Rejected.

Clarification:
ISO/IEC 14443, a normative reference, provides sufficient description.

R1-p1_v2_sIII_0028

Reference:
Also Supplement issue R6-p3_v2_sIII_0001.

Issue:
Define how a reader can recognize that a document is using Basic Access Control. Proposal that
EF.COM is free to read
EF.COM has indicator that BAC is in use

Conclusion:
See clarification.

Clarification:
The *Basic Access Control* mechanism is optional. When presenting a MRTD with an ICC to a reader, this reader doesn't know in advance if the mechanism must be performed. How can the reader solve this problem?

A solution can be a simple trial-and-error mechanism. First try to get direct access to the ICC and if this fails, perform the *Basic Access Control Mechanism*.

Step 1:
Select the LDS DF by AID. If this fails, the MRTD isn't equipped with an ICAO LDS compliant ICC. Otherwise the correct response will be '90 00'.
(send: '00 A4 04 0C 07 A0 00 00 02 47 10 01', response: '90 00')

Step 2.
Try to select the EF.COM by file ID. Depending on the answer of the ICC, Basic Access Control is, or is not, implemented.

Option 1:
No Basic Access Control required.
(send: '00 A4 02 0C 02 01 1E', response: '90 00').
The file is selected and the data can be read.

Option 2:
Basic Access Control required.
(send: '00 A4 02 0C 02 01 1E', response: '69 82').
The file is NOT selected and the ISO-7816-4 error-code means "Security status not satisfied". The Basic Access Control Mechanism must be performed after which the file should be selected again using Secure Messaging.

Option 3:
An error occurs.
(send: '00 A4 02 0C 02 01 1E', response: error-code other than '69 82').
The file is NOT selected. The MRTD isn't equipped with an ICAO LDS compliant ICC.

The READ BINARY command may also be used as a trigger to indicate if the document is protected using Basic Access Control. When READ BINARY is used

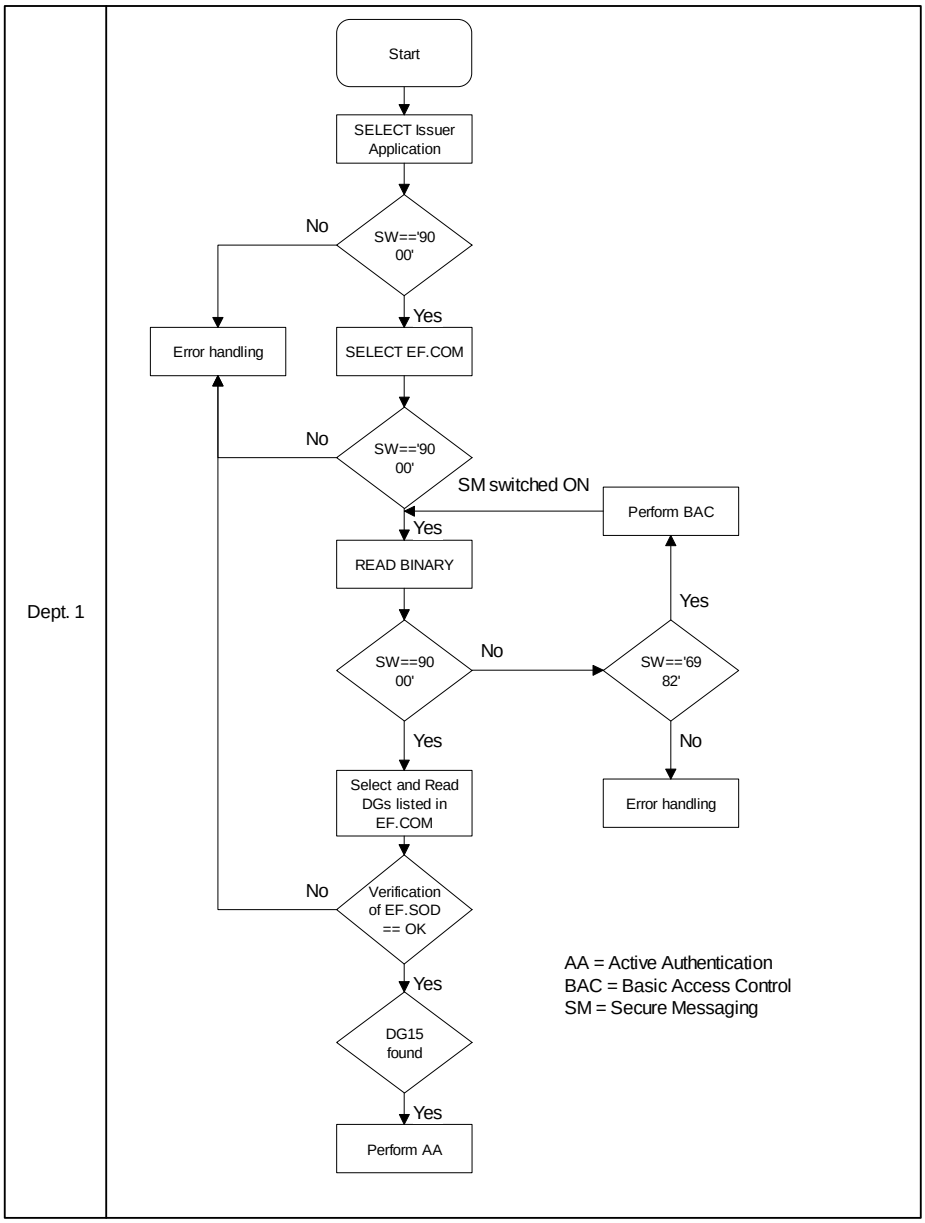
Case a): using separate SELECT command and then READ BINARY

1) Select EF.COM using SELECT command: send '00 A4 02 0C 02 01 1E'.
2) If response is '90 00'
   - Try to read the content using READ BINARY command:
     send '00 B0 00 00 00'
     - If '6982' error code is returned, the Issuer Application is protected using BAC. Then The Basic Access Control Mechanism must be performed after which the file should be read again using Secure Messaging.
     - If the content (first 256 bytes) + '90 00' SW bytes are returned, the Issuer Application is NOT protected using BAC.
     - Otherwise some error has occurred, go to the error handling.
3) Otherwise the Issuer Application isn't ICAO LDS compliant.

Case b): using SFID combined to READ BINARY

1) Try to read the content of EF:COM using SFID combined to READ BINARY command:
   send '00 B0 9E 00 00'
   - If '6982' error code is returned, then the Issuer Application is protected using BAC. Then The Basic Access Control Mechanism must be performed after which the file should be read again using Secure Messaging.
   - If the content (first 256 bytes) + '90 00' SW bytes are returned, the Issuer Application is NOT protected using BAC.
   - Otherwise the Issuer Application isn't ICAO LDS compliant.

Below the case a) is presented as a process flow diagram:



R1-p1_v2_sIII_0029

Reference:

Issue:
Relationship between Short EFID and File ID need to be defined. Proposal that File ID should be defined by adding '00' as MSB of Short EFID.

Conclusion:
Rejected.

Clarification:
Not needed.

R1-p1_v2_sIII_0030

Reference:

Issue:

Extended binary command B1:
For some purposes, B1 and the traditional B0 read binary commands could not overlap. In other words, B0 only should be used to read the first 32,767 bytes and B1 from 32K upward. For others there could be a small overlap of 256 bytes around the 32,767 threshold to allow a smoother transition between B0 and B1. For this latter group, B1 could be used right from the beginning of the file, i.e. with an offset starting from 0 to allow the same command to be used to read the full content. With respect to ISO/IEC 7816-4: 2005, there are no constraints specified on the offset value when bit 1 of INS is set to 1 to allow a broader use.

Conclusion:
Accepted.

Clarification:

R2-p1_v2_sIII_0031

Reference:

Issue:
Support of Short File ID is MANDATORY for MRTDs. Therefore it is RECOMMENDED to be used by inspection systems.

Conclusion:
Accepted.

Clarification:

R2-p1_v2_sIII_0032

Reference:
Also Supplement issue R6-p3_v2_sIII_0002.

Issue:
Odd INS data field structure
Three different implementations were found at read binary of Odd_INS Byte when reading data greater than 32k byte
1) The Le byte contains V only
2) The Le byte contains TL and V
3) The Le byte contains extended TL and V
Need to clarify recommended implementation

Conclusion:
Accepted.

Clarification:
Option 3: ‘The Le byte contains extended TL and V’ should be implemented, being the most common practice.

R2-p1_v2_sIII_0035

Reference:
Also Supplement issue R6-p3_v2_sIII_0003.

Issue:
Le at Mutual authentication.
Mutual Authentication can take Le = 28 (hex) or 00. In the PKI main section, Le is not specified. However Le = 28 (hex) is specified as an example in the Appendix. But in 7816-4, Le can be 00 also, which means that the response can be up to 256 bytes and the card will decide. From our Singapore

InterFest experience, we know some card vendors expect Le = 28 and some expect Le = 00 (or will only respond correctly if Le = 00).

Conclusion:
See clarification.

Clarification:
The ISO/IEC 7816-4:2005 (as well as the earlier edition) specifies that Le encodes Ne, which in turn "denotes the maximum number of bytes expected in the response data field." In addition, it specifies for short Le fields that "If the byte (Le) is set to '00', then Ne is 256."
Therefore, the card cannot return more than Ne bytes in the response data field, but it can return less (or no) bytes. The specification of the authentication command does not define specific values for the Le, or any rules for rejecting specific Le values. eMRTDs should therefore accept both '00' and '28' in the Le field if they return always '28' bytes of response data (actually '00' or any value between '28' and 'FF', but that is not relevant here).

R2-p1_v2_sIII_0036

Reference:
Also Supplement issue R6-p3_v2_sIII_0004.

Issue:
APDU at Le=00.
In the case of Le = 00 (in general), 7816-3 allows both 5-byte APDU (i.e. Le is sent) or 4-byte APDU (i.e. Le is not sent). Usually in 7816-3, for T=0, 5-byte APDU is sent, while for T=1, 4-byte APDU is sent. But T=0 and T=1 are both for contact interface and so in the case of contactless, there is no proper guideline. We have found that some cards expect 4-byte and some 5-byte APDU when Le = 00.

Conclusion:
See clarification.

Clarification:
The ISO/IEC 7816-4:2005 as well as the ISO/IEC FCD 7816-3 specify the generic APDU structure, and ISO/IEC 7816-3 and ISO/IEC FCD 7816-3 specify how the APDUs are mapped on the TPDUs of the protocols T=0 and T=1.
The case 1 APDU, which is the subject of this issue, is specified as a 4-byte string.
For the T=0 it is specified that the C-TPDU always uses a byte P3, which is set to '00' in case 1. This is required for the byte-oriented transfer method, as the card cannot know whether it should expect 4- or 5-byte command header.
For the T=1 it is specified that the APDUs are mapped directly onto the TPDUs, as there is no requirement to do otherwise in a block-oriented transfer method.
The ISO/IEC 14443-4 does not specify how the APDUs are mapped on the INF fields, which is clearly a slight problem. However, as there is no rule or other requirement to use any conversion in the mapping from APDUs to TPDUs due to the used transfer method, the mapping intuitively equals that of T=1.
Therefore, if the command comes with five bytes, the card shall assume the fifth byte to be Le, and the commands is thereby given as a case 2 command.
In general it is not a problem to allow data to be returned in the response data field even though it is not available, but for the card it may be justified to reject commands which do not use the correct case (1, 2, 3 or 4). For maximal compatibility, the commands should always be sent using the correct case. eMRTDs which require usage of incorrect case (as indicated in the issue text) shall be rejected.

R2-p1_v2_sIII_0037

Reference:

Issue:
3 byte Le would support faster transaction.

Conclusion:
Accepted.

Clarification:
Due to the potential impact to existing implementations, extended Lc/Le field (3 bytes) support will not be mandated at this time. However, its support does offer significant bandwidth improvements and it is anticipated that support may be mandated in version 2 of the LDS. Therefore, it is RECOMMENDED that any new MRTD and MRTD reader implementation support both short Lc/Le field (1 byte) and extended Lc/Le field (3 bytes).

R2-p1_v2_sIII_0038

Reference:

Issue:
The e-passport may serve as a "beacon" in which the chip emits when initially activated data (the UID number) that might allow identification of the issuing authority. When opening the dialogue between an ePassport and an ePassport reader, some information is immediately exchanged between them. That start of the dialogue between an ePassport and a reader, which is technically specified in ISO/IEC 14443, allows the choice of the option whether the ePassport presents a fixed identifier, assigned uniquely for only that ePassport, or a random number, which is different at each start of such a dialogue. Some issuers of passports wish to implement a unique number for security reasons or any other reason. Other issuers give greater preference to concerns about data privacy and the possibility to trace persons due to fixed numbers.

Conclusion:
Accepted.

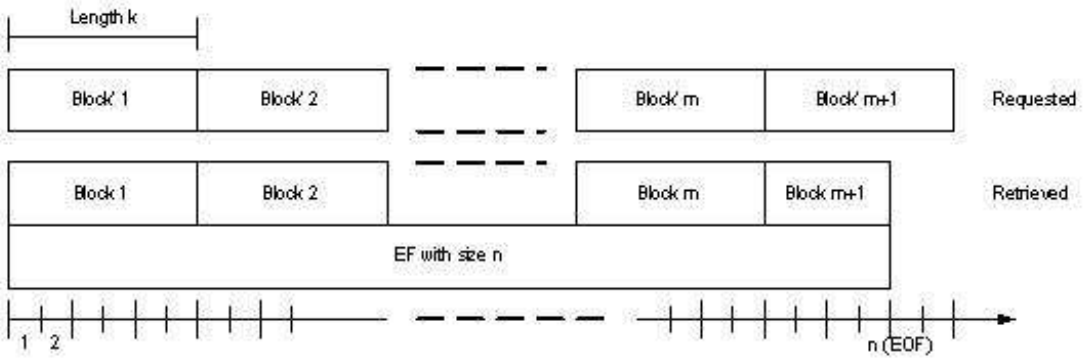
Clarification:
Choosing the one or the other option does not decrease interoperability, because a reader, when compliant with ISO/IEC 14443, will understand both methods. The use of random UIDs is RECOMMENDED, but States MAY choose to apply unique UIDs.

R2-p1_v2_sIII_0039

Reference:
Also Supplement issue R6-p3_v2_sIII_0005.

Issue:
The main use case of an inspection system is to read data groups from the e-passport with or without BAC. The Sixth Edition Part 1 ICAO Doc 9303 does only specify the general way how to retrieve a data group. It is defined as a sequence of READ BINARY COMMANDS with Le = 00. This leaves several options which have an influence on the e-Passport APDU command specifications in terms of return codes. These options are as follows:

1) The inspection system reads blocks of k bytes – where k is 256 bytes or less – increasing the offset of the READ BINARY command appropriately.

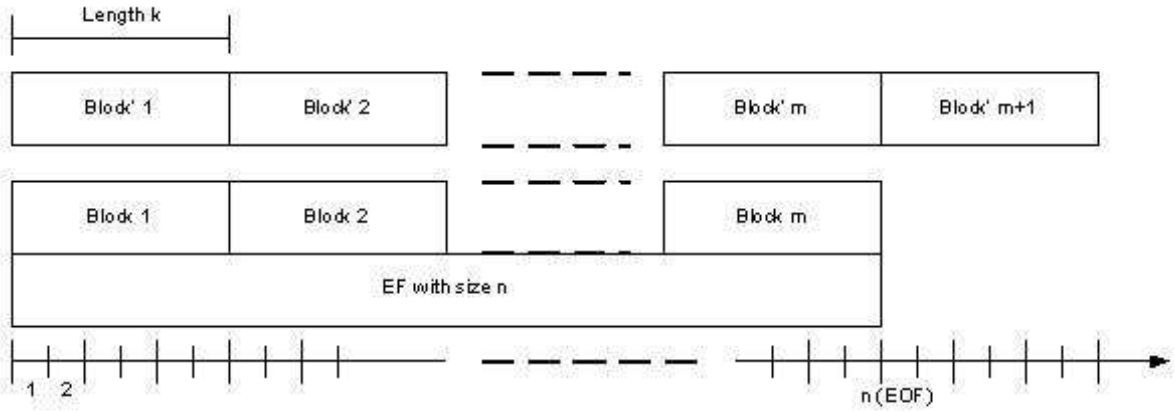


Since the length of the file is unknown in advance (the e-passport does not provide file control parameters to the inspection system), the inspection system must read until end of file (EOF). Reading the last block it may happen that the e-Passport is asked to retrieve data beyond end of file, e.g. Le = '00' for every READ BINARY. In this case it has to be clearly defined what the passport returns. The following return data is valid with respect to ISO 7816-4.

a) Block m+1 plus status word '90 00'
b) Block m+1 plus status word '62 82'
c) Checking error '6C XX', where 'XX' is the length of Block m+1

In all three cases, the BAC session keys of the e-Passport MUST NOT be deleted. All status words MUST be returned with SM data if BAC is applied.

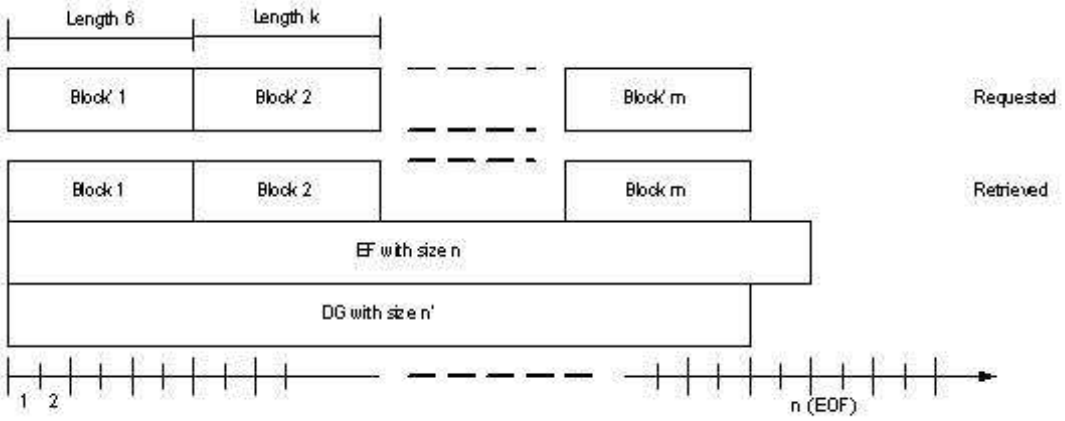
2) The inspection system reads blocks of k bytes – where k is 256 bytes or less – increasing the offset of the READ BINARY command appropriately.



Since the length of the file is unknown in advance (see option 1), the inspection system reads until the end of the file (EOF). Reading the last block it may happen that the offset of the last block (block' m+1) is already EOF. It means that n is a multiple of k. In this case it has to be clearly defined what the passport returns. The status word '6B 00' or at least a checking error is valid with respect to ISO 7816-4. Data MUST NOT be returned.

Once again, the BAC session keys of the e-Passport MUST NOT be deleted. All status words MUST be returned with SM data if BAC is applied.

3) The inspection system reads the first 5 or 6 bytes and tries to decode the length of the ASN-1 structure stored in the elementary file. In this case the inspection system knows in advance the length of the data group.



The disadvantage of this approach is that it mixes up two different layers of information. Moreover, it may be a little bit slower than the first two options, e.g. reading EF.COM may involve two consecutive READ BINARY commands instead of one command. Using this option excludes the implementation of the first two options unless the return codes defined in 1) and 2) are specified.

Conclusion:
See clarification

Clarification:
The following facts have to be considered:

1. ISO/IEC 7816-4 allows several different status words as response to some of the described read scenarios.
2. There are already several different e-Passport implementations out in the field.
3. The performance of reading the data groups is largely influenced by the amount of data to be transferred.

For the current generation of e-Passports being compliant with LDS version 1.7, specifying new requirements should be avoided (due to 1. and 2.), and elementary files should not be read completely but only until the end of the application template (due to 3.).

Therefore, option 3 (the inspection system reading the first 6 bytes to extract the exact length of a data group) should be used. Then there is no urgent need to define EOF status bytes.

For the next generation of e-Passports, e.g. according to the planned LDS version 2.0, this use case should be specified as stated in options 1 and 2 of the Request for Clarification.

R4-p1_v2_sIII_0040

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section III, Appendix 1, A.23.1.
Also Supplement issue R6-p3_v2_sIII_0006.

Issue:
Clarification if command READ BINARY with odd INS byte is a mandatory command on e-Passports even if there are no EFs greater than 32k.

Conclusion:
See clarification.

Clarification:
Doc 9303-part 1-sixth edition: Volume 2, Section III, Appendix 1, A.23.1. states:
The maximum size of an EF is normally 32,767 bytes, but some ICs support larger files. A different READ BINARY parameter option and command format is required to access the data area when the

offset is greater than 32,767. This format of command should be used after the length of the template has been determined and the need to access the data in the extended data area has been determined. For example, if the data area contains multiple biometric data objects, it may not be necessary to read the entire data area. **Once the offset for the data area is greater than 32,767, this command format shall be used.** The offset is placed in the command field rather than in the parameters P1 and P2.

This leads to the conclusion that the odd INS byte is not to be used if the size of an EF is 32,767 bytes or less.

R4-p1_v2_sIII_0041

Reference:
Also Supplement issue R6-p3_v2_sIII_0010.

Issue:
1. In the TR-LDS Version 1.7 the Data Group 14 is reserved for future use.
2. Data Group 15 contains the Active Authentication Public Key Info. This is the public part of the document specific Active Authentication Key Pair.
3. In the TR-PKI Version 1.1 the security of additional biometrics, like fingers and irisses has not been specified yet, but the TR recognizes the need for this.
4. Developments in the EU in the area of the use of fingerprint biometrics are leading to specifications that incorporate a similar construction to Active Authentication, called Chip Authentication.

To support this in an ICAO consistent way it is suggested to redefine Data Group 14.
Present definition:
DG14 - Reserved for future use.
Suggested definition:
DG14 - Security options for secondary biometrics.

DG14 should be specified in such way, that it can be used for various security options for DG3 (fingers) and DG4 (irisses).

Conclusion:
Accepted

Clarification:
In its meeting in Minneapolis, July 2005, TF1 has accepted this proposal. Therefore DG14 MUST be considered being reserved for Security options for secondary biometrics.
The following generic ASN.1 data structure **`SecurityInfos`** has been defined, allowing for various implementations of Security options for secondary biometrics. For interoperability reasons, it is RECOMMENDED that this data structure be provided by the MRTD chip in DG14 to indicate supported security protocols. The data structure is specified as follows:

```
SecurityInfos    ::=  SET of SecurityInfo

SecurityInfo     ::=  SEQUENCE {
     protocol         OBJECT IDENTIFIER,
     requiredData     ANY DEFINED BY protocol,
     optionalData     ANY DEFINED BY protocol OPTIONAL
}
```

The elements contained in a **`SecurityInfo`** data structure have the following meaning:
• The object identifier **`protocol`** identifies the supported protocol.
• The open type **`requiredData`** contains protocol specific mandatory data.

• The open type **`optionalData`** contains protocol specific optional data.

R4-p1_v2_sIII_0042

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section III, Appendix 1, A.19.2.

Issue:
Selection of Master File:
Current wording says the command should be '00 A4 00 00 00 00':

Selection of Master File

CLA	INS	P1	P2	Lc	Data	Le
'00'	'A4'	'00'	'00'	0	Empty	0

According to ISO/IEC 7816-4 section 5.1: Command-response pairs:

L_c field	Absent for encoding $N_c = 0$, present for encoding $N_c > 0$	0, 1 or 3
Command data field	Absent if $N_c = 0$, present as a string of N_c bytes if $N_c > 0$	N_c
L_e field	Absent for encoding $N_e = 0$, present for encoding $N_e > 0$	0, 1, 2 or 3

To comply with ISO/IEC 7816-4 definition, Select MF APDU should be as follows:
00 A4 00 00 00 (Lc is absent, Le = 0)

CLA	INS	P1	P2	Lc	Data	Le
'00'	**'A4'**	**'00'**	**'00'**	**Absent**	**Empty**	**0**

Conclusion:
Noted.

Clarification:
The observation is correct. However, it is RECOMMENDED that the SELECT MF command not be used.

R4-p1_v2_sIII_0043

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section III, Appendix 1, A.17.1

Issue:
It is now stated:

The PCD shall detect and resolve any collision that may occur if multiple documents are within the operating field.
ICAO AFI = See Section II

In section II is NO mention about the ICAO AFI.

Conclusion:
Accepted.

Clarification:
The AFI values for MRTDs (E1 for passports, E2 for Visas and so on) are now specified in ISO 14443-3.
The same kind of issue is the CRC_B bytes of the AID, which are returned in the ATQB. The application AID of the Issuer Application is 'A0000002471001' -> the value of 2 CRC_B bytes calculated from this AID is 'F35E'.

R5-p1_v2_sIII_0044

Reference:

Issue:
Regarding Secure Messaging Data Object Doc 9303 Part 1 Volume 2 6th edition:
An empty value field of Le Data Object in Secure Messaging command ISO/IEC 7816-4:2005 allows using empty value field of Le Data Object. Section 6.4 in ISO/IEC 7816-4:2005 describes “Both zero and the empty Le data object mean the maximum, i.e., 256 or 65536 depending upon whether the new Le field is short or extended”. But Doc 9303 Part 1 Volume 2 6th edition do not describe such empty value field of Le Data Object. See Figure IV-5-2 Computation of a SM command APDU.

Proposal: Do not use an empty value field of Le Data Object

Conclusion:
Accepted.

Clarification:
To avoid ambiguity it is RECOMMENDED not to use an empty value field of Le Data Object.

R5-p1_v2_sIII_0045

Reference:

Issue:
Regarding Secure Messaging Data Object Doc 9303 Part 1 Volume 2 6th edition:
An empty value field of Status Word Data Object in Secure Messaging response ISO/IEC 7816-:2005 allows using empty value field of Status Word Data Object. Section 6.4 in ISO/IEC 7816-4:2005 describes “The empty processing status data object means SW1-SW2 set to ‘9000’”. But Doc 9303 Part 1 Volume 2 6th edition do not describe such empty value field of Le Data Object. See Figure IV--3 Computation of a SM response APDU.

Proposal: Do not use an empty value field of Status Word Data Object
Because an inspection system may not handle this data object.

Conclusion:
Accepted

Clarification:
Resolved in R5-p1_v2_sIII_0044

R5-p1_v2_sIII_0046

Reference:
Also Supplement issue R6-p3_v2_sIII_0007.

Issue:
ISO/IEC 7816-4:2005 specifies that length of value field in Le Data Object is one or two bytes. (See Table 27 or 28 in ISO/IEC 7816-4:2005). On the other hand ISO/IEC 7816-4:2005 Annex B shows Examples of secure messaging. In this annex, value filed of Le Data Object is equal to original Le field. In Case 2E of Command APDU, length of Le field is 3 bytes. From experiences in Japanese smart card project using extended Le field, a smart card reader send 3 bytes value field of Le Data Object in secure messaging and a smart card can interpret it.

Proposal: To notify length of value field in Le Data Object is one or two bytes.

Conclusion:
Accepted.

Clarification:
The specification should be followed, meaning that the length of value field in Le Data Object is one or two bytes.

R5-p1_v2_sIII_0047

Reference:

Issue:
The table in A 13.3 contains a typo error. The length of Tag '81' is defined as being '01'-'03' for the first biometric, while it is defined as being '01' for the second biometric. The correct length definition for both instances must be '01'-'03' in accordance with ISO/IEC 7816-11.

Conclusion:
Accepted

Clarification:
The length of Tag '81' must be '01'-'03', both for the first as for the second biometric.

R6-p1_v2_sIII_0048

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section III, A13.1 and A.14.
Also Supplement issue R6-p3_v2_sIII_0008.

Issue:
Concerning the encoding of several TAGs in the LDS there is a mismatch between the LDS 1.7 specifications (Doc 9303, Part 1, Sixth edition, Volume 2, Section III) and ISO/IEC 8825-1 (BER/DER encoding rules).

ISO/IEC 8825-1:
For tags with a number ranging from zero to 30 (inclusive), the identifier octets shall comprise a single octet encoded as follows:
a) bits 8 and 7 shall be encoded to represent the class of the tag as specified in Table 1;
b) bit 6 shall be a zero or a one according to the rules of 8.1.2.5;
c) bits 5 to 1 shall encode the number of the tag as a binary integer with bit 5 as the most significant bit.

This means that (for instance) the TAG for the version number of the LDS 1.7 specification should be defined as TAG 41h:
41h = 01 0 00001b
where 01 means Application class (bits 8 and 7);
where 0 means that it is a primitive (bit 6);
where 00001 is the encoding of TAG NUMBER 1 (bits 5-1).

Doc.9303, part 1, 6th edition, Volume 2, Section III:
The TAG for the version number of the LDS 1.7 specification is defined as TAG 5F01h.
5F01h = 01 0 11111 0 0000001b
where 01 means Application class;
where 0 means that it is a primitive (not constructed);
where 11111 means that the tag number is encoded in the next bytes;
where 0 means that it is the last byte encoding the TAG number;
where 0000001 is the encoding of TAG NUMBER 1.

This counts for all TAGs from zero to 30 (inclusive):
5F01, 5F08, 5F09, 5F0A, 5F0B, 5F0C, 5F0E, 5F0F, 5F10, 5F11, 5F12, 5F13, 5F14, 5F15, 5F16, 5F17, 5F18, 5F19, 5F1A, 5F1B, 5F1C, 5F1D, 5F1E.

Conclusion:
Noted

Clarification:
Implementers should be aware of this mismatch and follow the specifications as set out in Doc9303. One should however note that:

- MRTD implementations cannot be created using a generator based on ASN.1;
- ASN.1/BER parsers may return an error instead of correctly parsing EF.COM;
- The hash over EF.COM cannot be re-created by decoding the EF.COM structure and encoding it again afterwards.

An analysis if this mismatch should be eliminated will be a workl item for TR-LDS V2.

R6-p1_v2_sIII_0049

Reference:

Issue:
The offset used in the READ BINARY command with oddset instruction byte is encoded with tag 54. The length for greater offsets is encoded in two bytes, e.g. 54 02 7F FF. But how should small offset be encoded? For example, an offset of one could be encoded as 54 01 01 or as 54 02 00 01. Are both options allowed? Does the passport have to process both options?

Conclusion:
See clarification

Clarification:
Both Length and Value fields of BER-TLV data object are variable length.
For example, offset '01' can be encoded in different BER-TLV formats (see below), which have different lengths:

1) 54 01 01 --> Tag='54' Length='01' Value='01'
2) 54 02 0001 --> Tag='54' Length='02' Value='0001'
3) 54 03 000001 --> Tag='54' Length='03' Value='000001'
4) 54 8101 01 --> Tag='54' Length='8101' Value='01'
5) 54 820001 01 --> Tag='54' Length='820001' Value='01'
6) 54 8102 0001 --> Tag='54' Length='8102' Value='0001'
7) 54 820003 000001 --> Tag='54' Length='820003' Value='000001'

For performance reasons, communication between e-Passport and Terminal should be kept as short as possible. Therefore it is suggested that both Length field and Value field in a BER-TLV data object SHOULD be as short as possible. This applies not only for Offset data objects in Odd INS READ BINARY commands but also for all other BER-TLV data objects exchanged between the eMRTD and the terminal.
For example above: Format 1) should be used and 2)-7) should not be used.

R6-p1_v2_sIII_0050

Reference:
Doc9303, Part 3, Vol2, Section III, Appendix 1.

Issue:
There are two different types of length field coding, i.e. "Definite form" and "Indefinite form" defined in paragraph 8.1.3.1. of ISO/IEC 8825-1(ASN.1).
In case of "Indefinite form", length field is 80H and "End-of-contents octet: 0000H" is needed.
Recently this type of coding at an eMRP sample in the field was discovered.

Conclusion:
See clarification

Clarification:

Doc9303, Part 1, Vol2, Section III, in the Normative Appendix 1, the table in A.24 clearly indicates that the “Definite” form MUST be used, so the use of “Indefinite form” is not correct.

R6-p3_v2_sIII_0051

Reference:
Doc9303, Part 1, Vol2, Section III, Appendix 1, A.13.10.

Issue:
With reference to the section A.13.10, Data Group 16 is specified as follows: “This data group lists emergency notification information. It is encoded as a series of templates using the tag ‘AX’ designation. This data group is not signed, allowing for updating by the document holder.”
The PKI section has been intended for “Machine Readable Travel Documents offering ICC read-only access”, as in the title of section IV. This is in line with the statement in section III, A.10.4, which states that DG16 is “write protected”.
Section III, A.13.10 (“allowing for updating by the holder”) contradicts with this. Can or cannot DG16 be updated?

Conclusion:
See clarification

Clarification:
Before the PKI Technical Report was written, earlier drafts of the LDS specified individually signed Data Groups, but this approach has been abandoned. Probably this sentence in A.13.10 is an unintended left-over of this history.
As a conclusion the interpretation MUST be:
DG16 (as all other Data Groups) should not be updated after issuance;
DG16 is represented by a hash value in the SOD and the SOD is only signed once, at personalization time.

R6-p1_v2_sIII_0052

Reference:
Doc9303, Part 1, Vol2, Section III, 10.4.1, 10.6.1, 10.7.1.
Also Supplement issue R6-p3_v2_sIII_0009.

Issue:
It seems that JPEG2000 encoding and decoding software do not have a compatibility by combination. Actually, if `the JPEG2000 format is wrong within DG2 most of the decoding software cannot handle it. In a discovered case, the reason of the problem was a missing EOC(End of code stream) or data length inconsistency of its header. These encoding errors will produce incompatibility and it is difficult to find these kind of errors if the issuer is using same vendor's encoding/decoding software when checking at issuance.

Conclusion:
Accepted

Clarification:
To prevent these kinds of problems it is suggested to perform a one-time check of the JPEG2000 image encoded data using reference software which has been specified at ISO/IEC 15444-5:2003/Amd 12003 Reference software for the JPEG2000 file format.
This reference software is specified at the JPEG committee home page as a public domain.
http://www.jpeg.org/jpeg2000/j2kpart5.html

- JasPer (C) version 1.700.2 or later
- JJ2000 (Java) version 5.1 or later

R6-p1_v2_sIII_0053

Reference:
Doc9303, Part 1, Vol2, Section III, 12.1.2.

Issue:
In Doc9303 Part 1, Volume 2, Section III the specification of DG11 states that characters to be used are A, S resp. A, N, S. This contradicts with the intention of DG11, which is to allow for national characters to overcome the limitations in DG1 set by MRZ rules.

Conclusion:
Accepted

Clarification:
In line with Appendix A.13.6 ("DG11 may contain non-latin characters") the characters to be used are A, S, B resp. A, N, S, B. This is to be able to incorporate national characters as specified in ISO/IEC 10646.

R6-p1_v2_sIII_0054

Reference:
Doc9303, Part 1, Vol2, Section III, Appendix 1, A.13.3.

Issue:
The table in A.13.3 contains an error. The TAG value for the first instance of "Validity period" must be '85' instead of '84'.

Conclusion:
Accepted

Clarification:

R6-p1_v2_sIII_0055

Reference:
Doc9303, Part 1, Vol2, Section III, Appendix 1, A.13.2.

Issue:
The example in A.13.2 (John Smith) contains an error. It appears that the document number exceeds 9 characters (according to the '<' sign in the check digit position). In this case '0121' in field 12 would be the continuation, meaning that the document number is 123456789012 with check digit 1.

Conclusion:
Accepted

Clarification:
This is an error in the example. According to Part 1, Volume 1, Section IV, paragraph 9.7, the document number in a passport book can not exceed 9 characters.

R7-p1_v2_sIII_0056

Reference:
Doc9303, Part 1, Vol2, Section III, paragraph 2.1.

Issue:
In Doc9303, Part 1, Vol2 the lists of reference documentation in Section III, paragraph 2.1 and Section IV, paragraph 4 contain references to documents, not referenced to in other parts of Volume 2. Also some documentation has been revised, as a result of which referenced dates have changed. An updated list of reference documentation is desirable.

Conclusion:
Accepted

Clarification:
In case of doubt the reader MAY use to the reference documentation listed in paragraph 1.4 of this Supplement as the reference documentation to be used in conjunction with Doc 9303. It SHOULD however be noted that these editorial addenda in no way affect, or interfere with, the specifications set out in Doc 9303 Part 1, Sixth edition.

R7-p1_v2_sIII_0057

Reference:
Doc9303, Part 1, Vol2, Section III, 12.1.1 and Appendix 1, A.13.3.
Also Supplement issue R7-p3_v2_sIII_0011.

Issue:
Doc9303 specifies the encoding of secondary biometrics in DG3 and DG4. The table in Vol2, Section III, 12.1.1 specifies that the number of fingers in DG3 and irisses in DG4 can be '1..9'. Are the values '0' and '10' excluded? There is a need for clarification on the encoding of 0, 1, and more than 1 instances of the biometric features in DG3 and DG4.

Conclusion:
Accepted

Clarification:
With respect to the encoding of DG3 and DG4 a guideline has been issued: WG3TF5_N0045 "A technical guideline for a compliant and interoperable coding of Data Group 3", version 1.3, 17-09-2007. For an interoperable coding of DG3 and DG4 this guideline MUST be followed.
The following clarifications from the guideline have been specifically addressed by the NTWG:

Number of instances.
The number of instances in DG3 and DG4, specified in Doc9303, Part 1, Vol2, Section III, 12.1.1 is to be corrected. The correct specification is '0..n'.

Encoding of zero instances.
States, not issuing eMRTDs with fingerprints or irises SHOULD NOT store DG3 at all.
For interoperability reasons States supporting fingerprints and/or irises in their eMRTDs MUST store an empty Biometric Information Group Template in cases where no fingerprints or irises are available. The template counter denotes a value of '00' in this case.
A Data Group 3 or 4 of this structure has the drawback that it will result in a static DG3 or DG4 hash in the SO_D for all eMRTDs where the biometric features are not present.
This allows distinguishing whether or not an EAC-protected passport contains fingerprints and/or irises just by performing BAC and thus, it makes those passports without fingerprints an interesting target for e.g. imposters.
To overcome this problem it is RECOMMENDED to add tag '53' with issuer defined content (e.g. a random number).

63	***Var***	LDS element			
	7F 61	***03***	Biometric Information Group Template		
		02	01	00	Defines that there are no Biometric Information Templates stored in this data group.
	53	*Var*	issuer defined content (e.g. a random number).		

Encoding of one instance.

In cases where only one fingerprint or iris is available, from a technical point of view no Biometric Information Group Template is required. However for the sake of consistency and to achieve interoperability, the single instance MUST be encoded in the following way (example for DG3 – fingerprint).

63	*aa*	LDS element where *aa* is the total length of the entire LDS data content					
	7F 61	*bb*	Biometric Information Group Template, where *bb* is the total length of the entire Group Template content.				
		02	01	01	Defines the total number of fingerprints stored as Biometric Information Templates that follow.		
		7F 60	*cc*	First biometric information template where *cc* is the total length of the entire BIT			
			‘A1’	*dd*	Biometric Header Template, where *dd* is the total length of the BHT		
				81	01	08	Biometric type “Fingerprint”
				82	01	0A	Biometric subtype “left pointer finger”
				87	02	01 01	Format Owner JTC 1 SC 37
				88	02	00 07	Format Type ISO/IEC 19794-4
				Note that the BHT may contain additional optional elements. Of course, this fingerprint can either be a left or right finger depending on the available image.			
			5F 2E	*ee*	Biometric Data Block where *ee* is total length of the encoded ISO 19794-4 structure. The Biometric Data Block MUST contain exactly one fingerprint image.		

Encoding of more than one instance.

There are two possible ways to store more than one instance. They can be either stored within multiple Biometric Information Templates or inside a single Biometric Data Block using the ISO/IEC 19794 format.

While both ways are possible from the technical point of view, for an interoperable solution each feature MUST be stored in an individual Biometric Information Template. The feature position MUST be specified within the CBEFF biometric subtype if this information is available. The following table contains a worked example for the CBEFF encoding of an interoperable DG 3 element with two fingerprint images.

63	*aa*	LDS element where *aa* is the total length of the entire LDS data content					
	7F 61	*bb*	Biometric Information Group Template, where *bb* is the total length of the entire Group Template content.				
		02	01	02	Defines the total number of fingerprints stored as Biometric Information Templates that follow.		
		7F 60	*cc*	First biometric information template where *cc* is the total length of the entire BIT			
			‘A1’	*dd*	Biometric Header Template, where *dd* is the total length of the BHT		
				81	01	08	Biometric type “Fingerprint”
				82	01	0A	Biometric subtype “left pointer finger”
				87	02	01 01	Format Owner JTC 1 SC 37

				88	02	00 07	Format Type ISO/IEC 19794-4
				Note that the BHT may contain additional optional elements. It is also possible that the order of fingerprints (left/right) is different.			
			5F 2E	*ee*	Biometric Data Block where *ee* is total length of the encoded ISO 19794-4 structure. The Biometric Data Block MUST contain exactly one fingerprint image.		
		7F 60	*ff*	Second biometric information template where *ff* is the total length of the entire BIT			
			'A1'	*gg*	Biometric Header Template, where *gg* is the total length of the BHT		
				81	01	08	Biometric type "Fingerprint"
				82	01	09	Biometric subtype "right pointer finger"
				87	02	01 01	Format Owner JTC 1 SC 37
				88	02	00 07	Format Type ISO/IEC 19794-4
				Note that the BHT may contain additional optional elements. It is also possible that the order of fingerprints (left/right) is different.			
			5F 2E	*hh*	Biometric Data Block where *hh* is total length of the encoded ISO 19794-4 structure. The Biometric Data Block MUST contain exactly one fingerprint image.		

R7-p1_v2_sIII_0058

Reference:
Doc9303, Part 1, Vol2, Section III, Appendix 1, A.13.6 and A.13.7.
Also Supplement issue R7-p3_v2_sIII_0013.

Issue:
According to Doc9303, Part 1, Vol2, Section III, 12.1.2 and 12.1.3 the dates in DG11 and DG12 must be encoded in 8 numeric characters. But the tables in Appendix A.13.6 and A.13.7 mention 4 Byte BCD encoding. These inconsistencies seem to be errors in the tables.

Conclusion:
Accepted

Clarification:
All dates are encoded in numeric characters. In the tables in A.13.6 and A.13.7 the addition "(BCD encoding)" must be discarded and the corresponding length fields must be corrected to '08'.
Since the LDS specifications have not been unambiguous with respect to date formats, it is RECOMMENDED that Inspection Systems support both 8 bytes ASCII and BCD.

R7-p1_v2_sIII_0059

Reference:
Doc9303, Part 1, Vol2, Section III, Appendix 1, A.13.7.
Also Supplement issue R7-p3_v2_sIII_0014.

Issue:
The description of encoding DG12 is not consistent with the encoding of DG11, although one should expect it to be.
The table is not consistent in using the terms **people** and **person**.
The example should be corrected.

Conclusion:

Accepted

Clarification:
In the table the tags ‘A0’, ‘02’ and ‘5F1A’ belong to each other. To reflect this, their value descriptions must be as follows:

‘A0’	X	Content-specific constructed data object of other **persons**
‘02’	01	Number of other **persons**
‘5F1A’	X	Name of other person formatted per Doc 9303 rules. **The data object repeats as many times as specified in the ‘02’ element.**

The example of encoding DG12 must be as follows:
‘**6C**’ ‘45’
‘**5C**’ ‘06’ ‘**5F19**’ ‘**5F26**’ ‘**5F1A**’
‘**5F19**’ ‘18’ UNITED STATES OF AMERICA
‘**5F26**’ ‘08’ 20020531
‘**0A**’ ‘15’
‘**02**’ ‘01’ ‘01’
‘**5F1A**’ ‘0F’ SMITH<<BRENDA<P

R10-p1_v2_sIII_0060

Reference:
Doc9303, Part 1, Vol2, Section III, paragraph 12.1.2.

Issue:
The encoding of DG11 allows for the use of A (Alpha character (a-z, A-Z)), N (Numeric character 0-9) and S (Special character (‘<’, ‘ ’)).
To comfort the use of more than just the latin character set it is suggested to change this specification into B (8-bit binary data (Unicode)).

Conclusion:
Accepted

Clarification:
In DG11 the type of coding of data elements 01, 02, 04, 05, 08, 09, 10 and 13 shall be specified as B in the table (column “type of coding”).

R11-p1_v2_sIII_0061

Reference:
Doc9303, Part 1, Vol2, Section III, paragraph 12.1.2.
Also Supplement issue R11-p3_v2_sIII_0015.

Issue:
According to ICAO 9303 Part 1 Vol 2 §12.1.2, the date of birth stored in the DG11 shall be full (complete) and encoded as CCYYMMDD with Numeric characters ([0…9]). It is not defined how a unknown date of birth shall be encoded here. Specifying the data element to be numeric doesn’t allow for the solution as specified for the MRZ (as well as DG1), using the special character ‘<’ on the unknown positions (see Doc9303 Part 1 Volume 1 Section IV paragraph 15.2.2).

Conclusion:
Accepted, see clarification.

Clarification:

In case, the month (MM) or the day (DD) are unknown, the interoperable way to indicate this in DG11 is to set the respective characters to '00'. In case, the century and the year (CCYY) are unknown, the interoperable way to indicate this in DG11 is to set the respective characters to '0000'. Issuer-assigned dates must always be used consistently.

3.2.4 Section IV - PKI for machine readable travel documents offering ICC read-only access

R1-p1_v2_sIV_0002

Reference:

Issue:
TLV structured example of SO_D.
The Document Security Object (SO_D) has been described in ASN.1 format. For clarification it has been requested to provide a TLV structured example.

Conclusion:
Accepted.

Clarification:
See Appendix A to this supplement.

R1-p1_v2_sIV_0003

Reference:

Issue:
Ability to verify authenticity/integrity of individual biometrics, e.g. one finger.
If more than one finger is stored in DG3, but only one finger is read for verification, it is not possible to verify its authenticity/integrity

Conclusion:
Work item for TR-PKI V2.

Clarification:
True: to verify authenticity/integrity the entire DG must be read.
ICAO PKI offers no possibility to verify authenticity/integrity of 'parts' of DGs.
ICAO LDS offers no possibility to use CBEFF signatures.
Are the security options in CBEFF structure applicable here?

R1-p1_v2_sIV_0006

Reference:

Issue:
TAG list not signed in EF.COM.
The Data Group Presence Map (DGPM) contains information to enable countries or approved receiving organisations in the countries to determine which Data Elements are present in the Data Group in the LDS of the MRTD.
In Form1 of the DGPMs, the TAGs are not signed, unlike the Document Security Object (SOD) in the MRTD chip. The SOD is digitally signed by the issuing country's Document Signer Private Key (KPRDS); with the Document Signer Public Key (KPUDS), or the Document Signer Certification (CDS), a border control inspection system will be able to authenticate that the content of the LDS.
As the TAG list of the DGPM is unsigned, there is no means to preserve the integrity of the TAG list. One possible attack scenario would be to modify the TAG list and the modification may be undetected.

As an illustration, the TAG list can be changed to show the absence of finger and/or iris biometric identifiers (DG 3 and DG4 respectively). Coupled with a look-alike attack, the holder of the MRTD would be able to fool the border control inspection control with the fake identity. Although there could be software countermeasures at the inspection system, e.g. perform a compare of the TAG list against that of the SOD, the design is not inherently strong and is prone to coding errors.

Conclusion:
Rejected.

Clarification:
EF.COM and EF.SOD are not data groups and, hence, are not in the tag list.
Authenticity, integrity and completeness of the LDS data should be verified using the Document Security Object and not the EF.COM, as a matter of good inspection system design.

R1-p1_v2_sIV_0007

Reference:

Issue:
Alternative for Basic Access Control.
An alternative solution is to implement a simple physical shielding mechanism that will counter skimming attacks. A pouch, with one portion made of anti-skimming material, is attached to the passport. When the passport booklet is closed, the pouch protects the chip against skimming attacks. When the passport booklet is open, the chip will then be available for read.

Conclusion:
Noted.

Clarification:
Shielding can prevent skimming. However, Basic Access Control is to prevent both skimming and eavesdropping. The physical shielding does not protect against eavesdropping.

R1-p1_v2_sIV_0008

Reference:

Issue:
DES to be de-certified.
NIST is proposing to de-certify DES from FIPS standards as it is assessed to no longer be secure. The implication is that if ICAO operations would to have any DES dependency, chip OS, product continuity cum support and security would be impacted. DES is currently used as part of CWA 14890-1, which is heavily referenced for secure messaging used in Basic Access Control.

Conclusion:
Accepted.

Clarification:
It is RECOMMENDED to use 3-DES.

R1-p1_v2_sIV_0009

Reference:

Issue:
Hash values for each EF.DGn are connected in EF.SOD, but it is not defined how to connect the hash values – conform to order of Tag list or list in ascending order.

Conclusion:
See clarification.

Clarification:
Connected by Data Group Number in Security Object.

R1-p1_v2_sIV_0010

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, Appendix 5, A5.3.

Issue:
After BAC, it is not clear whether to use a secure messaging or not for all commands and its responses.
One of ideas is use for only READ BINARY command. There seems not to be the need about the SELECT command.
For avoiding such idea, it shall be described clearly for the TR to use a secure messaging for all commands / response after BAC.
Proposal:
It should be added the above sentence to E for interoperable management.

Conclusion:
Rejected.

Clarification:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, Appendix 5, A5.3 states that 'All further communication MUST be protected by Secure Messaging in MAC_ENC mode'.
This must be interpreted as: Secure Messaging MUST be used for ALL commands and responses.

R1-p1_v2_sIV_0014

Reference:
See Supplement issue R8-p1_v2_sIV_0059.

Issue:
A CRL distribution mechanism should be described.

Conclusion:
Accepted.

Clarification:
See Appendix C to this supplement for a proposed distribution mechanism for CSCA certificates and CRLs.

R1-p1_v2_sIV_0017

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, 5.8.1

Issue:
Integration of the "Extended Access" protocol.

Conclusion:
Work item for TR-PKI V2.

Clarification:
A proposal about possible EAC protocols, submitted by DIN, has been withdrawn. An EU proposal is being developed.

R1-p1_v2_sIV_0021

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, 9.5.
Also Supplement issue R6-p3_v2_sIV_0001.

Issue:
There is no description about the usage of ARL (Authority Revocation List). If the usage of ARL is included in ICAO PKI scheme, detailed operation relating bilateral and PKD-based exchange needs to be specified.

Conclusion:
Rejected.

Clarification:
For Authority Revocation an ARL can be used, but this is not necessary. The existing CRL can be used for Authority revocation.

R1-p1_v2_sIV_0024

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, Appendix 5, A5.3.

Issue:
After a successful execution of the authentication protocol both the IFD and the ICC compute session keys KS_ENC and KS_MAC using the key derivation mechanism described in *Doc 9303-part 1-sixth edition: Volume 2, Section IV, Appendix 5, A5.1* with (K.ICC xor K.IFD) as key seed. All further communication MUST be protected by Secure Messaging in MAC_ENC mode.

1.
If the IFD send a command to the ICC without Secure Messaging does the ICC need to response? I.e. is it allowed also to answer to commands without secure messaging?
2.
If No then what is the ICC response in this case (i.e. error type and value)? The error response is encapsulated in secure messaging response?.

Conclusion:
See clarification.

Clarification:
1.
See R1-p1_v2_sIV_0016:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, Appendix 5, A5.3.2 states that 'Note: Further SM status bytes can occur in application specific contexts. When the ICC returns status bytes without SM DOs or with an erroneous SM DO the ICC deletes the session keys. As a consequence the secure session is aborted.'
In other words, if an error occurs the session is aborted.
2.
Response of the ICC can be 0x6987 or 0x6988. This response is in plain mode because the SM channel is terminated as consequence of the error.

R1-p1_v2_sIV_0026

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, Appendix 4, A4.2.
Also Supplement issue R6-p3_v2_sIV_0002.

Issue:
Active Authentication.

Does the ICC use the RND.IFD which has been provided in the BAC process or it is a new value? If this is a new value we recommend a special note like RND**2**.IFD.

Conclusion:
See clarification.

Clarification:
It is not specified that the ICC should use the RND.IFD that was provided in the BAC process, neither that it should be a new value.

R1-p1_v2_sIV_0027

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, Appendix 4, A4.2.
Also Supplement issue R6-p3_v2_sIV_0003.

Issue:
The Active Authentication uses the Internal Authentication command, Does this command should be send to the ICC with Secure Messaging?

Conclusion:
See clarification.

Clarification:
If Basic Access Control is applied, yes.

R1-p1_v2_sIV_0028

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, Appendix 4, A4.2.

Issue:
Active Authentication.
Does the required implementation is 4A – Total recovery header or 6A – Partial recovery?

Conclusion:
See clarification.

Clarification:
'6A'. The known part (RND.IFD) is not returned, but must be appended by the IFD itself. So Partial Recovery.

R1-p1_v2_sIV_0029

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, Appendix 4, A4.2.
Also Supplement issue R6-p3_v2_sIV_0004.

Issue:
Active Authentication.
Does the signature response is with Secure Messaging? i.e. encrypting the Σ with KS_ENC and concatenation of the MAC with KS_MAC and adding the SW (90,00) encapsulate?

Conclusion:
See clarification.

Clarification:
If Basic Access Control is applied, yes.

R2-p1_v2_sIV_0033

Reference:

Issue:
Odd INS commands with Secure Messaging.
It is hard to find justification for using exactly the same security mechanisms for confidentiality with even and odd INS commands because of the clear wording of clauses 6.4 and 7.2.2 of the ISO/IEC 7816-4:2005, albeit its convenience.

Conclusion:
Accepted (TF5; 2006-06-06).

Clarification:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, Appendix 5, A5.3.1 should be extended with DO '85' for file sizes > 32k.

Message structure of SM APDUs:
The SM Data Objects MUST be used according to the table below in the following order:
- Command APDU: [DO'85' or DO'87'] [DO'97'] DO'8E'.
- Response APDU: [DO'85' or DO'87'] [DO'99'] DO'8E'.

All SM Data Objects MUST be encoded in BER TLV as specified in ISO/IEC 7816-4. The command header MUST be included in the MAC calculation, therefore the class byte CLA = 0x0C MUST be used.

The actual value of Lc will be modified to Lc' after application of Secure Messaging. If required, an appropriate data object may optionally be included into the APDU data part in order to convey the original value of Lc. In the protected command APDU the *new Le* byte MUST be set to '00'.

	DO'85' *	**DO'87' ***	**DO'97'**	**DO'99'**	**DO'8E'**
Meaning	Cryptogram (plain value encoded in BER-TLV, but not including SM data objects)	Padding-content indicator byte ('01' for ISO-Padding) followed by the cryptogram	Le (to be protected by CC)	Processing status (SW1-SW2, protected by MAC)	Cryptographic checksum (MAC)
Command APDU	Mandatory if data is send, otherwise absent.	Mandatory if data is send, otherwise absent.	Mandatory if data is requested, otherwise absent.	Not used	Mandatory
Response APDU	Mandatory if data is returned, otherwise absent.	Mandatory if data is returned, otherwise absent.	Not used	Mandatory if data is absent, otherwise optional (however usage is recommended)	Mandatory

Usage of SM Data Objects

* DO'85' (odd INS byte) or DO'87' (even INS byte) is used

R2-p1_v2_sIV_0035

Reference:
See Supplement issue R8-p1_v2_sIV_0059.

Issue:
CSCA Certificates bilateral exchange.
CSCA Certificates must be exchanged bilaterally by diplomatic means. A protocol for this exchange should be defined.

Conclusion:
Accepted.

Clarification:
Initial exchange of Country Signing CA Certificates shall be diplomatic. That is, countries exchanging certificates shall:

- Agree upon representatives for initial key exchange.
- Determine the appropriate mechanism for key exchange (e.g. diplomatic pouch or through some existing trusted mechanism)
- Exchange certificates
- Test certificates against a Document Signer Certificate shared through a separate mechanism

Further Country Signing CA Certificate exchange between two nations could happen in a more simple manner if link certificates are used at renewal.

R2-p1_v2_sIV_0037

Reference:

Issue:
BAC Additional Entropy.
It is suggested that 20 additional bits of entropy be added to the seed mechanism.

Conclusion:
Rejected.

Clarification:
The NTWG determined that this issue should be referred to TF5 for further examination.
In its meeting in February 2006 in Rome, the NTWG discussed several options, presented by TF5. After balancing all the options in relation to the existing specifications and consequences for present implementations of e-passports, the NTWG concluded not to change the specifications and recommended that member States, who wish to enlarge the entropy, implement their own measures within the current specifications, such as generating their document numbers in a random way.

R3-p1_v2_sIV_0038

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, Appendix 1, A1.2

Issue:
The certificate profile contains an error. It specifies pathlenConstraint = ‘1’ for linked certificates. pathlenConstraint must always be ‘0’.

Conclusion:
Accepted.

Clarification:
pathlenConstraint must always be ‘0’.

R3-p1_v2_sIV_0039

Reference:

Issue:
SHA_1:
Not to be recommended anymore.

Conclusion:
Noted.

Clarification:
The issue concerns only hash collisions, which already have been described in the risk analysis *Doc 9303-part 1-sixth edition: Volume 2, Section IV, Appendix 7, A7.4.2*.
The risk analysis should be followed, bearing in mind that such a collision attack requires full control over the data to be signed.

R3-p1_v2_sIV_0040

Reference:

Issue:
ECDSA:
Refer to ISO 15946: Choice of curves to be used.

Conclusion:
Accepted.

Clarification:
For ECDSA, next to the reference to **ANSI X9.62**, implementers MUST also acknowledge **ISO/IEC 15946-1&2** as a reference. ISO/IEC 15946 is largely copied from ANSI X9.62. The difference is, that ANSI X9.62 only defines SHA_1 as hashing algorithm to be used, where ISO/IEC 15946 defines hashing algorithms >SHA_1. Therefore, referring to X9.62 ***and*** ISO/IEC 15946 provides allowance for use of all hashing algorithms, mentioned in both standards. Hashing algorithms to be used have been specified in the ICAO specifications, which are not affected by adding the reference for ECDSA with ISO/IEC 15946. Therefore there are no consequences for existing implementations of eMRTDs and inspection systems.
An implementer's guidance document on ECDSA ('WG3TF5_N0034 TR03111_TechnicalGuideline_ECC') has been published on the WG3 website.

R3-p1_v2_sIV_0041

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, 7.2.2.

Issue:
Basic Access Control.
To authenticate the inspection system it reads the 'MRZ_information' consisting of the concatenation of Document-Number, Date-of-Birth and Date-of-Expiry, including their respective checkdigits from the MRZ using an OCR-B reader. Alternatively, the required information can be typed in as it appears in the MRZ. The most significant 16 bytes of the SHA-1 hash of this 'MRZ_information' is used as key seed to derive the Document Basic Access Keys.

For ID-1 size documents, it is now a bit unclear, how the situation is handled, when the document number exceeds 9 characters, meaning that '<' character is placed in the following check digit field, and the remaining document number digits are placed in the optional data field, immediately followed by the document number check digit. Note that this applies only to ID-1 size documents. So, the question is, are the document numbers + check digit found in the optional data field incorporated into the "MRZ Information" constructing for the hash calculation?

Conclusion:
See clarification.

Clarification:
The specification states that one must use Document Number, Date of Birth and Date of Expiry, "as it appears in the MRZ".

According to *Doc 9303-part 1-sixth edition: Volume 1, Section IV, 9.7* concerning **(ID3)** passport books, the Document Number is always 9 characters.
According to *Doc 9303-part 3-second edition: Section IV, 6.5 (ref. note j)* concerning **(ID1)** passport cards, the Document Number can exceed 9 characters.

Therefore the issue only applies for ID1 and for this the interpretation should be: Use the entire document number by concatenation of the first part (9 characters) and the second part (in the optional data field), including the check digit (following the second part), but without the '<' sign, that indicates the long document number.
The following is an example of an ID-1 size MRZ with a document number with more than 9 characters:

I<UTOD23145890<7349<<<<<<<<<<
3407127M9507122UTO<<<<<<<<<<2
STEVENSON<<PETER<JOHN<<<<<<<<

Document number = D23145890734, check digit = 9
Date of Birth = 340712, check digit = 7
Date of Expiry: = 950712, check digit = 2

MRZ_information = **D2314589073493**4071279507122

R3-p1_v2_sIV_0042

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Appendix 5, A5.3.2.
Also Supplement issue R6-p3_v2_sIV_0005.

Issue:
During some experiments regarding the Secure Messaging, the following question arose:
„How does the ICC react if it is not able to respond as much data as requested by the Le data object (DO '97') in the command APDU?"
This could happen in the case of READ BINARY with e.g. a zero or empty Le data object (DO '97') requesting the maximum, i.e., 256 plain data bytes (see chapter 6.4 of ISO/IEC 7816-4). Due to the protection of the response APDU with secure messaging its length would exceed 256 Bytes, which is not supported by some ICC operating systems.
In the experiments different behaviors, like responds with several different errors or responds with several different lengths, could be observed.

Therefore we propose to clarify this situation by adapting *Doc 9303-part 1-sixth edition: Volume 2, Appendix 5, A5.3.2* as follows:

"SM specific Status Bytes

When the ICC recognizes an SM error while interpreting a command, then the status bytes must be returned without SM. In ISO/IEC 7816-4 the following status bytes are defined to indicate SM errors:
• ´6987´: Expected SM data objects missing

• ´6988´: SM data objects incorrect
If due to APDU size limitations of the ICC, it is not able to respond as much data as requested by the command APDU, the protected response APDU shall contain only as much plain data bytes as possible and indicate this with the warning:
• ´6287´: less data responded than requested.

This could happen for ICCs not supporting response APDUs exceeding a length of 256 Bytes which could occur due to the protection with secure messaging.
In the case of a warning the secure session is not affected and the following READ BINARY needs to increase the offset for reading corresponding to the received response.

Note: Further SM status bytes can occur in application specific contexts. When the ICC returns status bytes without SM DOs or with an erroneous SM DO the ICC deletes the session keys. As a consequence the secure session is aborted."

Conclusion:
Rejected.

Clarification:
This proposal uses a new warning which is not standardized in ISO/IEC 7816.
As the correct response of an ICC in such a situation is currently under discussion in SC17 WG4 no requirements for the PICC can be specified. The inspection system SHOULD avoid such a situation by requesting only an amount of plain data bytes where the secured response for this amount of plain data does not exceed 256 bytes.

R3-p1_v2_sIV_0043

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Appendix 5, A5.3.

Issue:
It is described that after the authentication protocol a secure messaging session begins. To also explain under which conditions this session will end, we propose to make the following adaptation:
"After a successful execution of the authentication protocol both the IFD and the ICC compute session keys KS_ENC and KS_MAC using the key derivation mechanism described in Annex E.1 with (K.ICC xor K.IFD) as key seed. All further communication MUST be protected by Secure Messaging in MAC_ENC mode.
The session ends

- when another authentication is started,
- when the ICC is depowered or reset,
- when the ICC aborts the command execution due to an execution or checking error,
- when the ICC deselects the LDS application, i.e. selects the LDS application or the MF."

Conclusion:
Accepted with changes.

Clarification:
ICAO specifications only consider the issuer (LDS) application and do not provide specifications for multi application cards.
Abortion of the Secure Channel for the issuer (LDS) application occurs when:

- the chip is de-powered.
- the ICC recognizes an SM error while interpreting a command. In this case the status bytes must be returned without SM. These can be the following status bytes:
  - ´6987´: Expected SM data objects missing
  - ´6988´: SM data objects incorrect

Note: There MAY be other circumstances in which the ICC aborts the session. At this point in time it is not feasible to create a complete list of situations in which the ICC aborts the session. At least 6987 and 6988 come with SC abortion, but there may be other situations. A list may be drawn-up from practical experiences for TR-PKI V2.

R3-p1_v2_sIV_0044

Reference:

Issue:
Currently in the PKCS#1 v2.1 the RSASSA-PSS-parameters for signature is defined as follows:

```
RSASSA-PSS-params ::= SEQUENCE {
   hashAlgorithm [0] HashAlgorithm DEFAULT sha1,
   maskGenAlgorithm [1] MaskGenAlgorithm DEFAULT mgf1SHA1,
   saltLength [2] INTEGER DEFAULT 20,
   trailerField [3] TrailerField DEFAULT trailerFieldBC
}
```

This ASN.1 definition means that if the DEFAULT values are used for parameters, then these fields are not included in the corresponding DER coding.
Earlier in the same document is stated:
a) **saltLength** is the octet length of the salt. It shall be an integer. For a given **hashAlgorithm**, the default value of **saltLength** is the octet length of the hash value. Unlike the other fields of type **RSASSA-PSS-params**, **saltLength** does not need to be fixed for a given RSA key pair.

This is a bit confusing, because the “default” word is also used in this context. In the ASN.1 definition, the only DEFAULT value is “20”, despite the used hash algorithm.

In other words, if you are using SHA-256 as a hash-algorithm, according to the text in a), the “default value of **saltLength**” is the 32. And when you are going to DER code the corresponding parameter

- the ASN.1 definition says that the only DEFAULT value is “20”
- this means that if 32 is used as **saltLength**, it is not the DEFAULT value in the DER coding sense
- and this means that is must be included into DER coding.

Our recommendation is to clarify this in the supplement.

Conclusion:
Accepted.

Clarification:
Refer to the RFC 4055, which clarifies the situation in the DER coding sense, saying:

- The **saltLength** field is the octet length of the salt. For a given **hashAlgorithm**, the recommended value of **saltLength** is the number of octets in the hash value. Unlike the other fields of type **RSASSA-PSS-params**, **saltLength** does not need to be fixed for a given RSA key pair; a different value could be used for each RSASSA-PSS signature generated.

In this text the “default” word is replaced by “recommended”, which doesn’t confuse the DER coding any more.

R4-p1_v2_sIV_0045

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Appendix 1, A1.4.

Issue:

The description regarding the public key encoding in Country Signing CA certificates and Document Signer certificates refers to RFC3279.
This referred standard RFC3279 was updated with RFC4055 *"Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"* in June 2005. In the section 1.2 of this new version, the conventions for using the RSA Probabilistic Signature Scheme (RSASSA-PSS) have been described as below.

> *When the RSA private key owner wishes to limit the use of the public key exclusively to RSASSA-PSS, then the id-RSASSA-PSS object identifier MUST be used in the algorithm field within the subject public key information, and, if present, the parameters field MUST contain RSASSA-PSS-params.*

This means the public key used for the document signing with RSASSA-PSS must set "id-RSASSA-PSS" in "subjectPublicKeyInfo.algorithm.identifier", and set "RSASSA-PSS-params" in "subjectPublicKeyInfo.algorithm.parameters".
As ICAO-PKI TR recommends RSA-PSS and specifies the key usage of both CSCA certificates and DS certificates as signing only, this update should be reflected.

Conclusion:
Rejected.

Clarification:
Complying with RFC4055 does not prevent to handle RFC3279 based certificates, which are signed with RSA and encoded in RSA-PSS signature mechanism. The related statement is also in the section 1.2 of RFC4055 as below.

> *The rsaEncryption object identifier continues to identify the subject public key when the RSA private key owner does not wish to limit the use of the public key exclusively to either RSASSA-PSS or RSAES-OAEP.*

Changing the reference into RFC4055 would provide the possibility to limit the usage of keys. The only difference is in the OID. This would require a minimal change to inspection systems.
Based on this, NTWG in its meeting in February 2006, rejected the proposal.

R4-p1_v2_sIV_0046

Reference:

Issue:
Verify if it is possible to successfully perform unsecured SELECT on BAC protected e-Passports

Conclusion:
See clarification.

Clarification:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, 7.2.2 states:
"A MRTD chip that supports Basic Access Control MUST respond to unauthenticated read attempts (including *selection* of (protected) files in the LDS) with 'Security status not satisfied' (0x6982)."
It is however recognized that certain ICC operating systems support an unsecured SELECT before the BAC secure messaging is established. Therefore, when no secure channel is established, both 6982 and 9000 should be expected as ICAO compliant responses to an unsecured SELECT. See this Supplement, R1-p1_v2_sIII_0028, option 2 and option 3, where the determination of BAC presence is described.

When, and as long as the BAC secure channel is present all further communication MUST be protected by Secure Messaging, as stated in *Doc 9303-part 1-sixth edition: Volume 2, Section IV, Appendix 5, A5.3.*
As a consequence, sending an unprotected SELECT in the secure channel containing existing LDS file ID, BAC secure session is aborted (one cannot read the contents of the file any more, like stated in R3-p1_v2_sIV_0043), but one can still SELECT existing file with response code '90 00', like you could do in the beginning, before BAC session was established in the first time.

R4-p1_v2_sIV_0047

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, 7.1.

Issue:
Make a clear definition of "personalization process SHOULD lock the chip".
What is exactly meant by "locking the chip"?
Does it read that locking the chip is not mandatory? Can it (if not locked) be written to after personalization?

Conclusion:
See clarification.

Clarification:
The term "lock" in this context has the following implications:
Once the chip has been locked (after personalization and before issuance) no data can be written, modified, or deleted to/at/from the chip anymore. After issuance a locked chip cannot be unlocked.
On this principle the PKI Technical Report is based ("PKI for Machine Readable Travel Documents offering ICC read-only Access").
Mechanisms for secure writing to the chip after issuance may be developed in the course of the PKI Technical Report Version 2.

RFC 2119, *S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, March 1997*, states about the key word SHOULD (see Appendix B to this supplement):
This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
Bearing this in mind an issuing state in principle has the possibility to leave the chip unlocked and, therefore, leave the possibility open to write to it afterwards, but should weigh the implications of such a decision very carefully.

R4-p1_v2_sIV_0048

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Appendix 4, A4.2.

Issue:
For Active Authentication signature generation, ISO/IEC 9796-2, scheme 1 is referenced. In 9796-2 there are two possible signature production functions (chapter A4 "Signature production function" and chapter A6 "Alternative signature production function"). Which function has to be used?

Conclusion:
See clarification.

Clarification:
In the implementation of Active Authentication in e-MRTDs, the signature generation scheme as described in ISO/IEC 9796-2, paragraph A.6. MAY be used, and is expected to be the most common

implementation. Inspection systems however SHOULD be prepared for e-MRTDs, supporting an Active Authentication signature, generated as described in ISO/IEC 9796-2, paragraph A.4.

The inspection system should support A4 signature verification.

The reasons for this stance are two-fold:

- The signature verification method implies checking of the last 4 bits (or, since the signature contents before exponentiation will contain BC as last byte, the last 8 bits) to choose which signature creation method was used. This implies that A6 is automatically supported by the verification method supporting A4. (*1)
- If the AA signature is generated using A6, and the inspection system uses A4 for the verification, then the inspection system must not explicitly check that the signature is a string of k-1 bits (first sentence of paragraph A.5 in ISO 9796-2), because if the signature is generated using A6, then the signature can be a string of k bits (k is the bit length of modulus).

(*1) The method of message recovery in the case of method 2, A4 can be found in D.1.2.2.1 of ISO 9796-2 (... since it is congruent to (n - 12) mod 16 ...), where 12 obviously points to the usage of the value BC or CC in the last byte, although this uses RIPE instead of SHA.

R5-p1_v2_sIV_0049

Reference:
Doc 9303-part 1-sixth edition: Volume 2, 5.6.1 and 7.2.

Issue:
It is stated in Section 5.6.1 that for Passive Authentication it is sufficient to read the Document Signer Certificate from the MRTD chip. Although Section 7.2 makes it mandatory to store the Country Signing CA Certificates in the inspection system, the procedure for verifying the Document Signer Certificate is left out.

Conclusion:
Accepted.

Clarification:
See red-marked additions to original text)

In 7.2.1 under '*For Passive authentication*' the text should be read as follows:

To be able to perform a passive authentication of the data stored in the MRTD's chip, the inspection system needs to have knowledge of key information of the issuing States:

1. Of each participating issuing State, the Country Signing CA Certificate (C_{CSCA}) SHALL be stored in the inspection system.
2. Of each participating issuing State, the Document Signer Certificate (C_{DS}) SHALL be stored in the inspection system.

Before using a Document Signer Certificate (C_{DS}) for verification of a SO_D, the inspection system SHALL verify its digital signature, using the Country Signing CA Public Key (KPu_{CSCA}).

In 7.2.2 under '*Passive authentication*' the text should be read as follows:

The inspection system performs the following steps:

1. The Document Security Object (S_{OD}) (OPTIONALLY containing the Document Signer Certificate (C_{DS})) is read from the chip.

2. The Document Signer (DS) is read from the Document Security Object (S_{OD}).

3. The digital signature of the Document Security Object (S_{OD}) is verified by the inspection system, using the Document Signer Public Key (KPu_{DS}). The Document Signer Certificate (C_{DS}) for this key is stored in the inspection system as downloaded from the ICAO PKD and MAY also be stored in the MRTD's chip. This ensures that the Document Security Object (S_{OD}) is authentic, issued by the authority mentioned in the Document Security Object (S_{OD}), and unchanged. Thus the contents of the Document Security Object (S_{OD}) can be trusted and SHOULD be used in the inspection process.
   Before using a Document Signer Certificate (C_{DS}) for verification of a SO_D, the inspection system SHALL verify its digital signature, using the Country Signing CA Public Key (KPu_{CSCA}).

4. The inspection system reads relevant Data Groups from the LDS.

5. By hashing the contents and comparing the result with the corresponding hash value in the Document Security Object (S_{OD}) it ensures that the contents of the Data Group are authentic and unchanged.

The biometric information can now be used to perform the biometrics verification with the person who offers the MRTD.

R5-p1_v2_sIV_0050

Reference:

Issue:
We have been party to several conversations lately where it has become apparent that folks are struggling with potentially confusing language in the PKI technical report. The report talks about the ICAO PKD as the PRIMARY source for C_{DS} information and the SECONDARY source for CRL information. In the report, we also talk about the member states as the SECONDARY source for C_{DS} and PRIMARY for CRL. Operationally this has been confusing for folks who interpret this as always needing to talk to both sources (the PKD once it exists and the member states for two different pieces of data). Furthermore, as each member state has adopted a slightly different distribution mechanism, communicating with them regularly is operationally fragile.
Operationally, it would be simpler if we added a clarification recognizing that receiving states may choose to use the PKD as their routine source for C_{DS} and CRL information but that they should be prepared to move to the member states mechanism if there is any gap in C_{DS} or CRL information.

Conclusion:
Accepted

Clarification:
The table below summarizes the objects and sources, defined as primary and secondary in Doc 9303.

	C_{CSCA}	**Null-CRL**	**Non-Null CRL**	**C_{DS}**
PKD		S	S	P
Chip				S
Bilateral	Only	P	P	

Operationally, States are not obliged to use *both* the primary and secondary source. In the daily operation of an inspection system, it is at the inspecting authority's discretion whether to use the primary *or* the secondary source. If an inspecting authority uses the secondary source for a certificate or CRL in its daily operations, it should be prepared to support the primary source as well.

R5-p1_v2_sIV_0051

Reference:

Issue:
Throughout Doc 9303, the term “Inspection System” is used. Although parties other than border control authorities are referred to (f.i. in Volume 2, Section IV, paragraph 5.5.2), the operators of inspection systems are used, are not explicitly defined. There is a need for clarification on the term “Inspection System” and on the entities to be expected to operate those inspection systems.

Conclusion:
Accepted.

Clarification:
The “Guide to Interfacing e-MRTDs and Inspection Systems”, version 1.0, February 14 2005, uses the term ‘Inspection System’, referring to the combination of Hardware and Software, used to retrieve information from the e-MRTD. In this definition an Inspection System typically consists of Reader Hardware, Low Level (communications) Software, High level (application) Software. The Inspection System takes care of powering the chip, communicating with the chip at 14443 as well as 7816 level, ICAO specified security features, retrieving LDS data groups. This Guide does not assume certain technical implementations of such an Inspection System (e.g. which functionality is covered in which system component).
This definition does not clarify the purpose an “Inspection System” is used for. An inspection system is defined as any system used for inspecting (e)MRTDs by any public or private entity having the need to validate the (e)MRTD, and using this document for identity verification, e.g. border control authorities, airlines and other transport operators, financial institutions, among others.

R6-p1_v2_sIV_0052

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, Appendix 5.
See also Supplement issue R7-p3_v2_sIV_0007.

Issue:
Apparently some errors were introduced in the Figures in Appendix 5 when 9303 was edited and the drawings were transferred from the TR-PKI V1.1 into the sixth edition of Doc9303 part 1.
It concerns the following:

- 9303 Part - 1 Volume 2, Figure IV-5.5.
  As described in the TR-PKI V1.1: Kb should be used to decrypt Yn.
- 9303 Part - 1 Volume 2, figure IV-5-4 TDS Encryption.
  As described in the TR-PKI V1.1: TDES Encryption should be (DES)Ka – (DES-1)Kb – (DES)Ka.
- 9303 Part - 1 Volume 2, figure IV-5-2 Add and pad command header.
  The left arrow from DO’87’ to “Add and pad command header” must originate from the left hand side (left corner of ‘87’) and not between ‘01’ and X1.
- 9303 Part - 1 Volume 2, figure IV-5-2 Protected APDU.
  A separation between ‘08’and CC is missing.
- 9303 Part - 1 Volume 2, figure IV-5-3 Protected APDU.
  A separation between ‘08’and CC is missing.

Conclusion:
Accepted.

Clarification:
In reviews this was missed since the drawings had been expected to be copied 1:1. Correct drawings are incorporated into Appendix D of this Supplement.

R6-p1_v2_sIV_0053

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, 5.5.1.
Also Supplement issue R3-p3_v2_sIV_0006.

Issue:
Doc 9303 states that the Country Signing CA Certificate (C_{CSCA}) SHALL be self-signed and issued by the Country Signing CA (CSCA). As per a certain State's IT Act, the CCA (Controller of Certification Authority) is the supreme authority to publish self signed certificates. Any other CA in the country is issued the Certificate by CCA to establish the Trust Chain. How to meet the ICAO specifications without violating this IT-act?

Conclusion:
See clarification.

Clarification:
A possible solution is to create a self signed CSCA certificate. This certificate meets the ICAO specifications. This certificate is then to be countersigned by the CCA, and as such meets the State's IT-act also. This solution is known to be implemented by at least two other States.

R7-p1_v2_sIV_0054

Reference:
Doc9303, Part 1, Vol2, Section IV, paragraph 4.

Issue:
In Doc9303, Part 1, Vol2 the lists of reference documentation in Section III, paragraph 2.1 and Section IV, paragraph 4 contain references to documents, not referenced to in other parts of Volume 2. Also some documentation has been revised, as a result of which referenced dates have changed. An updated list of reference documentation is desirable.

Conclusion:
Accepted

Clarification:
In case of doubt the reader MAY use to the reference documentation listed in paragraph 1.4 of this Supplement as the reference documentation to be used in conjunction with Doc 9303. It SHOULD however be noted that these editorial addenda in no way affect, or interfere with, the specifications set out in Doc 9303 Part 1, Sixth edition.

R7-p1_v2_sIV_0055

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, 9.5.
Also Supplement issue R7-p3_v2_sIV_0008.

Issue:
Doc9303 does not specify the use of ARLs. CRLs can be used in case a CSCA needs to be revoked. Which authority should sign the CRL in such an event?

Conclusion:
See clarification

Clarification:
A valid approach for the CSCA is to issue a CRL signed with the CSCA's compromised key. The compromised key is the only key the receiver of the CRL is able to validate.
An attacker who has compromised the key is not expected to issue a rogue CRL, since he then will not be able to benefit from it anymore.

Therefore, at the moment the CRL is received the key should be regarded as being still valid. After that moment the key is compromised.

R7-p1_v2_sIV_0056

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, 8.4.
Also Supplement issue R7-p3_v2_sIV_0009.

Issue:
This Supplement recommends that for ECDSA, next to the reference to ANSI X9.62, implementers MUST also acknowledge ISO/IEC 15946-1&2 as a reference (see R3-p1_v2_sIV_0040). ISO/IEC 15946 allows for hashes > SHA-1, where ANSI X9.62 does not. However, no OID's for these combinations have been defined. The 2005 revision of X9.62 2005 defines OIDs but not all of them are sensible to use. There is a need for guidance.

Conclusion:
Accepted

Clarification:
It is RECOMMENDED to follow the guideline “TR03111_Elliptic Curve Cryptography Based on ISO 15946”. The present version of this guideline is V1.00, dated 14-02-2007. A new version has been announced. When it becomes available this will be notified in the Supplement.

R7-p1_v2_sIV_0057

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, 8.1 and 8.4.
Also Supplement issue R7-p3_v2_sIV_0010.

Issue:
Doc9303 specifies in section IV, paragraph 8.1 with respect to Active Authentication that “For signature generation in the Active Authentication mechanism, States SHALL use ISO/IEC 9796-2 Digital Signature scheme 1 (ISO/IEC 9796-2, Information Technology — Security Techniques — Digital Signature Schemes giving message recovery — Part 2: Integer factorisation based mechanisms, 2002.)”

Doc9303 specifies in section IV, paragraph 8.4 with respect to the use of ECDSA that “Those States implementing the ECDSA algorithm for signature generation or verification SHALL use X 9.62 (X9.62, “Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)”, 7 January 1999).

ISO/IEC 9796 specifies that the hash value is incorporated in the signature format. X9.62 specifies that the hash value itself must be used as input for the signature algorithm. This is confusing, use of ECDSA conforming to X9.62 would violate the requirement in paragraph 8.1.

Conclusion:
Accepted

Clarification:
For reasons of clarity and interoperability it is RECOMMENDED to use RSA for Active Authentication and comply to section IV, paragraph 8.1. In this case X9.62 is not relevant and therefore not confusing.

R8-p1_v2_sIV_0058

Reference:

Doc 9303-part 1-sixth edition: Volume 2, Section IV, 9.1 and Appendix A.1.1, A.1.2, Appendix 2, Appendix A.3.2, and Appendix A.4.1.
Also Supplement issue R8-p3_v2_sIV_0011.

Issue:
It should be noted that RFC 5280, *D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", May 2008* supersedes RFC 3280, *R. Housley, W. Polk, W. Ford, D. Solo, "X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002*.

Conclusion:
Accepted

Clarification:
References to RFC 3280 should be interpreted as references to RFC 5280. Contents wise there is no difference, except for the Certificate Extension **PrivateKeyUsagePeriod**, which is not specified in RFC 5280. **PrivateKeyUsagePeriod** is the issuing period of the private key (ref. RFC3280, section 4.2.1.4).

R8-p1_v2_sIV_0059

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, 5.5.1.
Also Supplement issue R8-p3_v2_sIV_0012.

Issue:
States are required to exchange their CSCA certificates bilaterally by diplomatic means. The first years in which States issue e-passports show that the lack of detailed specifications on mechanisms for this exchange has lead to wide interpretation and inefficient processes.
A more efficient way of CSCA Certificate exchange should be specified.

Conclusion:
Accepted

Clarification:
Such specifications are now provided by ICAO's Technical Report "CSCA countersigning and Master List issuance", version 1.0, June 2009. The approach described in this Technical Report aims to provide an electronic means of distributing and publishing issuing States' CSCA Public Keys. The modified approach is based on countersigning the CSCA certificates of issuing States by other States, and distributing the countersigned CSCA certificates via the ICAO PKD, to support but not to replace bilateral distribution of self-signed certificates.

R8-p1_v2_sIV_0060

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, 8.1 and 8.4.
Also Supplement issue R8-p3_v2_sIV_0013.

Issue:
For reasons of clarity and interoperability this Supplement recommends to use RSA for Active Authentication and not ECDSA (see issue **R7-p1_v2_sIV_0057**). An unambiguous specification for the use of ECDSA in Active Authentication should be provided.

Conclusion:
Accepted

Clarification:

See Appendix F of this Supplement for the specification of the use of ECDSA in Active Authentication.

R8-p1_v2_sIV_0061

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, 8.2.
Also Supplement issue R8-p3_v2_sIV_0014.

Issue:
RSA key lengths of 1024 bits should not be recommended anymore..

Conclusion:
Accepted

Clarification:
For newly issued eMRTDs the RECOMMENDED minimum key length for RSA is 1280 bits. Recommendations for the minimum lengths of the moduli of Document Signer Keys and Country Signing CA keys remain unchanged (2048 and 3072 bits respectively).
It should be noted that when using key lengths exceeding 1848 bits in Active Authentication, Extended Length must be supported by the Inspection System. Since the use of Extended Length is not specified in Doc 9303, systems may not support it and inspection might fail.

R8-p1_v2_sIV_0062

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV, 9.3.
Also Supplement issue R8-p3_v2_sIV_0015.

Issue:
It was decided that the storage of the Document Signer certificate in the Security Object will become MANDATORY.

Conclusion:
Accepted

Clarification:
The PKD board has endorsed specifications for the CSCA Master List (see ICAO's Technical Report "CSCA countersigning and Master List issuance", version 1.0, June 2009) as a means of CSCA certificate distribution through the PKD. Also the decision was taken to MANDATORY store the DS certificate on the chip in the Document Security Object for newly issued eMRTDs.

R11-p1_v2_sIV_0063

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV.
Also Supplement issue R11-p3_v2_sIV_0016.

Issue:
States are issuing CSCAs with a specific key usage period corresponding to the time period within which the CSCA will be used to sign Document Signers. The current practice in some States is to issue a long term CRL just before the expiry of the private key to cover the period for which the CSCA itself is valid. There is no guidance on how to issue a CRL in case of discovery of compromise on a DSC after the private key of the CSCA is no longer valid.

Conclusion:
See clarification

Clarification:
It should be noted that for signing CRLs and Document Signer Certificates always the actual (newest) CSCA Private Key MUST be used. This prevents the problem from occurring.

4 Doc 9303 - Part 2 (third edition)

Issues, related to Doc 9303-part 2-third edition are gathered in this section.

4.1 Section III - Technical specifications for Machine Readable Visas Common to all Machine Readable Travel Documents

R7-p2_v-_sIII_0001

Reference:
Doc 9303-part 2 - third edition: Section III, Appendix 1.
Also R7-p1_v1_sIV_0004 and R7-p3_v1_sIV_0002.

Issue:
It should be noted that since 2002 the term "Dependant territories citizen - GBD*" has been changed into "British Overseas Territories Citizen - GBD*".

Conclusion:
Accepted.

Clarification:
The description at the 3-lettercode GBD* has changed into "British Overseas Territories Citizen".

R7-p2_v-_sIII_0002

Reference:
Doc9303, Part 2, Section III, Annex to section III.
Also Supplement issue R7-p1_v1_sIII_0001 and R7-p3_v1_sIII_0001.

Issue:
The worldwide increase in the number of people travelling and the expected continuing growth, together with the growth in international crime, terrorism, and illegal immigration has led to increasing concerns over the security of travel documents and calls for recommendations on what may be done to help improve their resistance to attack or misuse.

Conclusion:
Accepted

Clarification:
To meet the need of increased document security, ICAO's technical advisors decided it would be desirable to publish a set of "recommended minimum security standards" as a guideline for all States issuing machine readable travel documents. This resulted in an updated Appendix 1 to Section III of Doc9303, part 1 and part 3 to replace the existing Annex to section III of part 2, third edition. States are RECOMMENDED to follow the updated Appendix 1, which has been incorporated into Appendix E of this Supplement.

R8-p2_v-_sIII_0003

Reference:
Doc 9303-part 2 - third edition: Section III, Appendix 1.
Also R8-p1_v1_sIV_0005 and R8-p3_v1_sIV_0003.

Issue:
It should be noted that in ISO 3166, where Doc 9303 refers to for three letter county codes, changes have been made.

Conclusion:
Accepted.

Clarification:
The following changes apply for the 3-lettercodes, as listed in Doc 9303-part 2-third edition: Section III, Appendix 1:

- France, Metropolitan – FXX: deleted
- Montenegro – MNE: added
- Serbia – SRB: added

Serbia and Montenegro – SCG: deleted

R10-p2_v-_sIII_0004

Reference:
Doc 9303-part 2-third edition: Section III, Appendix 1.
Also R10-p1_v1_sIV_0006 and R10-p3_v1_sIV_0004.

Issue:
It should be noted that in ISO 3166, where Doc 9303 refers to for three letter county codes, changes have been made.

Conclusion:
Accepted.

Clarification:
The following changes apply for the 3-lettercodes, as listed in Doc 9303-part 2-third edition: Section III, Appendix 1:

- Bonaire, Saint Eustatius and Saba – BES: added
- Curaçao – CUW: added
- Saint-Barthélemy – BLM: added
- Saint-Martin (French part) – MAF: added

Sint Maarten (Dutch part) – SXM: added

R11-p2_v-_sIII_0005

Reference:
Doc 9303-part 2-third edition: Section III, Appendix 2.
Also R11-p1_v1_sIV_0008 and R11-p3_v1_sIV_0005.

Issue:
A three letter code has been assigned to South Sudan.

Conclusion:
Accepted.

Clarification:
The country code for South Sudan is SSD.

R11-p2_v-_sIII_0006

Reference:
Doc 9303-part 2-third edition: Volume 1, Section IV, Appendix 3.
Also R11-p1_v-_sIV_0009 and R11-p3_v1_sIV_0006.

Issue:
A request has been received to accommodate the transliteration of Turkish characters.

Conclusion:
Accepted.

Clarification:

In the transliteration table the following transliterations apply for the characters mentioned below:
Ö can be transliterated by OE or O.
Ü can be transliterated by UE, UXX or U.
Ä can be transliterated by AE or A.
Å can be transliterated by AA or A.

4.2 Section IV - Technical specifications for format-A Machine Readable Visas

R6-p2_v-_sIV_0001

Reference:
Doc 9303-part 2-third edition: Section IV, page IV-21.

Issue:
Technical limitations associated with the introduction of ePassports mean that it is not currently feasible for ICAO to permit the use of contactless Integrated Circuits in visas. This is because of the risk of interference with the readability of the IC in the ePassport.

ICAO no longer considers the use of bar codes to be a globally interoperable means of data storage. Also the only biometric technologies now recognised by ICAO are the mandatory use of facial recognition optionally supported by fingerprint and iris. In each case the biometric is stored as an image. There is currently no globally interoperable machine readable method of storing such image(s) on a visa label.

Accordingly page IV-21 has been amended to reflect these changes. Also Annexes B, C, E and F to Section IV have been removed as they no longer form part of these specifications.

Conclusion:
Accepted.

Clarification:
Doc 9303-part 2-third edition: Section IV, page IV-21 has to be replaced by the following:

Optional expansion of machine readable data capacity

16. A State wishing to increase the data storage capacity of its MRV-A may utilize a one or two dimensional bar code. However, the use of such a technology is not globally interoperable and this edition of ICAO Doc 9303 does not make any specifications relating to the technology other than to require that the readability of the Machine Readable Zone be unimpaired by the placement of the technology within the Visual Inspection Zone.

17. The use of a contactless integrated circuit to increase data capacity of an MRV-A is **NOT CURRENTLY PERMITTED** because of the risk of interference with the readability of any eMRP into which the MRV-A may be placed, or of other eMRVs in the same passport booklet.

Document security feature verification using a MRV-A

18. Machine Assisted Security Feature Verification. See Annex D for details on machine assisted document security feature verification for a MRV-A.

Biometric Identity Confirmation Using an MRV-A

19. This Edition of ICAO Doc 9303 Part 2 does not specify methods for Biometric Identity Confirmation for use in visas. Under present limitations of interoperable data storage, it is not

possible to specify methods of globally interoperable biometric identity confirmation in MRVs. However, States should note the technical possibility of capturing biometric data at the time of issue of a visa and storing the data in a database; at the border the State may use the information on the visa or the passport to access the stored biometric database.

4.3 Section V - Technical specifications for format-B Machine Readable Visas

R6-p2_v-_sV_0001

Reference:
Doc 9303-part 2-third edition: Section V, page V-21.

Issue:
Technical limitations associated with the introduction of ePassports mean that it is not currently feasible for ICAO to permit the use of contactless Integrated Circuits in visas. This is because of the risk of interference with the readability of the IC in the ePassport.

ICAO no longer considers the use of bar codes to be a globally interoperable means of data storage. Also the only biometric technologies now recognised by ICAO are the mandatory use of facial recognition optionally supported by fingerprint and iris. In each case the biometric is stored as an image. There is currently no globally interoperable machine readable method of storing such image(s) on a visa label.

Accordingly page V-21 has been amended to reflect these changes. Also Annexes B, C, E and F to Section V have been removed as they no longer form part of these specifications.

Conclusion:
Accepted.

Clarification:
Doc 9303-part 2-third edition: Section V, page IV-21 has to be replaced by the following:

Optional expansion of machine readable data capacity

16. A State wishing to increase the data storage capacity of its MRV-B may utilize a one or two dimensional bar code. However, the use of such a technology is not globally interoperable and this edition of ICAO Doc 9303 does not make any specifications relating to the technology other than to require that the readability of the Machine Readable Zone be unimpaired by the placement of the technology within the Visual Inspection Zone.

17. The use of a contactless integrated circuit to increase data capacity of an MRV-B is **NOT CURRENTLY PERMITTED** because of the risk of interference with the readability of any eMRP into which the MRV-B may be placed, or of other eMRVs in the same passport booklet.

Document security feature verification using a MRV-B

18. Machine Assisted Security Feature Verification. See Annex D for details on machine assisted document security feature verification for a MRV-B.

Biometric Identity Confirmation Using an MRV-B

19. This Edition of ICAO Doc 9303 Part 2 does not specify methods for Biometric Identity Confirmation for use in visas. Under present limitations of interoperable data storage, it is not

possible to specify methods of globally interoperable biometric identity confirmation in MRVs. However, States should note the technical possibility of capturing biometric data at the time of issue of a visa and storing the data in a database; at the border the State may use the information on the visa or the passport to access the stored biometric database.

---

5 Doc 9303 - Part 3 (third edition)

5.1 Volume 1

Issues, related to Doc 9303-part 3-third edition, Volume 1, are gathered in this section.

5.1.1 Section III – Technical specifications for security of design, manufacture and issuance of machine readable official travel documents

R7-p3_v1_sIII_0001

Reference:
Doc9303, Part 3, Vol1, Section III, Appendix 1.
Also Supplement issue R7-p1_v1_sIII_0001 and R7-p2_v-_sIII_0002.

Issue:
The worldwide increase in the number of people travelling and the expected continuing growth, together with the growth in international crime, terrorism, and illegal immigration has led to increasing concerns over the security of travel documents and calls for recommendations on what may be done to help improve their resistance to attack or misuse.

Conclusion:
Accepted

Clarification:
To meet the need of increased document security, ICAO's technical advisors decided it would be desirable to publish a set of "recommended minimum security standards" as a guideline for all States issuing machine readable travel documents. This resulted in an updated Appendix 1 to Section III of Doc9303, part 3, third edition to replace the existing Appendix. States are RECOMMENDED to follow the updated Appendix 1, which has been incorporated into Appendix E of this Supplement.

5.1.2 Section IV - Specifications common to both sizes of MRtd

R6-p3_v1_sIV_0001

Reference:
Also R6-p1_v1_sIV_0003.

Issue:
At TAG 17, Germany presented data from several e-passport issuing States in support of a request to relax some of the face image acquisition tolerances in the image quality guidelines. This same report had been submitted to ISO/IEC SC 37 for consideration and incorporation into a Technical Corrigendum with respect to the specifications of ISO/IEC 19794-5. The TAG directed that the next Supplement acknowledge this work and note the stage of progress at the time of Supplement publication.

Conclusion:
Accepted.

Clarification:
The drafting group of SC 37 circulated a draft that was discussed at the SC 37 meetings in Berlin in late June 2007. At the time of preparation of Supplement Release 6, as affirmatively voted, the Corrigendum called for relaxing the tolerance in head roll (tilt) to ±8° and for the following relaxations of tolerances in head size and position (where A is image width, B is image height, CC is head width, DD is head height, and M_x and M_y are the x and y coordinates of M, the center of the face, as measured from the upper left corner of the image).

Section	Definition	Requirements
8.3.1	General requirement	Head entirely visible in the image
8.3.2	Horizontal Position of Face	$0.45\ A \leq M_x \leq 0.55\ A$
8.3.3	Vertical Position of Face	$0.3\ B \leq M_y \leq 0.5\ B$
8.3.3	Vertical Position of Face (Children under the age of 11)	$0.3\ B \leq M_y \leq 0.6\ B$
8.3.4	Width of Head	$0.5\ A \leq CC \leq 0.75\ A$
8.3.5	Length of Head	$0.6\ B \leq DD \leq 0.9\ B$
8.3.5	Length of Head (Children under the age of 11)	$0.5\ B \leq DD \leq 0.9\ B$

The work of the SC 37 with respect to the final specifications affected by this Corrigendum are backward compatible with the earlier provisions of 19794-5 since only the normative requirements will be relaxed; best practice requirements remain unchanged and are strongly recommended for the application in the e-passport framework. This ensures that, e.g., issuing authorities and/or photographers do not have to change their already-published photo requirements which are based on the existing best practice requirements. Also, issuing authorities will now be able to accept more of the submitted photographs without degrading facial recognition performance. In its 18th meeting in May 2008 the TAG acknowledged the adjustments made by this Technical Corrigendum to ISO/IEC 19794-5 affecting the according reference of ICAO Doc 9303 for photographs, and approved the continuation of on-going awareness or research in this area..
See also **R6-p3_v2_sII_0001**

R7-p3_v1_sIV_0002

Reference:
Doc 9303-part 3 - third edition: Volume 1, Section IV, Appendix 1.
Also R7-p1_v1_sIV_0004 and R7-p2_v-_sIII_0001.

Issue:
It should be noted that since 2002 the term “Dependant territories citizen - GBD*” has been changed into “British Overseas Territories Citizen - GBD*”.

Conclusion:
Accepted.

Clarification:
The description at the 3-lettercode GBD* has changed into “British Overseas Territories Citizen”.

R8-p3_v1_sIV_0003

Reference:
Doc 9303-part 3 - third edition: Volume 1, Section IV, Appendix 1.
Also R8-p1_v1_sIV_0005 and R8-p2_v-_sIII_0003.

Issue:
It should be noted that in ISO 3166, where Doc 9303 refers to for three letter county codes, changes have been made.

Conclusion:
Accepted.

Clarification:
The following changes apply for the 3-lettercodes, as listed in Doc 9303:

- France, Metropolitan – FXX: deleted
- Montenegro – MNE: added
- Serbia – SRB: added

Serbia and Montenegro – SCG: deleted

R10-p3_v1_sIV_0004

Reference:
Doc 9303-part 3-third edition: Volume 1, Section IV, Appendix 1.
Also R10-p1_v1_sIV_0006 and R10-p2_v-_sIII_0004.

Issue:
It should be noted that in ISO 3166, where Doc 9303 refers to for three letter county codes, changes have been made.

Conclusion:
Accepted.

Clarification:
The following changes apply for the 3-lettercodes, as listed in Doc 9303-part 3-sixth edition: Volume 1, Section IV, Appendix 1:

- Bonaire, Saint Eustatius and Saba – BES: added
- Curaçao – CUW: added
- Saint-Barthélemy – BLM: added
- Saint-Martin (French part) – MAF: added

Sint Maarten (Dutch part) – SXM: added

R11-p3_v1_sIV_0005

Reference:
Doc 9303-part 3-third edition: Volume 1, Section IV, Appendix 1.
Also R11-p1_v1_sIV_0008 and R11-p2_v-_sIII_0005.

Issue:
A three letter code has been assigned to South Sudan.

Conclusion:
Accepted.

Clarification:
The country code for South Sudan is SSD.

R11-p3_v1_sIV_0006

Reference:
Doc 9303-part 3-third edition: Volume 1, Section IV, Appendix 2.
Also R11-p1_v1_sIV_0009 and R11-p2_v-_sIII_0006.

Issue:
A request has been received to accommodate the transliteration of Turkish characters.

Conclusion:
Accepted.

Clarification:
In the transliteration table the following transliterations apply for the characters mentioned below:
Ö can be transliterated by OE or O.
Ü can be transliterated by UE, UXX or U.
Ä can be transliterated by AE or A.
Å can be transliterated by AA or A.

5.1.3 Section V - Technical specifications - Size 1 MRtds

R10-p3_v1_sV_0001

Reference:
Doc 9303-part 3-third edition: Volume 1, Section V, par 3.3.2.

Issue:
When a td1 sized Identity Card, conforming ICAO Doc 9303 part 3, will be equipped with an integrated circuit (IC) with contacts it is not clear what positions for this IC are allowed according to ICAO Doc 9303 part 3.
In that respect the following two questions are of interest:

1. Does ICAO Doc 9303 allow to place the contacts of the contact IC at the rear side of the card?
2. In case it is allowed to place the contacts of the contact IC at the rear side, does this imply that the holder's portrait must be located at the left side of the card (as prescribed in clause 3.3.1 of Section V of Doc 9303, part 3, volume 1) or must the holder's portrait be located at the right side of the card (as indicated in clause 3.3.2 of Section V of Doc 9303 , part 3, volume 1)?

Conclusion:
See clarification.

Clarification:

1. ICAO Doc 9303 part 3 does allow placement of the contacts at either the side where the photograph and other personal data are located ('front side') as well as at the other side where the MRZ resides ('rear side').
   The preferred position is at the rear side, where the MRZ is located, since this leaves more space available for printed data and features at the front side. The position of the IC contacts needs to be in accordance with ISO/IEC 7816-2 and must not interfere with the MRZ. As a consequence they must be located at the left side.
2. When the contacts of the IC are positioned at the rear side of the card, as a consequence they do not interfere with the photograph. Therefore the photograph should be located according to paragraph 3.3.1 in Section V of Doc 9303, part 3, volume 1, being along the left edge of the front side.

5.2 Volume 2

Issues, related to Doc-9303-part 3-third edition, Volume 2, are gathered in this section.

5.2.1 Section II - The deployment of biometric identification and the electronic storage of data in Machine Readable Official Travel Documents

R6-p3_v2_sII_0001

Reference:
Also R6-p1_v2_sII_0002.

Issue:
At TAG 17, Germany presented data from several e-passport issuing States in support of a request to relax some of the face image acquisition tolerances in the image quality guidelines. This same report had been submitted to ISO/IEC SC 37 for consideration and incorporation into a Technical Corrigendum with respect to the specifications of ISO/IEC 19794-5. The TAG directed that the next Supplement acknowledge this work and note the stage of progress at the time of Supplement publication.

Conclusion:
Accepted.

Clarification:
The drafting group of SC 37 circulated a draft that was discussed at the SC 37 meetings in Berlin in late June 2007. At the time of preparation of Supplement Release 6, as affirmatively voted, the Corrigendum called for relaxing the tolerance in head roll (tilt) to ±8° and for the following relaxations of tolerances in head size and position (where A is image width, B is image height, CC is head width, DD is head height, and M_x and M_y are the x and y coordinates of M, the center of the face, as measured from the upper left corner of the image).

Section	Definition	Requirements
8.3.1	General requirement	Head entirely visible in the image
8.3.2	Horizontal Position of Face	$0.45\ A \leq M_x \leq 0.55\ A$
8.3.3	Vertical Position of Face	$0.3\ B \leq M_y \leq 0.5\ B$
8.3.3	Vertical Position of Face (Children under the age of 11)	$0.3\ B \leq M_y \leq 0.6\ B$
8.3.4	Width of Head	$0.5\ A \leq CC \leq 0.75\ A$
8.3.5	Length of Head	$0.6\ B \leq DD \leq 0.9\ B$
8.3.5	Length of Head (Children under the age of 11)	$0.5\ B \leq DD \leq 0.9\ B$

The work of the SC 37 with respect to the final specifications affected by this Corrigendum are backward compatible with the earlier provisions of 19794-5 since only the normative requirements will be relaxed; best practice requirements remain unchanged and are strongly recommended for the application in the e-passport framework. This ensures that, e.g., issuing authorities and/or photographers do not have to change their already-published photo requirements which are based on the existing best practice requirements. Also, issuing authorities will now be able to accept more of

the submitted photographs without degrading facial recognition performance. In its 18th meeting in May 2008 the TAG acknowledged the adjustments made by this Technical Corrigendum to ISO/IEC 19794-5 affecting the according reference of ICAO Doc 9303 for photographs, and approved the continuation of on-going awareness or research in this area..
See also **R6-p3_v1_sIV_0001**

5.2.2 Section III - A Logical Data Structure for contactless integrated circuit data storage technology

R6-p3_v2_sIII_0001

Reference:
Also Supplement issue R1-p1_v2_sIII_0028.

Issue:
Define how a reader can recognize that a document is using Basic Access Control. Proposal that
EF.COM is free to read
EF.COM has indicator that BAC is in use

Conclusion:
See clarification.

Clarification:
The *Basic Access Control* mechanism is optional. When presenting a MRTD with an ICC to a reader, this reader doesn't know in advance if the mechanism must be performed. How can the reader solve this problem?

A solution can be a simple trial-and-error mechanism. First try to get direct access to the ICC and if this fails, perform the *Basic Access Control Mechanism*.

Step 1:
Select the LDS DF by AID. If this fails, the MRTD isn't equipped with an ICAO LDS compliant ICC. Otherwise the correct response will be '90 00'.
(send: '00 A4 04 0C 07 A0 00 00 02 47 10 01', response: '90 00')

Step 2.
Try to select the EF.COM by file ID. Depending on the answer of the ICC, Basic Access Control is, or is not, implemented.

Option 1:
No Basic Access Control required.
(send: '00 A4 02 0C 02 01 1E', response: '90 00').
The file is selected and the data can be read.

Option 2:
Basic Access Control required.
(send: '00 A4 02 0C 02 01 1E', response: '69 82').
The file is NOT selected and the ISO-7816-4 error-code means "Security status not satisfied". The Basic Access Control Mechanism must be performed after which the file should be selected again using Secure Messaging.

Option 3:
An error occurs.
(send: '00 A4 02 0C 02 01 1E', response: error-code other than '69 82').
The file is NOT selected. The MRTD isn't equipped with an ICAO LDS compliant ICC.

The READ BINARY command may also be used as a trigger to indicate if the document is protected using Basic Access Control. When READ BINARY is used

Case a): using separate SELECT command and then READ BINARY

1) Select EF.COM using SELECT command: send '00 A4 02 0C 02 01 1E'.

2) If response is '90 00'

- Try to read the content using READ BINARY command:
  send '00 B0 00 00 00'
  - If '6982' error code is returned, the Issuer Application is protected using BAC. Then The Basic Access Control Mechanism must be performed after which the file should be read again using Secure Messaging.
  - If the content (first 256 bytes) + '90 00' SW bytes are returned, the Issuer Application is NOT protected using BAC.
  - Otherwise some error has occurred, go to the error handling.

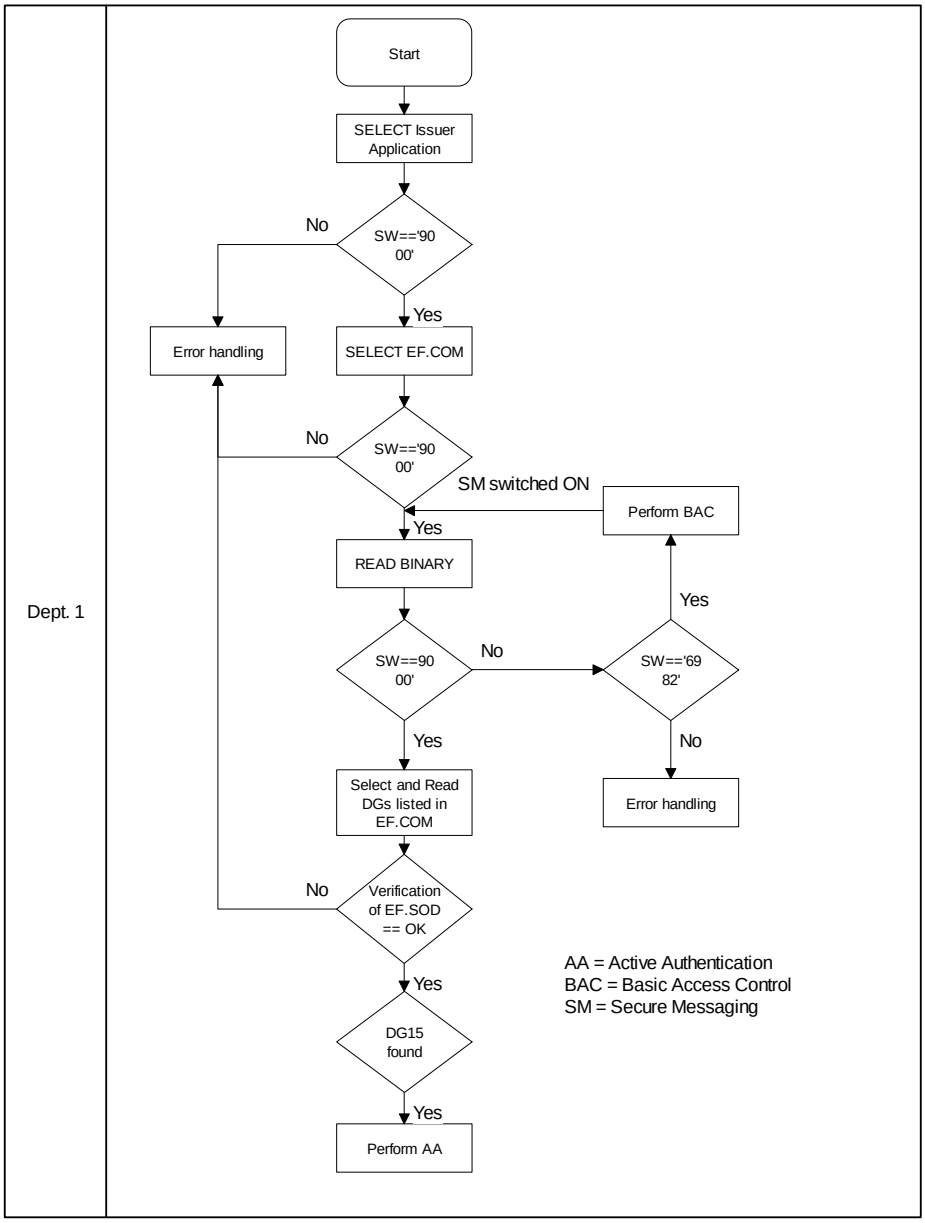
3) Otherwise the Issuer Application isn't ICAO LDS compliant.

Case b): using SFID combined to READ BINARY

1) Try to read the content of EF:COM using SFID combined to READ BINARY command:
send '00 B0 9E 00 00'

- If '6982' error code is returned, then the Issuer Application is protected using BAC. Then The Basic Access Control Mechanism must be performed after which the file should be read again using Secure Messaging.
- If the content (first 256 bytes) + '90 00' SW bytes are returned, the Issuer Application is NOT protected using BAC.
- Otherwise the Issuer Application isn't ICAO LDS compliant.

Below the case a) is presented as a process flow diagram:



R6-p3_v2_sIII_0002

Reference:
Also Supplement issue R2-p1_v2_sIII_0032.

Issue:
Odd INS data field structure
Three different implementations were found at read binary of Odd_INS Byte when reading data greater than 32k byte
1) The Le byte contains V only
2) The Le byte contains TL and V
3) The Le byte contains extended TL and V
Need to clarify recommended implementation

Conclusion:
Accepted.

Clarification:

Option 3: ‘The Le byte contains extended TL and V’ should be implemented, being the most common practice.

R6-p3_v2_sIII_0003

Reference:
Also Supplement issue R2-p1_v2_sIII_0035.

Issue:
Le at Mutual authentication.
Mutual Authentication can take Le = 28 (hex) or 00. In the PKI main section, Le is not specified. However Le = 28 (hex) is specified as an example in the Appendix. But in 7816-4, Le can be 00 also, which means that the response can be up to 256 bytes and the card will decide. From our Singapore InterFest experience, we know some card vendors expect Le = 28 and some expect Le = 00 (or will only respond correctly if Le = 00).

Conclusion:
See clarification.

Clarification:
The ISO/IEC 7816-4:2005 (as well as the earlier edition) specifies that Le encodes Ne, which in turn "denotes the maximum number of bytes expected in the response data field." In addition, it specifies for short Le fields that "If the byte (Le) is set to '00', then Ne is 256."
Therefore, the card cannot return more than Ne bytes in the response data field, but it can return less (or no) bytes. The specification of the authentication command does not define specific values for the Le, or any rules for rejecting specific Le values. eMRTDs should therefore accept both '00' and '28' in the Le field if they return always '28' bytes of response data (actually '00' or any value between '28' and 'FF', but that is not relevant here).

R6-p3_v2_sIII_0004

Reference:
Also Supplement issue R2-p1_v2_sIII_0036.

Issue:
APDU at Le=00.
In the case of Le = 00 (in general), 7816-3 allows both 5-byte APDU (i.e. Le is sent) or 4-byte APDU (i.e. Le is not sent). Usually in 7816-3, for T=0, 5-byte APDU is sent, while for T=1, 4-byte APDU is sent. But T=0 and T=1 are both for contact interface and so in the case of contactless, there is no proper guideline. We have found that some cards expect 4-byte and some 5-byte APDU when Le = 00.

Conclusion:
See clarification.

Clarification:
The ISO/IEC 7816-4:2005 as well as the ISO/IEC FCD 7816-3 specify the generic APDU structure, and ISO/IEC 7816-3 and ISO/IEC FCD 7816-3 specify how the APDUs are mapped on the TPDUs of the protocols T=0 and T=1.
The case 1 APDU, which is the subject of this issue, is specified as a 4-byte string.
For the T=0 it is specified that the C-TPDU always uses a byte P3, which is set to '00' in case 1. This is required for the byte-oriented transfer method, as the card cannot know whether it should expect 4- or 5-byte command header.
For the T=1 it is specified that the APDUs are mapped directly onto the TPDUs, as there is no requirement to do otherwise in a block-oriented transfer method.
The ISO/IEC 14443-4 does not specify how the APDUs are mapped on the INF fields, which is clearly a slight problem. However, as there is no rule or other requirement to use any conversion in

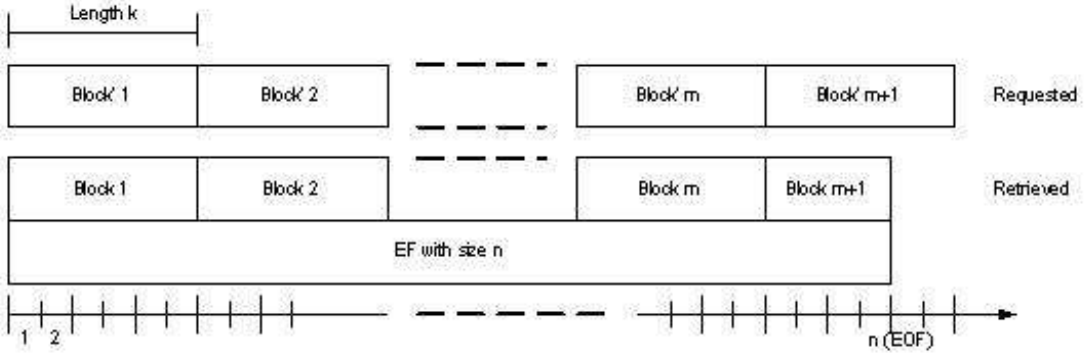
the mapping from APDUs to TPDUs due to the used transfer method, the mapping intuitively equals that of T=1.
Therefore, if the command comes with five bytes, the card shall assume the fifth byte to be Le, and the commands is thereby given as a case 2 command.
In general it is not a problem to allow data to be returned in the response data field even though it is not available, but for the card it may be justified to reject commands which do not use the correct case (1, 2, 3 or 4). For maximal compatibility, the commands should always be sent using the correct case. eMRTDs which require usage of incorrect case (as indicated in the issue text) shall be rejected.

R6-p3_v2_sIII_0005

Reference:
Also Supplement issue R2-p1_v2_sIII_0039.

Issue:
The main use case of an inspection system is to read data groups from the e-passport with or without BAC. The Sixth Edition Part 1 ICAO Doc 9303 does only specify the general way how to retrieve a data group. It is defined as a sequence of READ BINARY COMMANDS with Le = 00. This leaves several options which have an influence on the e-Passport APDU command specifications in terms of return codes. These options are as follows:

1) The inspection system reads blocks of k bytes – where k is 256 bytes or less – increasing the offset of the READ BINARY command appropriately.

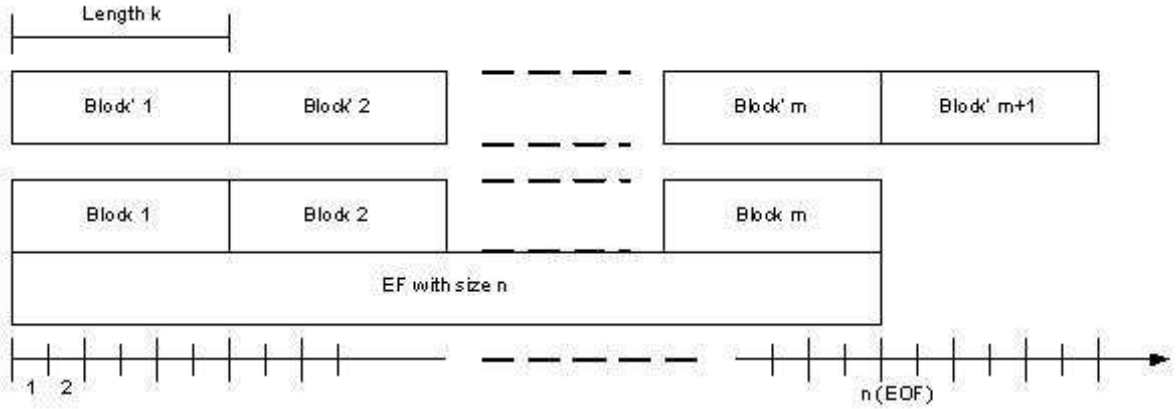


Since the length of the file is unknown in advance (the e-passport does not provide file control parameters to the inspection system), the inspection system must read until end of file (EOF). Reading the last block it may happen that the e-Passport is asked to retrieve data beyond end of file, e.g. Le = '00' for every READ BINARY. In this case it has to be clearly defined what the passport returns. The following return data is valid with respect to ISO 7816-4.

a) Block m+1 plus status word '90 00'
b) Block m+1 plus status word '62 82'
c) Checking error '6C XX', where 'XX' is the length of Block m+1

In all three cases, the BAC session keys of the e-Passport MUST NOT be deleted. All status words MUST be returned with SM data if BAC is applied.

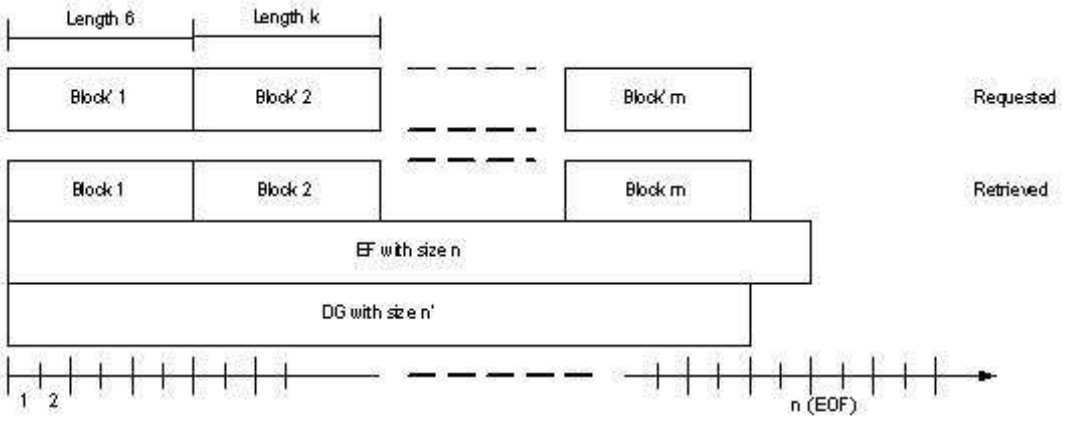
2) The inspection system reads blocks of k bytes – where k is 256 bytes or less – increasing the offset of the READ BINARY command appropriately.



Since the length of the file is unknown in advance (see option 1), the inspection system reads until the end of the file (EOF). Reading the last block it may happen that the offset of the last block (block' m+1) is already EOF. It means that n is a multiple of k. In this case it has to be clearly defined what the passport returns. The status word '6B 00' or at least a checking error is valid with respect to ISO 7816-4. Data MUST NOT be returned.

Once again, the BAC session keys of the e-Passport MUST NOT be deleted. All status words MUST be returned with SM data if BAC is applied.

3) The inspection system reads the first 5 or 6 bytes and tries to decode the length of the ASN-1 structure stored in the elementary file. In this case the inspection system knows in advance the length of the data group.



The disadvantage of this approach is that it mixes up two different layers of information. Moreover, it may be a little bit slower than the first two options, e.g. reading EF.COM may involve two consecutive READ BINARY commands instead of one command. Using this option excludes the implementation of the first two options unless the return codes defined in 1) and 2) are specified.

Conclusion:
See clarification

Clarification:
The following facts have to be considered:

1. ISO/IEC 7816-4 allows several different status words as response to some of the described read scenarios.
2. There are already several different e-Passport implementations out in the field.
3. The performance of reading the data groups is largely influenced by the amount of data to be transferred.

For the current generation of e-Passports being compliant with LDS version 1.7, specifying new requirements should be avoided (due to 1. and 2.), and elementary files should not be read completely but only until the end of the application template (due to 3.).

Therefore, option 3 (the inspection system reading the first 6 bytes to extract the exact length of a data group) should be used. Then there is no urgent need to define EOF status bytes.

For the next generation of e-Passports, e.g. according to the planned LDS version 2.0, this use case should be specified as stated in options 1 and 2 of the Request for Clarification.

R6-p3_v2_sIII_0006

Reference:
Doc 9303-part 3-third edition: Volume 2, Section III, Appendix 1, A1.21.
Also Supplement issue R4-p1_v2_sIII_0040.

Issue:
Clarification if command READ BINARY with odd INS byte is a mandatory command on e-Passports even if there are no EFs greater than 32k.

Conclusion:
See clarification.

Clarification:
Doc 9303-part 3-third edition: Volume 2, Section III, Appendix 1, A1.21 states:
The maximum size of an EF is normally 32,767 bytes, but some ICs support larger files. A different READ BINARY parameter option and command format is required to access the data area when the offset is greater than 32,767. This format of command should be used after the length of the template has been determined and the need to access the data in the extended data area has been determined. For example, if the data area contains multiple biometric data objects, it may not be necessary to read the entire data area. **Once the offset for the data area is greater than 32,767, this command format shall be used.** The offset is placed in the command field rather than in the parameters P1 and P2.

This leads to the conclusion that the odd INS byte is not to be used if the size of an EF is 32,767 bytes or less.

R6-p3_v2_sIII_0007

Reference:
Also Supplement issue R5-p1_v2_sIII_0046.

Issue:
ISO/IEC 7816-4:2005 specifies that length of value field in Le Data Object is one or two bytes. (See Table 27 or 28 in ISO/IEC 7816-4:2005). On the other hand ISO/IEC 7816-4:2005 Annex B shows Examples of secure messaging. In this annex, value filed of Le Data Object is equal to original Le field. In Case 2E of Command APDU, length of Le field is 3 bytes. From experiences in Japanese smart card project using extended Le field, a smart card reader send 3 bytes value field of Le Data Object in secure messaging and a smart card can interpret it.

Proposal: To notify length of value field in Le Data Object is one or two bytes.

Conclusion:
Accepted.

Clarification:

The specification should be followed, meaning that the length of value field in Le Data Object is one or two bytes.

R6-p3_v2_sIII_0008

Reference:
Doc 9303-part 3-third edition: Volume 2, Section III, Appendix 1, A1.13.
Also Supplement issue R6-p1_v2_sIII_0048.

Issue:
Concerning the encoding of several TAGs in the LDS there is a mismatch between the LDS specifications and ISO/IEC 8825-1 (BER/DER encoding rules).

ISO/IEC 8825-1:
For tags with a number ranging from zero to 30 (inclusive), the identifier octets shall comprise a single octet encoded as follows:
a) bits 8 and 7 shall be encoded to represent the class of the tag as specified in Table 1;
b) bit 6 shall be a zero or a one according to the rules of 8.1.2.5;
c) bits 5 to 1 shall encode the number of the tag as a binary integer with bit 5 as the most significant bit.

This means that (for instance) the TAG for the version number of the LDS specification should be defined as TAG 41h:
41h = 01 0 00001b
where 01 means Application class (bits 8 and 7);
where 0 means that it is a primitive (bit 6);
where 00001 is the encoding of TAG NUMBER 1 (bits 5-1).

Doc.9303, part 3, third edition, Volume 2, Section III:
The TAG for the version number of the LDS specification is defined as TAG 5F01h.
5F01h = 01 0 11111 0 0000001b
where 01 means Application class;
where 0 means that it is a primitive (not constructed);
where 11111 means that the tag number is encoded in the next bytes;
where 0 means that it is the last byte encoding the TAG number;
where 0000001 is the encoding of TAG NUMBER 1.

This counts for all TAGs from zero to 30 (inclusive):
5F01, 5F08, 5F09, 5F0A, 5F0B, 5F0C, 5F0E, 5F0F, 5F10, 5F11, 5F12, 5F13, 5F14, 5F15, 5F16, 5F17, 5F18, 5F19, 5F1A, 5F1B, 5F1C, 5F1D, 5F1E.

Conclusion:
Noted

Clarification:
Implementers should be aware of this mismatch and follow the specifications as set out in Doc9303.
One should however note that:

- MRTD implementations cannot be created using a generator based on ASN.1;
- ASN.1/BER parsers may return an error instead of correctly parsing EF.COM;
- The hash over EF.COM cannot be re-created by decoding the EF.COM structure and encoding it again afterwards.

An analysis if this mismatch should be eliminated will be a workl item for TR-LDS V2.

R6-p3_v2_sIII_0009

Reference:

Doc9303, Part 3 - third edition, Vol2, Section III, 10.4.1, 10.6.1, 10.7.1.
Also Supplement issue R6-p1_v2_sIII_0052.

Issue:
It seems that JPEG2000 encoding and decoding software do not have a compatibility by combination. Actually, if `the JPEG2000 format is wrong within DG2 most of the decoding software cannot handle it. In a discovered case, the reason of the problem was a missing EOC(End of code stream) or data length inconsistency of its header. These encoding errors will produce incompatibility and it is difficult to find these kind of errors if the issuer is using same vendor's encoding/decoding software when checking at issuance.

Conclusion:
Accepted

Clarification:
To prevent these kind of problems it is suggested to perform a one-time check of the JPEG2000 image encoded data using reference software which has been specified at ISO/IEC 15444-5:2003/Amd 12003 Reference software for the JPEG2000 file format.
This reference software is specified at the JPEG committee home page as a public domain.
http://www.jpeg.org/jpeg2000/j2kpart5.html

- JasPer (C) version 1.700.2 or later
- JJ2000 (Java) version 5.1 or later

R6-p3_v2_sIII_0010

Reference:
Doc9303, Part 3 - third edition, Vol2, Section III, 10.9, A1.11.9.,
Also Supplement issue R6-p1_v2_sIII_0041.

Issue:
In Doc9303, Part 3 - third edition, Data Group 14 is reserved for Security options for secondary biometrics, without its contents being specified.
DG14 should be specified in such way, that it can be used for various security options for DG3 (fingers) and DG4 (irises).

Conclusion:
Accepted

Clarification:
The following generic ASN.1 data structure **`SecurityInfos`** has been defined, allowing for various implementations of Security options for secondary biometrics. For interoperability reasons, it is RECOMMENDED that this data structure be provided by the MRTD chip in DG14 to indicate supported security protocols. The data structure is specified as follows:

```
SecurityInfos    ::=  SET of SecurityInfo

SecurityInfo     ::=  SEQUENCE {
     protocol         OBJECT IDENTIFIER,
     requiredData     ANY DEFINED BY protocol,
     optionalData     ANY DEFINED BY protocol OPTIONAL
}
```

The elements contained in a **`SecurityInfo`** data structure have the following meaning:
• The object identifier **`protocol`** identifies the supported protocol.
• The open type **`requiredData`** contains protocol specific mandatory data.
• The open type **`optionalData`** contains protocol specific optional data.

R7-p3_v2_sIII_0011

Reference:
Doc9303, Part 3-third edition, Vol2, Section III, 12.1.1 and Appendix 1, A1.11.3.
Also Supplement issue R7-p1_v2_sIII_0057.

Issue:
Doc9303 specifies the encoding of secondary biometrics in DG3 and DG4. The table in Vol2, Section III, 12.1.1 specifies that the number of fingers in DG3 and irisses in DG4 can be '1..9'. Are the values '0' and '10' excluded? There is a need for clarification on the encoding of 0, 1, and more than 1 instances of the biometric features in DG3 and DG4.

Conclusion:
Accepted

Clarification:
With respect to the encoding of DG3 and DG4 a guideline has been issued: WG3TF5_N0045 "A technical guideline for a compliant and interoperable coding of Data Group 3", version 1.3, 17-09-2007. For an interoperable coding of DG3 and DG4 this guideline MUST be followed.
The following clarifications from the guideline have been specifically addressed by the NTWG:

Number of instances.
The number of instances in DG3 and DG4, specified in Doc9303, Part 1, Vol2, Section III, 12.1.1 is to be corrected. The correct specification is '0..n'.

Encoding of zero instances.
States, not issuing eMRTDs with fingerprints or irises SHOULD NOT store DG3 at all.
For interoperability reasons States supporting fingerprints and/or irises in their eMRTDs MUST store an empty Biometric Information Group Template in cases where no fingerprints or irises are available. The template counter denotes a value of '00' in this case.
A Data Group 3 or 4 of this structure has the drawback that it will result in a static DG3 or DG4 hash in the SO_D for all eMRTDs where the biometric features are not present.
This allows distinguishing whether or not an EAC-protected passport contains fingerprints and/or irises just by performing BAC and thus, it makes those passports without fingerprints an interesting target for e.g. imposters.
To overcome this problem it is RECOMMENDED to add tag '53' with issuer defined content (e.g. a random number).

63	***Var***	LDS element			
	7F 61	***03***	Biometric Information Group Template		
		02	01	00	Defines that there are no Biometric Information Templates stored in this data group.
	53	*Var*	issuer defined content (e.g. a random number).		

Encoding of one instance.
In cases where only one fingerprint or iris is available, from a technical point of view no Biometric Information Group Template is required. However for the sake of consistency and to achieve interoperability, the single instance MUST be encoded in the following way (example for DG3 – fingerprint).

63	*aa*	LDS element where *aa* is the total length of the entire LDS data content

	7F 61	*bb*	Biometric Information Group Template, where *bb* is the total length of the entire Group Template content.				
		02	01	01	Defines the total number of fingerprints stored as Biometric Information Templates that follow.		
		7F 60	*cc*	First biometric information template where *cc* is the total length of the entire BIT			
			‘A1’	*dd*	Biometric Header Template, where *dd* is the total length of the BHT		
				81	01	08	Biometric type “Fingerprint”
				82	01	0A	Biometric subtype “left pointer finger”
				87	02	01 01	Format Owner JTC 1 SC 37
				88	02	00 07	Format Type ISO/IEC 19794-4
				Note that the BHT may contain additional optional elements. Of course, this fingerprint can either be a left or right finger depending on the available image.			
			5F 2E	*ee*	Biometric Data Block where *ee* is total length of the encoded ISO 19794-4 structure. The Biometric Data Block MUST contain exactly one fingerprint image.		

Encoding of more than one instance.

There are two possible ways to store more than one instance. They can be either stored within multiple Biometric Information Templates or inside a single Biometric Data Block using the ISO/IEC 19794 format.

While both ways are possible from the technical point of view, for an interoperable solution each feature MUST be stored in an individual Biometric Information Template. The feature position MUST be specified within the CBEFF biometric subtype if this information is available. The following table contains a worked example for the CBEFF encoding of an interoperable DG 3 element with two fingerprint images.

63	*aa*	LDS element where *aa* is the total length of the entire LDS data content					
	7F 61	*bb*	Biometric Information Group Template, where *bb* is the total length of the entire Group Template content.				
		02	01	02	Defines the total number of fingerprints stored as Biometric Information Templates that follow.		
		7F 60	*cc*	First biometric information template where *cc* is the total length of the entire BIT			
			‘A1’	*dd*	Biometric Header Template, where *dd* is the total length of the BHT		
				81	01	08	Biometric type “Fingerprint”
				82	01	0A	Biometric subtype “left pointer finger”
				87	02	01 01	Format Owner JTC 1 SC 37
				88	02	00 07	Format Type ISO/IEC 19794-4
				Note that the BHT may contain additional optional elements. It is also possible that the order of fingerprints (left/right) is different.			
			5F 2E	*ee*	Biometric Data Block where *ee* is total length of the encoded ISO 19794-4 structure. The Biometric Data Block MUST contain exactly one fingerprint image.		

		7F 60	*ff*	Second biometric information template where *ff* is the total length of the entire BIT			
			‘A1’	*gg*	Biometric Header Template, where *gg* is the total length of the BHT		
				81	01	08	Biometric type “Fingerprint”
				82	01	09	Biometric subtype “right pointer finger”
				87	02	01 01	Format Owner JTC 1 SC 37
				88	02	00 07	Format Type ISO/IEC 19794-4
				Note that the BHT may contain additional optional elements. It is also possible that the order of fingerprints (left/right) is different.			
			5F 2E	*hh*	Biometric Data Block where *hh* is total length of the encoded ISO 19794-4 structure. The Biometric Data Block MUST contain exactly one fingerprint image.		

R7-p3_v2_sIII_0012

Reference:
Doc9303, Part 3-third edition, Vol2, Section III, Appendix 1, A1.11.2.

Issue:
The examples of the DG1 encoding for both the td1 as well as the td2 sized MRtd contain errors in the length byte.

Conclusion:
Accepted

Clarification:
The example for the td1 sized MRtd states that DG1 will be ‘61’ ‘**5B**’ ‘5F1F’ ‘5A’ <et cetera>. This must be ‘61’ ‘**5D**’ ‘5F1F’ ‘5A’ <et cetera>.
The example for the td2 sized MRtd states that DG1 will be ‘61’ ‘**5B**’ ‘5F1F’ ‘48’ <et cetera>. This must be ‘61’ ‘**4B**’ ‘5F1F’ ‘48’ <et cetera>.

R7-p3_v2_sIII_0013

Reference:
Doc9303, Part 3-third edition, Vol2, Section III, Appendix 1, A1.11.6 and A1.11.7.
Also Supplement issue R7-p1_v2_sIII_0058.

Issue:
According to Doc9303, Part 3, Vol2, Section III, 12.1.2 and 12.1.3 the dates in DG11 and DG12 must be encoded in 8 numeric characters. But the tables in Appendix A1.11.6 and A1.11.7 mention 4 Byte BCD encoding. These inconsistencies seem to be errors in the tables.

Conclusion:
Accepted

Clarification:
All dates are encoded in numeric characters. In the tables in A1.11.6 and A1.11.7 the addition “(BCD encoding)” must be discarded and the corresponding length fields must be corrected to ‘08’.
Since the LDS specifications have not been unambiguous with respect to date formats, it is RECOMMENDED that Inspection Systems support both 8 bytes ASCII and BCD.

R7-p3_v2_sIII_0014

Reference:
Doc9303, Part 3, Vol2, Section III, Appendix 1, A.11.7.
Also Supplement issue R7-p1_v2_sIII_0059.

Issue:
The description of encoding DG12 is not consistent with the encoding of DG11, although one should expect it to be.
The table is not consistent in using the terms **people** and **person**.
The example should be corrected.

Conclusion:
Accepted

Clarification:
In the table the tags ‘A0’, ‘02’ and ‘5F1A’ belong to each other. To reflect this, their value descriptions must be as follows:

‘A0’	X	Content-specific constructed data object of other **persons**
‘02’	01	Number of other **persons**
‘5F1A’	X	Name of other person formatted per Doc 9303 rules. **The data object repeats as many times as specified in the ‘02’ element.**

The example of encoding DG12 must be as follows:
‘**6C**’ ‘45’
‘**5C**’ ‘06’ ‘**5F19**’ ‘**5F26**’ ‘**5F1A**’
‘**5F19**’ ‘18’ UNITED STATES OF AMERICA
‘**5F26**’ ‘08’ 20020531
‘**0A**’ ‘15’
‘**02**’ ‘01’ ‘01’
‘**5F1A**’ ‘0F’ SMITH<<BRENDA<P

R11-p3_v2_sIII_0015

Reference:
Doc9303, Part 3, Vol2, Section III, paragraph 12.1.2.
Also Supplement issue R11-p1_v2_sIII_0061

Issue:
According to ICAO 9303 Part 3 Vol 2 §12.1.2, the date of birth stored in the DG11 shall be full (complete) and encoded as CCYYMMDD with Numeric characters ([0…9]). It is not defined how a unknown date of birth shall be encoded here. Specifying the data element to be numeric doesn’t allow the solution as specified for the MRZ (as well as DG1), using the special character ‘<’ on the unknown positions (see Doc9303 Part 3 Volume 1 Section IV paragraph 14.2.2).

Conclusion:
Accepted, see clarification.

Clarification:
In case, the month (MM) or the day (DD) are unknown, the interoperable way to indicate this in DG11 is to set the respective characters to ‘00’. In case, the century and the year (CCYY) are unknown, the interoperable way to indicate this in DG11 is to set the respective characters to ‘0000’. Issuer-assigned dates must always be used consistently.

5.2.3 Section IV - PKI for machine readable travel documents offering ICC read-only access

R6-p3_v2_sIV_0001

Reference:
Doc 9303-part 3-third edition: Volume 2, Section IV, 9.5.
Also Supplement issue R1-p1_v2_sIV_0021.

Issue:
There is no description about the usage of ARL (Authority Revocation List). If the usage of ARL is included in ICAO PKI scheme, detailed operation relating bilateral and PKD-based exchange needs to be specified.

Conclusion:
Rejected.

Clarification:
For Authority Revocation an ARL can be used, but this is not necessary. The existing CRL can be used for Authority revocation.

R6-p3_v2_sIV_0002

Reference:
Doc 9303-part 3-third edition: Volume 2, Section IV, Appendix 4, A4.2.
Also Supplement issue R1-p1_v2_sIV_0026.

Issue:
Active Authentication.
Does the ICC use the RND.IFD which has been provided in the BAC process or it is a new value? If this is a new value we recommend a special note like RND**2**.IFD.

Conclusion:
See clarification.

Clarification:
It is not specified that the ICC should use the RND.IFD that was provided in the BAC process, neither that it should be a new value.

R6-p3_v2_sIV_0003

Reference:
Doc 9303-part 3-third edition: Volume 2, Section IV, Appendix 4, A4.2.
Also Supplement issue R1-p1_v2_sIV_0027.

Issue:
The Active Authentication uses the Internal Authentication command, Does this command should be send to the ICC with Secure Messaging?

Conclusion:
See clarification.

Clarification:
If Basic Access Control is applied, yes.

R6-p3_v2_sIV_0004

Reference:
Doc 9303-part 3-third edition: Volume 2, Section IV, Appendix 4, A4.2.
Also Supplement issue R1-p1_v2_sIV_0029.

Issue:

Active Authentication.
Does the signature response is with Secure Messaging? i.e. encrypting the Σ with KS_ENC and concatenation of the MAC with KS_MAC and adding the SW (90,00) encapsulate?

Conclusion:
See clarification.

Clarification:
If Basic Access Control is applied, yes.

R6-p3_v2_sIV_0005

Reference:
Doc 9303-part 3-third edition: Volume 2, Appendix 5, A5.3.2.
Also Supplement issue R3-p1_v2_sIV_0042.

Issue:
During some experiments regarding the Secure Messaging, the following question arose:
„How does the ICC react if it is not able to respond as much data as requested by the Le data object (DO '97') in the command APDU?“
This could happen in the case of READ BINARY with e.g. a zero or empty Le data object (DO '97') requesting the maximum, i.e., 256 plain data bytes (see chapter 6.4 of ISO/IEC 7816-4). Due to the protection of the response APDU with secure messaging its length would exceed 256 Bytes, which is not supported by some ICC operating systems.
In the experiments different behaviors, like responds with several different errors or responds with several different lengths, could be observed.

Therefore we propose to clarify this situation by adapting *Doc 9303-part 1-sixth edition: Volume 2, Appendix 5, A5.3.2* as follows:

“SM specific Status Bytes

When the ICC recognizes an SM error while interpreting a command, then the status bytes must be returned without SM. In ISO/IEC 7816-4 the following status bytes are defined to indicate SM errors:
• ´6987´: Expected SM data objects missing
• ´6988´: SM data objects incorrect
If due to APDU size limitations of the ICC, it is not able to respond as much data as requested by the command APDU, the protected response APDU shall contain only as much plain data bytes as possible and indicate this with the warning:
• ´6287´: less data responded than requested.

This could happen for ICCs not supporting response APDUs exceeding a length of 256 Bytes which could occur due to the protection with secure messaging.
In the case of a warning the secure session is not affected and the following READ BINARY needs to increase the offset for reading corresponding to the received response.

Note: Further SM status bytes can occur in application specific contexts. When the ICC returns status bytes without SM DOs or with an erroneous SM DO the ICC deletes the session keys. As a consequence the secure session is aborted.”

Conclusion:
Rejected.

Clarification:
This proposal uses a new warning which is not standardized in ISO/IEC 7816.

As the correct response of an ICC in such a situation is currently under discussion in SC17 WG4 no requirements for the PICC can be specified. The inspection system SHOULD avoid such a situation by requesting only an amount of plain data bytes where the secured response for this amount of plain data does not exceed 256 bytes.

R6-p3_v2_sIV_0006

Reference:
Doc 9303-part 3-third edition: Volume 2, Section IV, 5.5.1.
Also Supplement issue R6-p1_v2_sIV_0053.

Issue:
Doc 9303 states that the Country Signing CA Certificate (C_{CSCA}) SHALL be self-signed and issued by the Country Signing CA (CSCA). As per a certain State's IT Act, the CCA (Controller of Certification Authority) is the supreme authority to publish self signed certificates. Any other CA in the country is issued the Certificate by CCA to establish the Trust Chain. How to meet the ICAO specifications without violating this IT-act?

Conclusion:
See clarification.

Clarification:
A possible solution is to create a self signed CSCA certificate. This certificate meets the ICAO specifications. This certificate is then to be countersigned by the CCA, and as such meets the State's IT-act also. This solution is known to be implemented by at least two other States.

R7-p3_v2_sIV_0007

Reference:
Doc 9303-part 3-third edition: Volume 2, Section IV, Appendix 5.
See also Supplement issue R6-p1_v2_sIV_0052.

Issue:
9303 Part - 3 Volume 2, figure IV-5-4 TDS Encryption is misleading. It is not clear in which way the parts of the figure belong to each other.

Conclusion:
Accepted.

Clarification:
Corrected drawings are incorporated into Appendix D of this Supplement.

R7-p3_v2_sIV_0008

Reference:
Doc 9303-part 3-third edition: Volume 2, Section IV, 9.5.
Also Supplement issue R7-p1_v2_sIV_0055.

Issue:
Doc9303 does not specify the use of ARLs. CRLs can be used in case a CSCA needs to be revoked. Which authority should sign the CRL in such an event?

Conclusion:
See clarification

Clarification:
A valid approach for the CSCA is to issue a CRL signed with the CSCA's compromised key. The compromised key is the only key the receiver of the CRL is able to validate.

An attacker who has compromised the key is not expected to issue a rogue CRL, since he then will not be able to benefit from it anymore.
Therefore, at the moment the CRL is received the key should be regarded as being still valid. After that moment the key is compromised.

R7-p3_v2_sIV_0009

Reference:
Doc 9303-part 3-third edition: Volume 2, Section IV, 8.4.
Also Supplement issue R7-p1_v2_sIV_0056.

Issue:
This Supplement recommends that for ECDSA, next to the reference to ANSI X9.62, implementers MUST also acknowledge ISO/IEC 15946-1&2 as a reference (see R3-p1_v2_sIV_0040). ISO/IEC 15946 allows for hashes > SHA-1, where ANSI X9.62 does not. However, no OID's for these combinations have been defined. The 2005 revision of X9.62 2005 defines OIDs but not all of them are sensible to use. There is a need for guidance.

Conclusion:
Accepted

Clarification:
It is RECOMMENDED to follow the guideline “TR03111_Elliptic Curve CryptographyBased on ISO 15946”. The present version of this guideline is V1.00, dated 14-02-2007. A new version has been announced. When it becomes available this will be notified in the Supplement.

R7-p3_v2_sIV_0010

Reference:
Doc 9303-part 3-third edition: Volume 2, Section IV, 8.1 and 8.4.
Also Supplement issue R7-p1_v2_sIV_0057.

Issue:
Doc9303 specifies in section IV, paragraph 8.1 with respect to Active Authentication that “For signature generation in the Active Authentication mechanism, States SHALL use ISO/IEC 9796-2 Digital Signature scheme 1 (ISO/IEC 9796-2, Information Technology — Security Techniques — Digital Signature Schemes giving message recovery — Part 2: Integer factorisation based mechanisms, 2002.)”

Doc9303 specifies in section IV, paragraph 8.4 with respect to the use of ECDSA that “Those States implementing the ECDSA algorithm for signature generation or verification SHALL use X 9.62 (X9.62, “Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)”, 7 January 1999).

ISO/IEC 9796 specifies that the hash value is incorporated in the signature format. X9.62 specifies that the hash value itself must be used as input for the signature algorithm. This is confusing, use of ECDSA conforming to X9.62 would violate the requirement in paragraph 8.1.

Conclusion:
Accepted

Clarification:
For reasons of clarity and interoperability it is RECOMMENDED to use RSA for Active Authentication and comply to section IV, paragraph 8.1. In this case X9.62 is not relevant and therefore not confusing.

R8-p1_v2_sIV_0011

Reference:
Doc 9303-part 3-third edition: Volume 2, Section IV, 9.1 and Appendix A.1.1, A.1.2, Appendix 2, Appendix A.3.2, and Appendix A.4.1.
Also Supplement issue R8-p1_v2_sIV_0058.

Issue:
It should be noted that RFC 5280, *D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", May 2008* supersedes RFC 3280, *R. Housley, W. Polk, W. Ford, D. Solo, "X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002.*

Conclusion:
Accepted

Clarification:
References to RFC 3280 should be interpreted as references to RFC 5280. Contents wise there is no difference, except for the Certificate Extension **PrivateKeyUsagePeriod**, which is not specified in RFC 5280. **PrivateKeyUsagePeriod** is the issuing period of the private key (ref. RFC3280, section 4.2.1.4).

R8-p3_v2_sIV_0012

Reference:
Doc 9303-part 3-third edition: Volume 2, Section IV, 5.5.1.
Also Supplement issue R8-p1_v2_sIV_0059.

Issue:
States are required to exchange their CSCA certificates bilaterally by diplomatic means. The first years in which States issue e-passports show that the lack of detailed specifications on mechanisms for this exchange has lead to wide interpretation and inefficient processes.
A more efficient way of CSCA Certificate exchange should be specified.

Conclusion:
Accepted

Clarification:
Such specifications are now provided by ICAO's Technical Report "CSCA countersigning and Master List issuance", version 1.0, June 2009. The approach described in this Technical Report aims to provide an electronic means of distributing and publishing issuing States' CSCA Public Keys. The modified approach is based on countersigning the CSCA certificates of issuing States by other States, and distributing the countersigned CSCA certificates via the ICAO PKD, to support but not to replace bilateral distribution of self-signed certificates.

R8-p3_v2_sIV_0013

Reference:
Doc 9303-part 3-third edition: Volume 2, Section IV, 8.1 and 8.4.
Also Supplement issue R8-p1_v2_sIV_0060.

Issue:
For reasons of clarity and interoperability this Supplement recommends to use RSA for Active Authentication and not ECDSA (see issue **R7-p1_v2_sIV_0010**). An unambiguous specification for the use of ECDSA in Active Authentication should be provided.

Conclusion:
Accepted

Clarification:
See Appendix F of this Supplement for the specification of the use of ECDSA in Active Authentication.

R8-p3_v2_sIV_0014

Reference:
Doc 9303-part 3-third edition: Volume 2, Section IV, 8.2.
Also Supplement issue R8-p1_v2_sIV_0061.

Issue:
RSA key lengths of 1024 bits should not be recommended anymore..

Conclusion:
Accepted

Clarification:
For newly issued eMRTDs the RECOMMENDED minimum key length for RSA is 1280 bits. Recommendations for the minimum lengths of the moduli of Document Signer Keys and Country Signing CA keys remain unchanged (2048 and 3072 bits respectively).
It should be noted that when using key lengths exceeding 1848 bits in Active Authentication, Extended Length must be supported by the Inspection System. Since the use of Extended Length is not specified in Doc 9303, systems may not support it and inspection might fail.

R8-p1_v2_sIV_0015

Reference:
Doc 9303-part 3-third edition: Volume 2, Section IV, 9.3.
Also Supplement issue R8-p1_v2_sIV_0062.

Issue:
It was decided that the storage of the Document Signer certificate in the Security Object will become MANDATORY.

Conclusion:
Accepted

Clarification:
The PKD board has endorsed specifications for the CSCA Master List (see ICAO's Technical Report "CSCA countersigning and Master List issuance", version 1.0, June 2009) as a means of CSCA certificate distribution through the PKD. Also the decision was taken to MANDATORY store the DS certificate on the chip in the Document Security Object for newly issued eMRTDs.

R11-p3_v2_sIV_0016

Reference:
Doc 9303-part 1-sixth edition: Volume 2, Section IV.
Also Supplement issue R11-p1_v2_sIV_0063.

Issue:
States are issuing CSCAs with a specific key usage period corresponding to the time period within which the CSCA will be used to sign Document Signers. The current practice in some States is to issue a long term CRL just before the expiry of the private key to cover the period for which the CSCA itself is valid. There is no guidance on how to issue a CRL in case of discovery of compromise on a DSC after the private key of the CSCA is no longer valid.

Conclusion:
See clarification

Clarification:
It should be noted that for signing CRLs and Document Signer Certificates always the actual (newest) CSCA Private Key MUST be used. This prevents the problem from occurring.

Appendix A TLV structured example of Document Security Object

The example shown below is based on the Silver Data Set.
The Distinguished Encoding Rules (DER) as specified in ISO/IEC 8825-1 (Information Technology - ASN.1 encoding rules) have been applied.

```
+- Application specific[23], length: 1188
| +- Sequence/sequence of , length: 1184
| | +- Object Identifier: signedData (1 2 840 113549 1 7 2)
| | +- Context specific[0], length: 1169
| | | +- Sequence/sequence of , length: 1165
| | | | +- Integer: 3
| | | | +- Set/set of , length: 11
| | | | | +- Sequence/sequence of , length: 9
| | | | | | +- Object Identifier: sha1 (1 3 14 3 2 26)
| | | | | | +- NULL, length: 0
| | | | +- Sequence/sequence of , length: 87
| | | | | +- Object Identifier: 1.2.528.1.1006.1.20.1
| | | | | +- Context specific[0], length: 74
| | | | | | +- Octet string , length: 72 << VALUE DECODED >>
                  +- Sequence/sequence of , length: 70
                  | +- Integer: 0
                  | +- Sequence/sequence of , length: 9
                  | | +- Object Identifier: sha1 (1 3 14 3 2 26)
                  | | +- NULL, length: 0
                  | +- Sequence/sequence of , length: 54
                  | | +- Sequence/sequence of , length: 25
                  | | | +- Integer: 1
                  | | | +- Octet string , length: 20
                  | | |        8D 1A CA 0B ED A1 4C EE B6 93 0B 5E A0 84 EF C0 ......L....^....
                  | | |        B9 67 0A 66                                     .g.f
                  | | +- Sequence/sequence of , length: 25
                  | | | +- Integer: 2
                  | | | +- Octet string , length: 20
                  | | |        8C D7 79 72 32 FC 58 76 A5 3E 5D BF 43 A2 C9 82 ..yr2.Xv.>].C...
                  | | |        EB 45 3B A9                                     .E;.
| | | | +- Context specific[0], length: 710
| | | | | +- Sequence/sequence of , length: 706
| | | | | | +- Sequence/sequence of , length: 426
| | | | | | | +- Context specific[0], length: 3
| | | | | | | | +- Integer: 2
| | | | | | | +- Integer: 18438939642695622
| | | | | | | +- Sequence/sequence of , length: 13
| | | | | | | | +- Object Identifier: sha1withRSAEncryption (1 2 840 113549 1 1 5)
| | | | | | | | +- NULL, length: 0
| | | | | | | +- Sequence/sequence of , length: 100
| | | | | | | | +- Set/set of , length: 27
| | | | | | | | | +- Sequence/sequence of , length: 25
| | | | | | | | | | +- Object Identifier: commonName (2 5 4 3)
| | | | | | | | | | +- Printable string (ASCII subset): "Country Signing CA"
| | | | | | | | +- Set/set of , length: 27
| | | | | | | | | +- Sequence/sequence of , length: 25
| | | | | | | | | | +- Object Identifier: organizationalUnitName (2 5 4 11)
| | | | | | | | | | +- Printable string (ASCII subset): "Country Signing CA"
| | | | | | | | +- Set/set of , length: 27
| | | | | | | | | +- Sequence/sequence of , length: 25
| | | | | | | | | | +- Object Identifier: organizationName (2 5 4 10)
| | | | | | | | | | +- Printable string (ASCII subset): "Country Signing CA"
| | | | | | | | +- Set/set of , length: 11
| | | | | | | | | +- Sequence/sequence of , length: 9
| | | | | | | | | | +- Object Identifier: countryName (2 5 4 6)
| | | | | | | | | | +- Printable string (ASCII subset): "NL"
| | | | | | | +- Sequence/sequence of , length: 30
| | | | | | | | +- UTC time: 29-10-04 10:40:47, Local time: 29-10-04 12:40:47
| | | | | | | | +- UTC time: 29-01-10 11:40:47, Local time: 29-01-10 12:40:47
| | | | | | | +- Sequence/sequence of , length: 46
| | | | | | | | +- Set/set of , length: 31
| | | | | | | | | +- Sequence/sequence of , length: 29
| | | | | | | | | | +- Object Identifier: commonName (2 5 4 3)
| | | | | | | | | | +- Printable string (ASCII subset): "Silver Document Signer"
| | | | | | | | +- Set/set of , length: 11
| | | | | | | | | +- Sequence/sequence of , length: 9
| | | | | | | | | | +- Object Identifier: countryName (2 5 4 6)
| | | | | | | | | | +- Printable string (ASCII subset): "NL"
| | | | | | | +- Sequence/sequence of , length: 159
| | | | | | | | +- Sequence/sequence of , length: 13
| | | | | | | | | +- Object Identifier: rsaEncryption (1 2 840 113549 1 1 1)
| | | | | | | | | +- NULL, length: 0
| | | | | | | | +- Bit string , length: 141
| | | | | | | |        00 30 81 89 02 81 81 00 CC 41 43 F1 27 33 E7 3A       .0.......AC.'3.:
| | | | | | | |        52 1F 53 BE 10 06 66 55 63 51 46 E7 2D 55 15 7B       R.S...fUcQF.-U.{
| | | | | | | |        22 35 16 73 00 64 45 F8 8B 0C 3E 80 87 D2 98 98       "5.s.dE...>.....
| | | | | | | |        4A FC FD 76 67 F3 8B 50 82 9F D8 06 C0 A4 56 E7       J..vg..P......V.
| | | | | | | |        F6 9A A4 69 C0 31 41 40 04 97 0E 3D 44 01 CF F3       ...i.1A@...=D...
| | | | | | | |        62 CA 70 39 69 37 B6 91 FF 80 16 3B 9F 0E B9 84       b.p9i7.....;....
| | | | | | | |        D5 36 1F 5A 9B 4D 6F A1 7E F1 FC 13 EE CE C3 9C       .6.Z.Mo.~........
| | | | | | | |        EA 68 3C 6A 21 7D 6F C4 34 F4 34 DA BF 10 EC F8       .h<j!}o.4.4.....
| | | | | | | |        27 3C 81 4D 97 31 77 01 02 03 01 00 01                '<.M.1w......
| | | | | | | +- Context specific[3], length: 51
| | | | | | | | +- Sequence/sequence of , length: 49
| | | | | | | | | +- Sequence/sequence of , length: 14
| | | | | | | | | | +- Object Identifier: keyUsage (2 5 29 15)
| | | | | | | | | | +- Boolean: TRUE
| | | | | | | | | | +- Octet string , length: 4 << VALUE DECODED >>
                          +- Bit string , length: 2 << VALUE DECODED >>
                              +- Object Descriptor: , length: 0
```

```
| | | | | | | | | +- Sequence/sequence of , length: 31
| | | | | | | | | | +- Object Identifier: authorityKeyIdentifier (2 5 29 35)
| | | | | | | | | | +- Octet string , length: 24 << VALUE DECODED >>
                       +- Sequence/sequence of , length: 22
                       | +- Context specific[0], length: 20
                       |        1A A3 10 81 D8 E7 75 F6 98 8F 2A 32 F4 DE 6A DC      ......u...*2..j.
                       |        19 9B 83 17                                          ....
| | | | | | +- Sequence/sequence of , length: 13
| | | | | | | +- Object Identifier: sha1withRSAEncryption (1 2 840 113549 1 1 5)
| | | | | | | +- NULL, length: 0
| | | | | | +- Bit string , length: 257
| | | | | |        00 99 A5 86 CE EF 7B 2A CE 39 AB 8A E6 DA F6 B8   ......{*.9......
| | | | | |        85 9F AB 06 DE 8F 69 5B 18 8A 10 B0 6B B6 2F 55   ......i[....k./U
| | | | | |        99 58 05 E7 D2 F6 4F 16 61 5F EA DE 87 84 79 EA   .X....O.a_....y.
| | | | | |        D2 9D 37 19 C0 A2 6A 31 0E 62 6C B5 B3 0D E1 5E   ..7...j1.bl....^
| | | | | |        13 8C 69 26 5D 0B 4D 92 63 FE 5E 04 C3 C8 5A F4   ..i&].M.c.^...Z.
| | | | | |        05 27 99 94 DB CC D1 9D 05 AF 42 74 8F 2F 89 FD   .'........Bt./..
| | | | | |        DF 07 11 C0 1C 1E A2 1C B2 E6 B5 D9 C6 50 77 CD   .............Pw.
| | | | | |        45 9A A2 38 7B E1 9E 46 68 41 AB 30 F9 F0 FE 84   E..8{..FhA.0....
| | | | | |        81 BE 38 B5 EB B5 78 00 93 AB 2A D7 CC B3 47 09   ..8...x...*...G.
| | | | | |        C4 23 CD B8 ED 65 E0 53 85 82 5C 4B 2C 3F 8C 1F   .#...e.S..\K,?..
| | | | | |        8B D8 DA D7 56 AB 72 8F D3 10 D0 65 84 30 83 1D   ....V.r....e.0..
| | | | | |        B8 D9 45 14 47 D2 82 31 32 1C 75 6E F4 82 87 EE   ..E.G..12.un....
| | | | | |        F7 0F 0D EC 00 FE 85 59 7A 98 69 7A 86 05 45 6D   .......Yz.iz..Em
| | | | | |        D2 D8 2E 9C F5 47 F2 BF 50 EC FA 2C 7D 49 ED EC   .....G..P..,}I..
| | | | | |        AD 2A D3 BB 7E CA 0E 54 1D A4 67 36 40 B0 A5 A6   .*..~..T..g6@...
| | | | | |        67 AB 04 2F BB 63 13 89 CD 63 BB FE 7B 23 92 D5   g../.c...c..{#..
| | | | | |        3F                                               ?
| | | | +- Set/set of , length: 342
| | | | | +- Sequence/sequence of , length: 338
| | | | | | +- Integer: 1
| | | | | | +- Sequence/sequence of , length: 111
| | | | | | | +- Sequence/sequence of , length: 100
| | | | | | | | +- Set/set of , length: 27
| | | | | | | | | +- Sequence/sequence of , length: 25
| | | | | | | | | | +- Object Identifier: commonName (2 5 4 3)
| | | | | | | | | | +- Printable string (ASCII subset): "Country Signing CA"
| | | | | | | | +- Set/set of , length: 27
| | | | | | | | | +- Sequence/sequence of , length: 25
| | | | | | | | | | +- Object Identifier: organizationalUnitName (2 5 4 11)
| | | | | | | | | | +- Printable string (ASCII subset): "Country Signing CA"
| | | | | | | | +- Set/set of , length: 27
| | | | | | | | | +- Sequence/sequence of , length: 25
| | | | | | | | | | +- Object Identifier: organizationName (2 5 4 10)
| | | | | | | | | | +- Printable string (ASCII subset): "Country Signing CA"
| | | | | | | | +- Set/set of , length: 11
| | | | | | | | | +- Sequence/sequence of , length: 9
| | | | | | | | | | +- Object Identifier: countryName (2 5 4 6)
| | | | | | | | | | +- Printable string (ASCII subset): "NL"
| | | | | | | +- Integer: 18438939642695622
| | | | | | | +- Sequence/sequence of , length: 9
| | | | | | | | +- Object Identifier: sha1 (1 3 14 3 2 26)
| | | | | | | | +- NULL, length: 0
| | | | | | | +- Context specific[0], length: 63
| | | | | | | | +- Sequence/sequence of , length: 24
| | | | | | | | | +- Object Identifier: contentType (1 2 840 113549 1 9 3)
| | | | | | | | | +- Set/set of , length: 11
| | | | | | | | | | +- Object Identifier: 1.2.528.1.1006.1.20.1
| | | | | | | | +- Sequence/sequence of , length: 35
| | | | | | | | | +- Object Identifier: messageDigest (1 2 840 113549 1 9 4)
| | | | | | | | | +- Set/set of , length: 22
| | | | | | | | | | +- Octet string , length: 20
| | | | | | | | | |        22 CB 92 1D 3C A9 62 8C 77 EB 78 D7 3D 04 B7 4C     "...<.b.w.x.=..L
| | | | | | | | | |        3D AA 22 67                                         =."g
| | | | | | | | +- Sequence/sequence of , length: 13
| | | | | | | | | +- Object Identifier: sha1withRSAEncryption (1 2 840 113549 1 1 5)
| | | | | | | | | +- NULL, length: 0
| | | | | | | +- Octet string , length: 128
| | | | | | |        98 0B A6 C7 C1 AE 81 FE D2 B9 5B B6 43 C4 D2 88   ..........[.C...
| | | | | | |        59 EE 54 23 75 72 28 52 CF 4C 82 42 B2 41 80 FE   Y.T#ur(R.L.B.A..
| | | | | | |        11 BA DC 5B 4E D4 09 3A 20 C6 F7 BD FF C4 0C D0   ...[N..: .......
| | | | | | |        DB 43 F9 AA 96 8A E7 12 37 9F 76 2F D1 55 62 C6   .C......7.v/.Ub.
| | | | | | |        07 DA C0 2D 0A E0 4A A7 C9 AE 7D C1 01 D8 33 6F   ...-..J...}...3o
| | | | | | |        A8 B9 72 FE 1B 2A D4 63 74 2E 26 A5 3B C4 44 20   ..r..*.ct.&.;.D
| | | | | | |        CB E4 FD 06 AC 83 06 D2 20 38 B9 40 DA 65 BA 30   ........ 8.@.e.0
| | | | | | |        5D CE D1 47 09 99 63 DF 3C 08 3D FA 35 9E 1E 78   ]..G..c.<.=.5..x
```

Appendix B Abstract of RFC 2119

S. Bradner, "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

Key words for use in RFCs to Indicate Requirement Levels

Abstract

In many standards track documents several words are used to signify the requirements in the specification. These words are often capitalized. This document defines these words as they should be interpreted in IETF documents. Authors who follow these guidelines should incorporate this phrase near the beginning of their document:

> The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Note that the force of these words is modified by the requirement level of the document in which they are used.

1. MUST This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

2. MUST NOT This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

3. SHOULD This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

4. SHOULD NOT This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

5. MAY This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

6. Guidance in the use of these Imperatives

Imperatives of the type defined in this memo must be used with care and sparingly. In particular, they MUST only be used where it is actually required for interoperation or to limit behavior which has potential for causing harm (e.g., limiting retransmisssions) For example, they must not be used to try to impose a particular method on implementors where the method is not required for interoperability.

7. Security Considerations

These terms are frequently used to specify behavior with security implications. The effects on security of not implementing a MUST or SHOULD, or doing something the specification says MUST NOT or SHOULD NOT be done may be very subtle. Document authors should take the time to elaborate the security implications of not following recommendations or requirements as most implementors will not have had the benefit of the experience and discussion that produced the specification.

8. Acknowledgments

The definitions of these terms are an amalgam of definitions taken from a number of RFCs. In addition, suggestions have been incorporated from a number of people including Robert Ullmann, Thomas Narten, Neal McBurnett, and Robert Elz.

Appendix C Bilateral exchange

See R8-p1_v2_sIV_0059
Country Signing Certificates and CRLs must be distributed bilaterally. No specific mechanism for bilateral exchange other than "diplomatic exchange" is defined in the technical report, and some States have already started with the distribution of their CSCA Certificates.

- Australia: CSCA Certificates are directly sent by email.
- Germany: Fingerprints of the CSCA Certificates are distributed in printed form, the certificates can be downloaded from a web site (URL is printed on the paper).
- USA: CDs containing the CSCA Certificates are distributed, a URL is provided that can be used to validate the certificate fingerprints.

The problems that arise with the distribution of self-signed certificates are as follows: a) The recipients are not a-priori known to the sender and b) the recipient does not know how to verify the authenticity of received data.

Both problems are related to the same solution: An authentic list of authorized contact persons in every State is required. We call this list the *CSCA Register*[1].
The CSCA Register is a list of contact details of the CSCA of every State issuing or reading e-passports.
The following information is REQUIRED:

- The name, the postal address, and the email-address of the person responsible for the operation of the CSCA.
- An LDAP server containing the certificates and CRLs issued by the CSCA.

The following information is OPTIONAL:

- A fax number.
- A website containing (additional) information on the CSCA, e.g. a certificate policy and/or a certification practice statement.

Contact Details	ICAO Register	CSCA Certificate	Format
Name	REQUIRED	N/A	UTF8
Postal address	REQUIRED	N/A	UTF8
Email address	REQUIRED	RECOMMENDED	RFC....
LDAP address	REQUIRED	RECOMMENDED	URL (ldap://)
Fax number	OPTIONAL	OPTIONAL	URL (fax://)
Website	OPTIONAL	OPTIONAL	URL (http://)

Bilateral Exchange of CSCA Certificates
As discussed above, there are various methods to distribute CSCA Certificates. Unless very uncommon media are used, the recipient should be able to retrieve the certificate. As this mechanism is not used very frequently, there is no need to standardize on a certain mechanism.
To verify a received certificate the recipient should use the CSCA register to find out the contact details of the issuing CSCA. Then the recipient should use at least two independent communication channels to validate the fingerprints of the received certificate (e.g. email and fax).

Bilateral Exchange of CRLs
Every CSCA must store its own CRLs on the local LDAP server. To inform other States of exceptional CRLs for every State the CSCA Register must be used to find out the contact details of the receiving CSCA. Then the issuing CSCA must use at least two independent communication

[1] Independently of this CSCA Register, Australia has compiled a list of "authorized recipients" to distribute their CSCA Certificates.

channels to send a notification to the receiving CSCA. It is recommended that the receiving CSCA acknowledges a received notification.

Appendix D Doc9303 part 1 sixth edition, App. 5 to Sect. IV - Figures

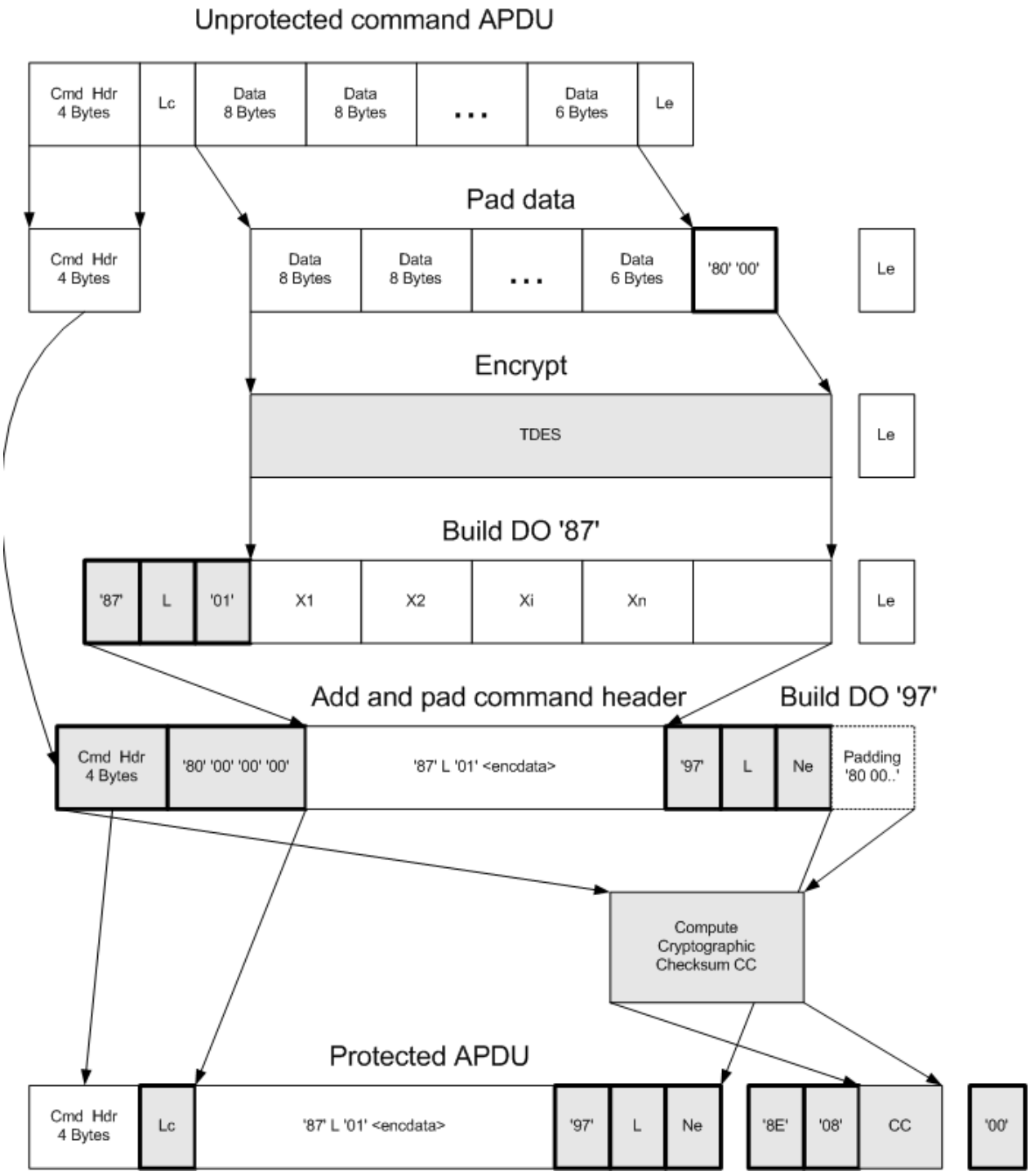


Figure IV-5-2. Example of computation of a SM command APDU for even INS byte

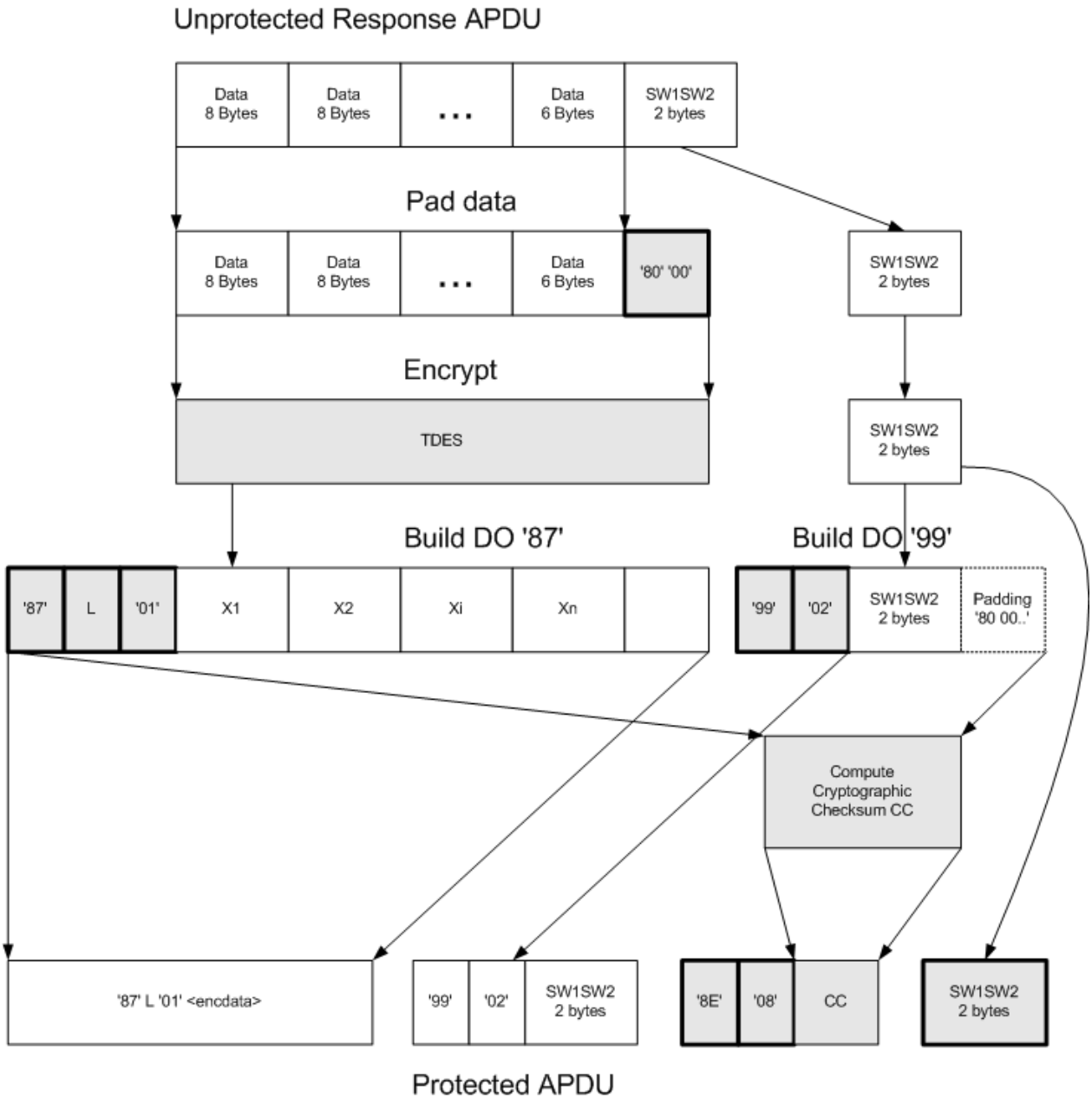


Figure IV-5-3. Example of computation of a SM response APDU for even INS byte

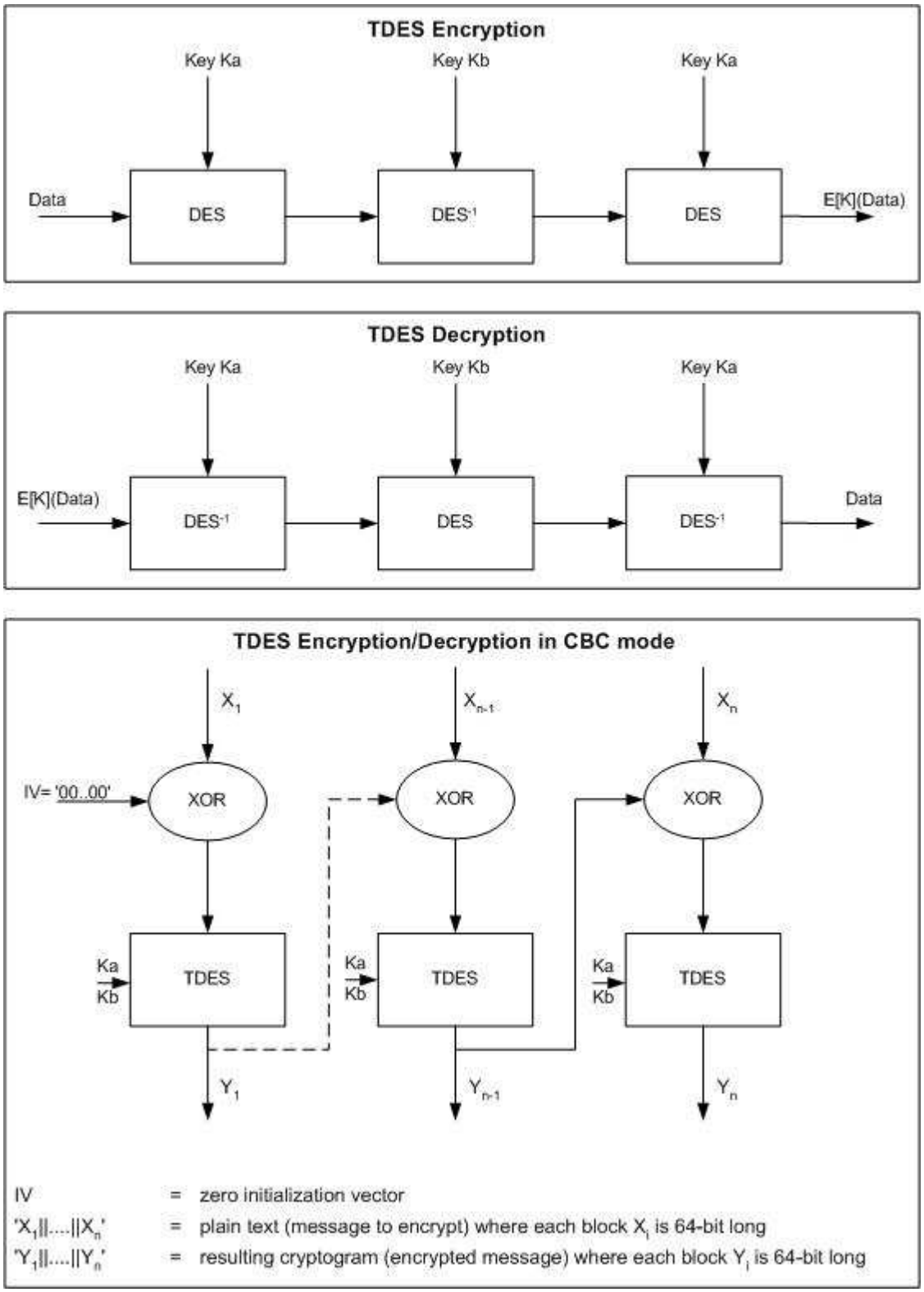


Figure IV-5-4. 3DES Encryption/Decryption in CBC Mode

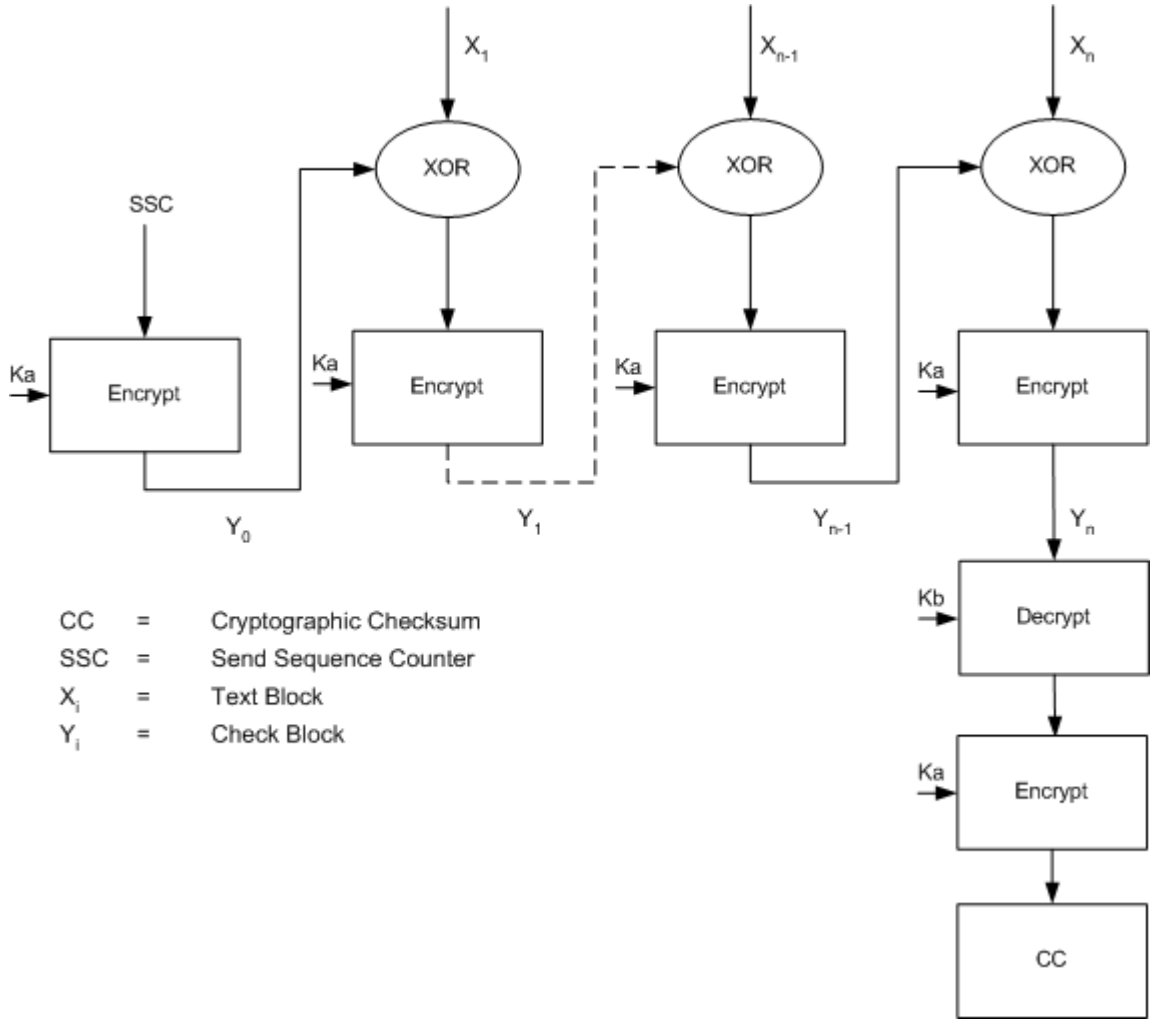


Figure IV-5-5: Retail MAC calculation

Appendix E Updated security standards

INFORMATIVE APPENDIX 1 to Section III

SECURITY STANDARDS FOR MACHINE READABLE TRAVEL DOCUMENTS

1. Scope

1.1 This Appendix provides advice on strengthening the security of machine readable travel documents made in accordance with the specifications set out in Doc 9303, Part 1 (Machine Readable Passports), Part 2 (Machine Readable Visas) and Part 3 (Machine Readable Size 1 and Size 2 Official Travel Documents). The recommendations cover the security of the materials used in the document's construction, the security printing and copy protection techniques to be employed, and the processes used in the production of document blanks. Also addressed are the security considerations that apply to the personalization and the protection of the biographical data in the document. All travel document-issuing authorities shall consider this Appendix.

2. Introduction

2.1 The worldwide increase in the number of people travelling and the expected continuing growth, together with the growth in international crime, terrorism, and illegal immigration has led to increasing concerns over the security of travel documents and calls for recommendations on what may be done to help improve their resistance to attack or misuse. Historically, Doc 9303 has not made recommendations on the specific security features to be incorporated in travel documents. Each issuing State has been free to incorporate such safeguards as it deemed appropriate to protect its nationally issued travel documents against counterfeiting, forgery and other forms of attack, as long as nothing was included which would adversely affect their OCR machine readability.

2.2 To meet the need of increased document security, ICAO’s technical advisors decided it would be desirable to publish a set of “recommended minimum security standards” as a guideline for all States issuing machine readable travel documents. This Appendix describes security measures to be taken within the structure of the MRTD and of the premises in which it is produced. Appendix **2** describes optional means of achieving machine-assisted document verification. Appendix **3** describes the security measures to be taken to ensure the security of the personalization operations and of the documents in transit.

2.3 This Appendix identifies the security threats to which travel documents are frequently exposed and the counter-measures that may be employed to protect these documents and their associated personalization systems. The lists of security features and/or techniques offering protection against these threats have been subdivided into: 1) basic security features and/or techniques considered essential and; 2) additional features and/or techniques from which States are encouraged to select items which are recommended for providing an enhanced level of security. This approach recognizes that a feature or technique that may be necessary to protect one State's documents may be superfluous or of minor importance to another State using different production systems. A targeted approach that allows States flexibility to choose from different document systems (paper-based documents, plastic cards, etc.) and a combination of security features and/or techniques most appropriate to their particular needs is therefore preferred to a "one size fits all" philosophy. However, to help ensure that a balanced set of security features and/or techniques is chosen, it is necessary for each State to conduct a risk assessment of its national travel documents to identify their

most vulnerable aspects and select the additional features and/or techniques that best address these specific problems.

2.4 The aim of the recommendations in this Appendix is to improve the security of machine readable travel documents worldwide by establishing a baseline for issuing States. Nothing within these recommendations shall prevent or hinder States from implementing other, more advanced security features, at their discretion, to achieve a standard of security superior to the minimum recommended features and techniques set forth in this Appendix.

2.5 A glossary of technical terms has been included with this Appendix in paragraph **6**

2.6 A summary table of typical security threats relating to travel documents and some of the security features and techniques that can help to protect against these threats is included.

3. Basic principles

3.1 Production and storage of passport books and travel documents, including the personalization processes, should be undertaken in a secure, controlled environment with appropriate security measures in place to protect the premises against unauthorized access. If the personalization process is decentralized, or if personalization is carried out in a location geographically separated from where the travel document blanks are made, appropriate precautions should be taken when transporting the blank documents and any associated security materials to safeguard their security in transit and storage on arrival. When in transit blank books or other travel documents should contain the unique document number. In the case of passports the passport number should be on all pages other than the biographical data page where it can be printed during personalization.

3.2 There should be full accountability over all the security materials used in the production of good and spoiled travel documents and a full reconciliation at each stage of the production process with records maintained to account for all security material usage. The audit trail should be to a sufficient level of detail to account for every unit of security material used in the production and should be independently audited by persons who are not directly involved in the production. Records certified at a level of supervision to ensure accountability should be kept of the destruction of all security waste material and spoiled documents.

3.3 Materials used in the production of travel documents should be of controlled varieties where applicable, and obtained only from reputable security materials suppliers. Materials whose use is restricted to high security applications should be used, and materials that are available to the public on the open market should be avoided.

3.4 Sole dependence upon the use of publicly available graphics design software packages for originating the security backgrounds should be avoided. These software packages may however be used in conjunction with specialist security design software.

3.5 Security features and/or techniques should be included in travel documents to protect against unauthorized reproduction, alteration and other forms of tampering, including the removal and substitution of pages in the passport book, especially the biographical data page. In addition to those features included to protect blank documents from counterfeiting and forgery, special attention must be given to protect the biographical data from removal or alteration. A travel document should include adequate security features and/or techniques to make evident any attempt to tamper with it.

3.6 The combination of security features, materials and techniques should be well chosen to ensure full compatibility and protection for the lifetime of the document.

3.7 Although this Appendix deals mainly with security features that help to protect travel documents from counterfeiting and fraudulent alteration, there is another class of security features comprised of covert (secret) features designed to be authenticated either by forensic examination or by specialist verification equipment. It is evident that knowledge of the precise substance and structure of such features should be restricted to very few people on a "need to know" basis. Among others, one purpose of these features is to enable authentication of documents where unequivocal proof of authenticity is a requirement (e.g., in a court of law). All travel documents should contain at least one covert security feature as a basic feature.

3.8 Important general standards and recommended practices for passport document validity period, one-person-one-passport principle, deadlines for issuance of Machine Readable Passports and withdrawal from circulation of non-MRPs and other guidance is found in ICAO Facilitation Annex 9.

3.9 As noted in Part 1, Volume 2, there is no other acceptable means of data storage for global interoperability other than a high-capacity contactless IC storage medium, specified by ICAO as the capacity expansion technology for use with Passports.

4. Main threats to the security of travel documents

4.1 The following threats to document security, listed in no particular order of importance, are identified ways in which the document, its issuance and use may be fraudulently attacked:

- Counterfeiting a complete travel document
- Photo substitution
- Deletion/alteration of data in the visual or machine readable zone of the MRP data page
- Construction of a fraudulent document, or parts thereof, using materials from legitimate documents
- Removal and substitution of entire page(s) or visas
- Deletion of entries on visa pages and the observations page
- Theft of genuine document blanks
- Impostors (assumed identity; altered appearance).
- Tampering with the contactless IC (where present) either physically or electronically.

These threats may be considered by using the following approach:

Detection of security features can be at any or all of the following three levels of inspection:

- Level 1– Cursory examination for rapid inspection at the point of usage (easily identifiable visual or tactile features)
- Level 2 – Examination by trained inspectors with simple equipment
- Level 3 – Inspection by forensic specialists

To maintain document security and integrity, periodic reviews and any resulting revisions of document design should be conducted. This will enable new document security measures to be incorporated and to certify the document’s ability to resist compromise and document fraud attempts regarding:

- Photo substitution
- Delamination or other effects of deconstruction
- Reverse engineering of the contactless IC as well as other components
- Modification of any data element
- Erasure or modification of other information
- Duplication, reproduction or facsimile creation

— Effectiveness of security features at all three levels: cursory examination, trained examiners with simple equipment and inspection by forensic specialists
— Confidence and ease of second level authentication

4.2 To provide protection against these threats and others, a travel document requires a range of security features and techniques combined in an optimum way within the document. Although some features can offer protection against more than one type of threat, no single feature can offer protection against them all. Likewise, no security feature is 100 per cent effective in eliminating any one category of threat. The best protection is obtained from a balanced set of features and techniques providing multiple integrated layers of security in the document that combine to deter or defeat fraudulent attack.

5. Security features and techniques

In the sections that follow, security features, techniques and other security measures are categorized according to the phases passed through during the production and personalization processes and the components of the travel document created thereby with regard to: 1) substrate materials; 2) security design and printing; 3) protection against copying, counterfeiting or fraudulent alteration; and 4) personalization techniques. Issuing States are recommended to incorporate all of the basic features/measures and to select a number of additional features/measures from the list having first completed a full risk assessment of their travel documents. Unless otherwise indicated, the security features may be assumed to apply to all parts of a travel document including the cover and the binding of the booklet and to all the interior pages of a passport, comprising the biographical data page, end leaves and visa pages. Care must be taken to ensure that features do not interfere with the machine readability of the travel document.

5.1 *Substrate Materials*

5.1.1 *Paper forming the pages of a travel document*

Basic features

— UV dull paper, or a substrate with a controlled response to UV, such that when illuminated by UV light it exhibits a fluorescence distinguishable in colour from the blue used in commonly available fluorescent materials;

— Watermark comprising two or more grey levels in the biographical data page and visa pages;

— Appropriate chemical sensitizers in the paper, at least for the biographical data page (if compatible with the personalization technique);

— Paper with appropriate absorbency, roughness and weak surface tear.

Additional features

— Watermark in register with printed design;

— A different watermark on the data page to that used on the visa pages to prevent page substitution;

— A cylinder mould watermark;

— Invisible fluorescent fibres;

— Visible (fluorescent) fibres;

— Security thread (embedded or window) containing additional security features such as micro print and fluorescence;

— A taggant designed for detection by special equipment.

— A laser perforated security feature.

5.1.2 *Paper or other substrate in the form of a label used as the biographical data page of a travel document*

Basic features

— UV dull paper, or a substrate with a controlled response to UV, such that when illuminated by UV light it exhibits a fluorescence distinguishable in colour from the blue used in commonly available fluorescent materials;

— Appropriate chemical sensitizers in the paper (not normally possible in a plastic label substrate);

— Invisible fluorescent fibres;

— Visible (fluorescent) fibres;

— A system of adhesives and/or other characteristics that prevents the label from being removed without causing clearly visible damage to the label and to any laminates or overlays used in conjunction with it.

Additional features

— Security thread (embedded or window) containing additional security features such as micro print and fluorescence;

— A watermark can be used in the paper of a data page in paper label form;

— A laser perforated security feature;

— Die cut security pattern within the label to create tamper evidence.

5.1.3 *Security aspects of paper forming the inside cover of a passport book*

— Paper used to form the inside cover of a passport book need not have a watermark. Although definitely not recommended, if an inside cover is used as a biographical data page, alternative measures must be employed to achieve an equivalent level of security against all types of attack as provided by locating the data page on an inside page;

— The paper forming the inside cover should contain appropriate chemical sensitizers when an inside cover is used as a biographical data page. The chemically sensitised paper should be compatible with the personalization technique, and the adhesive used

to adhere the end paper to the cover material of the passport.

5.1.4 *Synthetic substrates*

Where the substrate used for the biographical data page (or inserted label) of a passport book or MRTD card is formed entirely of plastic or a variation of plastic, it is not usually possible to incorporate many of the security components described in 5.1.1 through 5.1.3. In such cases additional security properties shall be included, including additional security printed features, enhanced personalization techniques and the use of optically variable features over and above the recommendations contained in 5.2 to 5.5.2. States should preferably ensure that the plastic substrate is manufactured under controlled conditions and contains distinctive properties, e.g. controlled fluorescence, to differentiate it from standard financial card substrates.

Basic Features

- Construction of the data page should be resistant to physical splitting into layers;
- Optically dull material to create contrast with fluorescent printing and as a countermeasure against alternative substrates;
- Appropriate measures should be used to incorporate the data page securely and durably into the passport;
- Optically variable feature.

Additional features

- Windowed or transparent feature;
- Tactile feature;
- Laser perforated feature.

5.2 *Security printing*

5.2.1 *Background and text printing*

Basic features (see glossary of terms)

- Two-colour guilloche security background design pattern[2];
- Rainbow printing;
- Microprinted text;
- Security background of the biographical data page printed in a design that is different from that of the visa pages or other pages of the document.

Additional features

- Single or multi-colour intaglio printing comprising a “black-line white-line” design

[2]. Where the guilloche pattern has been computer-generated, the image reproduced on the document must be such that no evidence of a pixel structure shall be detectable. Guilloches may be displayed as positive images, where the image lines appear printed with white spaces between them, or as negative images, where the image lines appear in white, with the spaces between them printed. A two-colour guilloche is a design that incorporates guilloche patterns created by superimposing two elements of the guilloche, reproduced in contrasting colours.

on one or more of the end leaves or visa pages;

— Latent (intaglio) image;

— Anti-scan pattern;

— Duplex security pattern;

— Relief (3-D) design feature;

— Front-to-back (see-through) register feature.

— Deliberate error (e.g. spelling);

— Every visa page printed with a different security background design;

— Tactile feature;

— Unique font(s) .

5.2.2 *Inks*

Basic features

— UV fluorescent ink (visible or invisible) on the biographical data page and all visa pages;

— Reactive ink, where the substrate of the document pages or of a label is paper, at least for the biographical data page (if compatible with the personalization technique).

Additional features

— Ink with optically variable properties;

— Metallic ink;

— Penetrating numbering ink;

— Metameric ink;

— Infrared drop-out ink;

— Infrared ink;

— Phosphorescent ink;

— Tagged ink;

— Invisible ink which fluoresces in different colours when exposed to different wave lengths.

5.2.3 *Numbering*

It is strongly recommended that the unique document number be used as the passport number.

Basic features

— The passport number should appear on all sheets of the document and on the biographical data page of the document.

— The number in a document shall be either printed and/or perforated.

— The document number on a label shall be in a special style of figures or typeface and be printed with ink that fluoresces under ultraviolet light in addition to having a visible colour.

— The number on a data page of a passport made of synthetic substrate or on an MRTD card can be incorporated using the same technique as is used for applying the biographical data in the personalisation process.

— For MRTD cards, the number should appear on both sides.

Additional features

— If perforated it is preferable that laser perforation is used. Perforate numbering of the data page is optional but care should be taken not to interfere with the clarity of the portrait or VIZ and not obstruct the MRZ in any way. It is desirable to perforate the cover of the passport.

— If printed it should ideally be in a special style of figures or typeface and be printed with an ink that fluoresces under ultraviolet light in addition to having a visible colour.

5.2.4 *Special security measures for use with non-laminated biographical data pages*

— The surface of the data page should be protected against soiling in normal use including regular machine reading of the MRZ, and against tampering.

— If a page of a document is used for biographical data that is not protected by a laminate or an overlay as a protective coating (see 5.3.2, 5.4.3 and 5.4.4), additional protection shall be provided by the use of intaglio printing incorporating a latent image and microprinting and preferably utilizing a colour-shifting ink (e.g. ink with optically variable properties).

5.2.5 *Special security measures for use with cards and biographical data pages made of plastic*

— Where a travel document is constructed entirely of plastic, optically variable security features shall be employed which give a changing appearance with angle of viewing. Such devices may take the form of latent images, lenticular features, colour-shifting ink, or diffractive optically variable image features.

5.3 *Protection against copying*

5.3.1 *Need for anticopy protection*

— The current state of development of generally available digital reproduction techniques and the resulting potential for fraud means that high-grade security features in the form of optically variable features or other equivalent devices will be required as safeguards against copying and scanning. Emphasis should be placed on the security of the biographical data page of a passport book, travel card or visa,

based on an independent, complex optically variable feature technology or other equivalent devices complementing other security techniques. Particular emphasis should be given to easily identifiable, visual or tactile features which are examined at level one inspection.

— Appropriate integration of optically variable feature components or other equivalent devices into the layered structure of the biographical data page should also protect the data from fraudulent alteration. The optically variable components and all associated security materials used to create the layered structure must also be protected against counterfeiting.

5.3.2 *Anticopy protection methods*

— Subject to the minimum recommendations described in 5.4.3 and 5.4.4 on the need for lamination, optically variable features should be used on the biographical data page of a passport book, travel card or visa as a *basic feature*.

— When a biographical data page of a passport book, travel card or visa is protected by a laminate film or overlay, an optically variable feature (preferably based on diffractive structure with tamper evident properties) should be integrated into the page. Such a feature should not affect the legibility of the entered data.

— When the biographical data page is an encapsulated paper label, or a page in a passport, the biographical data must be suitably protected by a protective laminate or measures providing equivalent security in order to deter alteration and/or removal.

— When the machine readable biographical data page of a passport book is made entirely of synthetic substrate, an optically variable feature should be incorporated. The inclusion of a diffractive optically variable feature is recommended to achieve an enhanced level of protection against reproduction.

— Devices such as a windowed or transparent feature, a laser perforated feature, and others are considered to offer equivalent protection may be used in place of an optically variable feature.

— When the travel document has no overlay or laminate protection, an optically variable feature (preferably based on diffractive structure) with intaglio overprinting or other printing technique shall be used.

5.4 *Personalization technique*

5.4.1 *Document personalization*

This is the process by which the portrait, signature and/or other biographical data relating to the holder of the document are applied to the travel document. This data records the personalized details of the holder and is at the greatest risk of counterfeit or fraudulent alteration. One of the most frequent types of document fraud involves the removal of the portrait image from a stolen or illegally obtained travel document and its replacement with the portrait of a different person. Documents with stick-in portrait photographs are particularly susceptible to photo substitution. Therefore, stick-in photographs are strongly NOT recommended.

5.4.2 *Protection against alteration*

To ensure that data are properly secured against attempts at forgery or fraudulent alteration it is very strongly recommended to integrate the biographical data, including the portrait, signature (if it is

included on the biographical data page) and main issue data, into the basic material of the document. A variety of technologies are available for imaging the document in this way, including the following, but not precluding the development of new technologies, which are listed in no particular order of importance:

— laser toner printing;

— thermal transfer printing;

— ink-jet printing;

— photographic processes;

— laser engraving.

The same imaging technologies may also be used to apply data to the observations page of the passport. Laser toner should not be used to personalise visas or other security documents that are not protected by a secure laminate.

Issuing authorities should carry out testing of their personalisation processes and techniques against malfeasance.

5.4.3 *Choice of document system*

The choice of a particular technology is a matter for individual issuing States and will depend upon a number of factors, such as the volume of travel documents to be produced, the construction of the document and whether it is to be personalized during the document or passport book making process or after the document or book has been assembled and whether a country issues passports centrally or from decentralised sites.

Whichever method is chosen, it is essential that precautions be taken to protect the personalized details against tampering. This is important because, even though eliminating the stick-in portrait reduces the risk of photo substitution, the unprotected biographical data remains vulnerable to alteration and needs to be protected by the application of a heat-sealed laminate with frangible properties, or equivalent technology that provides evidence of tampering.

5.4.4 *Protection against photo substitution and alteration of data on the biographical data page of a passport book*

Basic features

— Imaging the portrait and all biographical data by integration into the basic material;

— The security printed background (e.g., guilloche) shall merge within the portrait area;

— Use of reactive ink and chemical sensitizers in the paper;

— There should be a visible security device overlapping the portrait without obstructing the visibility of the portrait; an optically variable feature is recommended;

— Use of a heat-sealed secure laminate, or the combination of an imaging technology and substrate material that provide an equivalent resistance to substitution and/or counterfeit of the portrait and other biographical data.

Additional features

— Displayed signature of the holder may be scanned and incorporated into the printing, as per paragraph 7.2 of Section IV, Volume 1 Part 1 MRP Specification;

— Steganographic image incorporated in the document;

— Additional portrait image(s) of holder;

— Machine verifiable biometric feature as detailed in Volume 2, Specifications for Electronically Enabled Passports with Biometric Identification Capability.

5.5 *Additional security measures for passport books*

5.5.1 *Position of the biographical data page*

It is recommended that States place the data page on an inside page (the second or penultimate page). When the data page is situated on the inside cover of a MRP, the normal method of construction used in the manufacture of passport covers has facilitated fraudulent attacks on the data page, typically photo substitution or whole-page substitution. However, an issuing State may place the data page on a cover provided that it ensures that the construction of the cover used in its passport offers a similar level of security against all types of fraudulent attack to that offered by locating the data page on an inside page. Placing the biographical data page on the cover is, nevertheless, strongly NOT recommended.

5.5.2 *Whole-page substitution*

Issuing States' attention is drawn to the fact that with integrated biographical data pages replacing stick-in photographs in passports, some cases of whole-page substitution have been noted in which the entire biographical data page of the passport has been removed and substituted with a fraudulent one. Although whole-page substitution is generally more difficult to effect than photo substitution of a stick-in photo, nevertheless, it is important that the following recommendations be adopted to help in combating this category of risk. As with all other categories of document fraud it is better to employ a combination of security features to protect against whole-page substitution rather than relying on a single feature which, if compromised, could undermine the security of the whole travel document.

Basic features

— The sewing technology that binds the pages into the book must be such that it must be difficult to remove a page without leaving clear evidence that it has happened;

— Security background of the biographical data page printed in a design that is different from that of the visa pages;

— Page numbers integrated into the security design of the visa pages;

— Serial number on every sheet, preferably perforated.

Additional features

— Multi-colour and/or specifically UV fluorescent sewing thread;

— Programmable thread-sewing pattern;

— UV cured glue applied to the stitching;

— Index or collation marks printed on the edge of every visa page;

— Laser perforated security features to the biographical data page

— Biographical data printed on an inside page in addition to the data page.

Where self-adhesive labels are used, additional security requirements as described in 5.1.2 and 5.2.4 are advised including linking the label to the passport book by the passport number.

5.6 *Quality control*

Quality checks and controls at all stages of the production process and from one batch to the next are essential to maintain consistency in the finished travel document. This should include quality assurance (QA) checks on all materials used in the manufacture of the documents and the readability of the machine readable lines. The importance of consistency in the finished travel document is paramount because immigration inspectors and border control officers rely upon being able to recognize fake documents from variations in their appearance or characteristics. If there are variations in the quality, appearance or characteristics of a State's genuine travel documents, detection of counterfeit or forged documents is made more difficult.

5.7 *Security control of production and product*

A major threat to the security of the MRP of an issuing State can come from the unauthorized removal from the production facility of genuine finished, but unpersonalized, MRPs or the components from which MRPs can be made.

5.7.1 *Protection against theft and abuse of genuine document blanks or document components*

Blank documents should be stored in locked and appropriately supervised premises. The following measures should be adopted:

Basic measures

— Good physical security of the premises with controlled access to delivery/shipment and production areas, and document storage facilities;

— Full audit trail, with counting and reconciliation of all materials (used, unused, defective or spoiled) and certified records of same;

— All document blanks and other security-sensitive components serially numbered with full audit trail for every document from manufacture to dispatch, as applicable;

— Where applicable, tracking and control numbers of other principal document components (e.g. rolls or sheets of laminates, optically variable feature devices);

— Secure transport vehicles for movement of blank documents and other principal document components (if applicable);

— Details of all lost and stolen travel document blanks to be rapidly circulated between governments and to border control authorities with details sent to the Interpol lost

and stolen database;

— Appropriate controls to be in place to protect the production procedures from internal fraud;

— Security vetting of staff.

Additional measure

— CCTV coverage/recording of all production areas, where permitted

— Centralized storage and personalisation of blank documents in as few locations as possible.

6. Glossary of terms

The glossary of terms in this document is included to assist the reader with understanding the general meanings of such terms within the context of this document.

Anti-scan pattern. An image usually constructed of fine lines at varying angular displacement and embedded in the security background design. When viewed normally, the image cannot be distinguished from the remainder of the background security print, but when the original is scanned of photocopied the embedded image becomes visible.

Biometric characteristic. A measurable, physical characteristic or personal behavioural trait used to recognize the identity, or verify the claimed identity of an enrollee.

Biographical data (biodata). The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book, or on the chip if present.

Chemical sensitizers. Security reagents to guard against tampering by chemical erasure, such that irreversible colours develop when bleach and solvents come into contact with the document.

Collation marks. See index marks.

Contactless integrated circuit. An electronic microchip coupled to an aerial (antenna) which allows data to be communicated between the chip and an encoding/reading device without the need for a direct electrical connection.

Counterfeit. An unauthorized copy or reproduction of a genuine security document made by whatever means.

Data Page. The page of the passport book, preferably the second or penultimate page, which contains the biographical data of the document holder. See “biographical data”.

Document blanks. A document blank is a travel document that does not contain personalized data. Typically, document blanks are the base stock from which personalized travel documents are created.

Digital signature. A method of securing and validating information by electronic means. This is NOT the displayed signature of the passport holder in digital form.

Digitized Photo. For purposes of this Appendix, the term "digitized photo" means that the image of the bearer is integrated directly into the substrate of the data page of the passport using a digital or equivalent personalization process. The image is then an integral aspect of the material to which it is

incorporated. This definition excludes, therefore, any photo image that is affixed, glued-in or otherwise added as a separate component of the data page itself.

Displayed signature. The original written signature or the digitally printed reproduction of the original.

DOVID. Features including diffraction structures with high resolution, also called diffractive optically variable image device.

Duplex security pattern. A design made up of an interlocking pattern of small irregular shapes, printed in two or more colours and requiring very close register printing in order to preserve the integrity of the image.

Embedded image. See Steganography.

ePassport. A Machine Readable Passport (MRP) containing a contactless integrated circuit (IC) chip, and marked by the ePassport symbol.

Fibres. Small, thread-like particles embedded in a substrate during manufacture.

Fluorescent ink. Ink containing material that glows when exposed to light at a specific wavelength, usually UV.

Forgery. Fraudulent alteration of any part of the genuine document.

Front-to-back (see-through) register. A design printed on both sides of an inner page of the document which, when the page is viewed by transmitted light, forms an interlocking image.

Global interoperability. The capability of inspection systems (either manual or automated) in different States throughout the world to obtain and 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 ePassports.

Guilloche design. A pattern of continuous fine lines, usually computer generated, and forming a unique image that can only be accurately re-originated by access to the equipment, software and parameters used in creating the original design.

Heat-sealed laminate. A laminate designed to be bonded to the biographical data page of a passport book by the application of heat and pressure.

Impostor. A person who applies for and obtains a document by assuming a false identity, or a person who alters his[3] physical appearance to represent himself as another person for the purpose of using that person's document.

Index marks. These marks are printed on the outside edge of each page in consecutive order starting from the top on the first page to a lower position on the following page and so on. The register mark of the last page appears at the bottom. This printing method leads to the appearance of a continuous stripe on the edge of the passport. Any page that has been removed will register as a gap. When printed in UV colour, this stripe becomes visible only under UV light. Also called collation marks.

[3]. Throughout this Appendix, the use of the male gender should be understood to include male and female persons.

Infrared drop-out ink. An ink which forms a visible image when illuminated with light in the visible part of the spectrum and which cannot be detected in the infrared region.

Infrared ink. An ink which is visible in the infrared light spectrum.

Intaglio. A printing process used in the production of security documents in which high printing pressure and special inks are used to create a relief image with tactile feel on the surface of the document.

Iris printing. See rainbow printing.

Label. A self-adhesive sticker which is used as the data page within the passport. This is not a generally recommended practice, particularly for longer-term validity documents.

Laminate. A clear material, which may have security features such as optically variable properties, designed to be securely bonded to protect the biographical data or other page of the document.

Laser engraving. A process whereby personalized data are "burned" into the substrate with a laser. The data may consist of text, portraits and other security features.

Laser perforation. A process whereby numbers, letters or images are created by perforating the substrate with a laser.

Latent image. A hidden image formed within a relief image which is composed of line structures which vary in direction and profile resulting in the hidden image appearing at predetermined viewing angles, achieved by intaglio printing.

Lenticular Image. A lens structure on the surface of a plastic document enables the tilted personalisation of different individual elements which appear and disappear once the document is tilted along the long or short document side.

Level 1 Inspection. Cursory examination for rapid inspection at the point of usage (easily identifiable visual or tactile features)

Level 2 Inspection. Examination by trained inspectors with simple equipment

Level 3 Inspection. Inspection by forensic specialists

Machine-verifiable biometric feature. A unique physical personal identification feature (e.g. facial image, fingerprint or iris) stored electronically in the chip of an ePassport.

Metallic ink. Ink exhibiting a metallic-like appearance.

Metameric inks. A pair of inks formulated to appear to be the same colour when viewed under specified conditions, normally daylight illumination, but which are a mismatch at other wavelengths.

Micro-printed text. Very small text printed in positive and/or negative form, which can only be read with the aid of a magnifying glass.

Optically variable feature (OVF). An image or feature whose appearance in colour and/or design changes dependent upon the angle of viewing or illumination. Examples are: features including diffraction structures with high resolution (diffractive optically variable image device/DOVID),

holograms, colour-shifting inks (e.g. ink with optically variable properties) and other diffractive or reflective materials.

Optional data capacity expansion technology. At the discretion of the issuing authorities, it is optional whether to use the data capacity expansion technology. If an issuing authority chooses to do so, only contactless integrated circuits conforming to Volume 2 are recognized by ICAO as globally interoperable.

Penetrating numbering ink. Ink containing a component that penetrates deep into a substrate.

Personalization. The process by which the portrait, signature and biographical data are applied to the document.

Phosphorescent ink. Ink containing a pigment that glows when exposed to light of a specific wavelength, the reactive glow remaining visible and then decaying after the light source is removed.

Photo substitution. A type of forgery in which the portrait in a document is substituted for a different one after the document has been issued.

Physical security. The range of security measures applied during production and personalization to prevent theft and unauthorized access to the process.

Plastic. See Synthetic.

Rainbow (split-fountain) printing. A technique whereby two or more colours of ink are printed simultaneously on a press to create a continuous merging of the colours similar to the effect seen in a rainbow. Also called prismatic, or iris printing.

Reactive inks. Inks that contain security reagents to guard against attempts at tampering by chemical erasure (deletion), such that a detectable reaction occurs when bleach and solvents come into contact with the document.

Relief (3-D) design (Medallion). A security background design incorporating an image generated in such a way as to create the illusion that it is embossed or debossed on the substrate surface.

Secondary image. A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means.

Security thread. A thin strip of plastic or other material embedded or partially embedded in the substrate during the paper manufacturing process. The strip may be metallized or partially de-metallized.

Sheet. The individual piece of substrate in a passport which comprises more than one passport page.

Steganography. An image or information encoded or concealed within a primary visual image.

Synthetic. A non-paper based material used for the biographical data page or cards. The term "synthetic" is used synonymously for "plastic", which encompasses materials like polycarbonate, PET and similar materials and combinations thereof.

Tactile feature. A surface feature giving a distinctive "feel" to the document.

Taggant. A not-naturally occurring substance that can be added to the physical components of a passport, and is typically a Level 3 feature, requiring special equipment for detection.

Tagged ink. Inks containing compounds that are not naturally occurring substances and which can be detected using special equipment.

UV. Ultraviolet light.

UV dull substrate. A substrate that exhibits no visibly detectable fluorescence when illuminated with UV light.

Variable laser image. A feature generated by laser engraving or laser perforation displaying changing information or images dependent upon the viewing angle.

Watermark. A custom design, typically containing tonal gradation, formed in the paper or other substrate during its manufacture, created by the displacement of materials therein, and traditionally viewable by transmitted light.

Windowed/Transparent feature. It is a security feature created by the construction of the substrate, whereby part of the substrate is removed or replaced by transparent material, which can incorporate additional security features such as lenses or tactile elements.

Table IIIA-1. Summary of security recommendations		
Elements	Basic features	Additional features
Substrate materials (5.1)		
Paper substrates (5.1.1)	– controlled UV response – two-tone watermark – chemical sensitizers – appropriate absorbency and surface characteristics	– registered watermark – different watermark on the data page and visa page – cylinder mould watermark – invisible fluorescent fibres – visible (fluorescent) fibres – security thread – taggant – laser perforated security feature
Paper or other substrate in the form of a label (5.1.2)	– controlled UV response – chemical sensitizers – invisible florescent fibres – visible (florescent) fibres – system of adhesives	– security thread – watermark – laser perforated security feature – die cut security pattern
Synthetic substrates (5.1.4)	– construction resistant to splitting – optically dull material – secure incorporation of data page – optically variable features – see 5.2 – 5.5 as appropriate	– window or transparent feature – tactile feature – laser perforated feature
Security printing (5.2)		
Background and text printing (5.2.1)	– two-colour guilloche background – rainbow printing – microprinted text – unique data page design	– intaglio printing – latent image – anti-scan pattern – duplex security pattern – relief design feature – front-to-back register feature – deliberate error – unique design on every page – tactile feature – unique font(s)

Elements	Basic features	Additional features
Inks (5.2.2)	– UV florescent ink – reactive ink	– ink with optically variable properties – metallic ink – penetrating numbering ink – metameric ink – infrared drop-out ink – infrared ink – phosphorescent ink – tagged ink – invisible ink
Numbering (5.2.3)	– numbering on all sheets – printed and/or perforated number – special typeface numbering for labels – identical technique for applying numbering and biographical data on synthetic substrates and cards	– laser perforated document number – special typeface
Personalization technique (5.4)		
Protection against photo substitution and alteration (5.4.4)	– integrated biographical data – security background merged within portrait area – reactive inks and chemical sensitizers in paper – visible security device overlapping portrait area – heat-sealed secure laminate or equivalent	– displayed signature – steganographic image – additional portrait image(s) – biometric feature as per Volume 2
Additional security measures for passport books (5.5)		
Page substitution (5.5.2)	– secure sewing technology – UV fluorescent sewing thread – unique data page design – page numbers integrated into security design – serial number on every sheet	– multi-colour sewing thread – programmable sewing pattern – UV cured glue to stitching – index marks on every page – laser perforated security feature – biographical data on inside page

Elements	Basic features	Additional features
Security control of production and product (5.7)		
Protection against theft and abuse (5.7.1)	– good physical security – full audit trail – serial numbers on blank documents as applicable – tracking and control numbers of components as applicable – secure transport of blank documents – international information exchange on lost and stolen documents – internal fraud protection procedures – security vetting of staff	– CCTV in production areas – centralized storage and personalization

Notes. ---

1. Issuing States and Organizations are recommended to include all of the basic features and to select from the additional features those that are best suited to their particular documents and issuing systems after conducting an assessment of the risks to which their documents are most susceptible. The list of additional features is not exhaustive and Issuing States and Organizations are encouraged to adopt other security features not explicitly mentioned in this Appendix.

2. The descriptions in the table above are necessarily abbreviated from the main text. For ease of reference, the relevant sections of this Appendix are referenced by the paragraph numbers in parentheses in the "Elements" column of the above table.

3. Certain of the features are repeated one or more times in the table. This indicates that the particular feature protects against more than one type of threat. It is only necessary to include these features once within any particular document.

4. There are many other factors associated with passport security than are elaborated here. Appendices 2 and 3 provide additional guidance. Therefore, Appendices 1,2, and 3 need to be considered collectively to ensure document issuance integrity.

5. *Any reference, direct or implied, to specific terms and/or technologies are solely intended to capture the terms and technologies in their generic form and do not have any association with specific vendors or technology providers.*

Appendix F Active Authentication with ECDSA

F.1. Present specification

ICAO Doc 9303 part 1 and 3, Volume 2, specifies in section IV, paragraph 8.1 with respect to Active Authentication that "For signature generation in the Active Authentication mechanism, States SHALL use ISO/IEC 9796-2 Digital Signature scheme 1 (ISO/IEC 9796-2, Information Technology — Security Techniques — Digital Signature Schemes giving message recovery — Part 2: Integer factorisation based mechanisms, 2002.)"

Doc9303 specifies in section IV, paragraph 8.4 with respect to the use of ECDSA that "Those States implementing the ECDSA algorithm for signature generation or verification SHALL use X 9.62 (X9.62, "Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", 7 January 1999).

ISO/IEC 9796 specifies that the hash value is incorporated in the signature format. X9.62 specifies that the hash value itself must be used as input for the signature algorithm. This is confusing, use of ECDSA conforming to X9.62 would violate the requirement in paragraph 8.1.

To prevent different implementations caused by this confusion the Supplement to Doc9303 Release 7 recommends the use of RSA for AA and not ECDSA.

The specification in this chapter provides a specification of the use of ECDSA in Active authentication, in which a choice is made between the alternative ways for implementation.

F.2. Revised specification

There are three issues that need clarification or additional specification:

- The signature type returned by AA.
- Way to specify the HASH algorithm used.
- When HASH algorithm output is longer than the length of the ECDSA key, there are different ways to form the result.

F.2.1. The signature type returned by AA

X9.62 and ISO/IEC 9796 propose different methods.
Within these ICAO specifications a **plain signature (r||s)** SHALL be returned by the eMRTD for AA when using ECDSA. With respect to the length of **r** and **s** please refer to BSI TR 03111, par 5.2.1. Only prime curves with uncompressed points SHALL be used.

Justification
plain signature (r||s) is

- recommended in TR-03111
- also used with EAC specified by EU
- already implemented on various products

F.2.2. Way to specify the HASH algorithm used

Following the current specification one can only specify in DG15 whether RSA or ECDSA is used. This can be done in the OID field of SubjectPublicKeyInfo, using the OIDs defined in RFC 3279. For RSA the used HASH algorithm is defined within the signature, in accordance to the signature generation scheme of ISO/IEC 9796-2. In case ECDSA is used there is no possibility to include any supplementary information within the signature itself.

The ASN.1 data structure `SecurityInfos` SHALL be provided by the MRTD chip in DG14 to indicate supported security protocols. Specification of the selected HASH algorithm MUST be incorporated into `SecurityInfos` in DG14. The `SecurityInfos` data structure is specified as follows:

```
SecurityInfos ::= SET of SecurityInfo

SecurityInfo ::= SEQUENCE {
      protocol OBJECT IDENTIFIER,
      requiredData ANY DEFINED BY protocol,
      optionalData ANY DEFINED BY protocol OPTIONAL
}
```

The elements contained in a SecurityInfo data structure have the following meaning:

- The object identifier protocol identifies the supported protocol.
- The open type requiredData contains protocol specific mandatory data.
- The open type optionalData contains protocol specific optional data.

If ECDSA based signature algorithm is used for Active Authentication by the MRTD chip, the SecurityInfos MUST contain following SecurityInfo entry:

```
ActiveAuthenticationInfo ::= SEQUENCE {
      protocol id-AA,
      version INTEGER  -- MUST be 1
      signatureAlgorithm OBJECT IDENTIFIER
}
```

The object identifier for Active Authentication (id-AA) is defined as:
`2.23.136.1.1.X = joint-iso-itu-t(2) international-organizations(23) icao(136) mrtd(1) security(1) AAProtocolObject(5)`

The object identifiers for `signatureAlgorithm` are defined in chapter 5.2.1 “Plain Format” of TR-03111.

NOTE: SecurityInfos MAY contain entries to other protocols than Active Authentication (like Basic Access Control, Chip Authentication, Terminal Authentication).

Justification
Using security info in DG14 allows the eMRTD to specify the exact algorithm without requiring changes to the DG15 structure which would introduce potential compatibility issues.
Implicit algorithm selection is not recommended due to being vague and prone to misinterpretations.

F.2.3. HASH calculation output versus ECDSA key length

Because of calculating hash value from the message to be signed is part of ECDSA signature process, using a HASH algorithm that gives a longer result than the length of used ECDSA key, will force part of the HASH value to be discarded.
Therefore a HASH algorithm, whose output length is of the same length or shorter than the length of the ECDSA key in use, SHALL be used with AA.

Appendix G PACE V2 Worked Examples

G.1. Generic Mapping

This paragraph provides two worked examples for the PACE protocol as defined in the Technical Report SAC using the generic mapping. The first example is based on ECDH while the second one uses DH. All numbers contained in the tables are noted hexadecimal. The notation follows the Technical Report SAC.
The PACE protocol is organized as follows. It starts with the initialization by MSE:AT. Then follows a chain of General Authenticate commands as shown below (for a detailed description see the Technical Report SAC).

1. Encrypted Nonce
2. Map Nonce
3. Perform Key Agreement
4. Mutual Authentication

In both examples, the MRZ is used as password. This also leads to the same symmetric key $K_{\pi.}$ The relevant data fields of the MRZ including the check digits are

- Serial Number: T220001293
- Date of Birth: 6408125
- Date of Expiry: 1010318.

Hence, the encoding K of the MRZ and the derived encryption key K_π are

K	7E2D2A41 C74EA0B3 8CD36F86 3939BFA8 E9032AAD
K_π	89DED1B2 6624EC1E 634C1989 302849DD

1. ECDH-based Example

This example is based on ECDH applying the standardized BrainpoolP256r1 domain parameters (see RFC 5639).
The first section introduces the corresponding `PACEInfo`. Subsequently, the exchanged APDU's including all generated nonces and ephemeral keys are listed and examined.

1.1 Elliptic Curve Parameters

Using standardized domain parameters, all informations required to perform PACE are given by the data structure `PACEInfo`. In particular, no `PACEDomainParameterInfo` is needed.

`PACEInfo`	3012060A 04007F00 07020204 02020201 0202010D

The detailed structure of `PACEInfo` is itemized in the following table.

Tag	***Length***	***Value***	***ASN.1 Type***	***Comment***
30	12		SEQUENCE	PACEInfo

06	0A	04 00 7F 00 07 02 02 04 02 02	OBJECT IDENTIFIER	PACE with ECDH, generic mapping and AES 128 session keys
02	01	02	INTEGER	Version 2
02	01	0D	INTEGER	Brainpool P256r1 Standardized Domain Parameters

For convenience, an ASN.1 encoding of the BrainpoolP256r1domain parameters is given below.

Tag	***Length***	***Value***	***ASN.1 Type***	***Comment***
30	81 EC		SEQUENCE	Domain parameter
06	0A	2A 86 48 CE 3D 02 01	OBJECT IDENTIFIER	Algorithm id-ecPublicKey
30	81 E0		SEQUENCE	Domain Parameter
02	01	01	INTEGER	Version
30	2C		SEQUENCE	Underlying field
06	07	2A 86 48 CE 3D 01 01	OBJECT IDENTIFIER	Prime field
02	21	00 A9 FB 57 DB A1 EE A9 BC 3E 66 0A 90 9D 83 8D 72 6E 3B F6 23 D5 26 20 28 20 13 48 1D 1F 6E 53 77	INTEGER	Prime p
30	44		SEQUENCE	Curve equation
04	20	7D 5A 09 75 FC 2C 30 57 EE F6 75 30 41 7A FF E7 FB 80 55 C1 26 DC 5C 6C E9 4A 4B 44 F3 30 B5 D9	OCTET STRING	Parameter a
04	20	26 DC 5C 6C E9 4A 4B 44 F3 30 B5 D9 BB D7 7C BF 95 84 16 29 5C F7 E1 CE 6B CC DC 18 FF 8C 07 B6	OCTET STRING	Parameter b
04	41		OCTET STRING	Group generator G
		04	-	Uncompressed point
		8B D2 AE B9 CB 7E 57 CB 2C 4B 48 2F FC 81 B7 AF B9 DE 27 E1 E3 BD 23 C2 3A 44 53 BD 9A CE 32 62	-	x-coordinate
		54 7E F8 35 C3 DA C4 FD 97 F8 46 1A 14 61 1D C9	-	y-coordinate

		C2 77 45 13 2D ED 8E 54 5C 1D 54 C7 2F 04 69 97			
02	21	00 A9 FB 57 DB A1 EE A9 BC 3E 66 0A 90 9D 83 8D 71 8C 39 7A A3 B5 61 A6 F7 90 1E 0E 82 97 48 56 A7	INTEGER		Group order n
02	01	01	INTEGER		Cofactor f

1.2 Application flow of the ECDH-based example

To initialize PACE, the terminal sends the command MSE:AT to the chip.

T>C :	00 22 C1 A4 0F 80 0A 04 00 7F 00 07 02 02 04 02 02 83 01 01
C>T :	90 00

Here, T>C is an abbreviation for an APDU sent from terminal to chip while C>T denotes the corresponding response sent by the chip to the terminal. The encoding of the command is explained in the next table.

Command				
CLA	00		Plain	
INS	22		Manage security environment	
P1/P2	C1 A4		Set Authentication Template for mutual authentication	
L_c	0F		Length of data field	
Data	Tag	Length	Value	Comment
	80	0A	04 00 7F 00 07 02 02 04 02 02	Cryptographic mechanism: PACE with ECDH, generic mapping and AES128 session keys
	83	01	01	Password: MRZ
Response				
Status Bytes	90 00		Normal operation	

1.2.1 Encrypted Nonce

Next, the chip randomly generates the nonce s and encrypts it by means of K_π.

Decrypted Nonce s	3F00C4D3 9D153F2B 2A214A07 8D899B22

Encrypted Nonce z	95A3A016 522EE98D 01E76CB6 B98B42C3

The encrypted nonce is queried by the terminal.

T>C :	10 86 00 00 02 7C 00 00
C>T :	7C 12 80 10 95 A3 A0 16 52 2E E9 8D 01 E7 6C B6 B9 8B 42 C3 90 00

The encoding of the command APDU and the corresponding response can be found in the following table.

Command				
CLA	10		Command chaining	
INS	86		General Authenticate	
P1/P2	00 00		Keys and protocol implicitly known	
L_c	02		Length of data	
Data	Tag	Length	Value	Comment
	7C	00	-	Absent
L_e	00		Expected maximal byte length of the response data field is 256	
Response				
Data	Tag	Length	Value	Comment
	7C	12		Dynamic Authentication Data
	80	10	95 A3 A0 16 52 2E E9 8D 01 E7 6C B6 B9 8B 42 C3	Encrypted Nonce
Status Bytes	90 00		Normal operation	

1.2.2 Map Nonce

The nonce is mapped to an ephemeral group generator via generic mapping. The required randomly chosen ephemeral keys are also collected in the next table.

Terminal's Priva	7F4EF07B 9EA82FD7 8AD689B3 8D0BC78C F21F249D 953BC46F 4C6E1925 9C010F99
Terminal's Public Key	7ACF3EFC 982EC455 65A4B155 129EFBC7 4650DCBF A6362D89 6FC70262 E0C2CC5E, 544552DC B6725218 799115B5 5C9BAA6D

	9F6BC3A9 618E70C2 5AF71777 A9C4922D
Chip's Private Key	498FF497 56F2DC15 87840041 839A8598 2BE7761D 14715FB0 91EFA7BC E9058560
Chip's Public Key	824FBA91 C9CBE26B EF53A0EB E7342A3B F178CEA9 F45DE0B7 0AA60165 1FBA3F57, 30D8C879 AAA9C9F7 3991E61B 58F4D52E B87A0A0C 709A49DC 63719363 CCD13C54
Shared secret H	60332EF2 450B5D24 7EF6D386 8397D398 852ED6E8 CAF6FFEE F6BF85CA 57057FD5, 0840CA74 15BAF3E4 3BD414D3 5AA4608B 93A2CAF3 A4E3EA4E 82C9C13D 03EB7181
Mapped generator $\tilde{G}$	8CED63C9 1426D4F0 EB1435E7 CB1D74A4 6723A0AF 21C89634 F65A9AE8 7A9265E2, 8C879506 743F8611 AC33645C 5B985C80 B5F09A0B 83407C1B 6A4D857A E76FE522

The following APDU's are exchanged by terminal and chip to map the nonce.

T>C :	10 86 00 00 45 7C 43 81 41 04 7A CF 3E FC 98 2E C4 55 65 A4 B1 55 12 9E FB C7 46 50 DC BF A6 36 2D 89 6F C7 02 62 E0 C2 CC 5E 54 45 52 DC B6 72 52 18 79 91 15 B5 5C 9B AA 6D 9F 6B C3 A9 61 8E 70 C2 5A F7 17 77 A9 C4 92 2D 00
C>T :	7C 43 82 41 04 82 4F BA 91 C9 CB E2 6B EF 53 A0 EB E7 34 2A 3B F1 78 CE A9 F4 5D E0 B7 0A A6 01 65 1F BA 3F 57 30 D8 C8 79 AA A9 C9 F7 39 91 E6 1B 58 F4 D5 2E B8 7A 0A 0C 70 9A 49 DC 63 71 93 63 CC D1 3C 54 90 00

The structure of the ADPU's can be described as follows:

Command				
CLA	10		Command chaining	
INS	86		General Authenticate	
P1/P2	00 00		Keys and protocol implicitly known	
L_c	45		Length of data	
Data	Tag	Length	Value	Comment
	7C	43	-	Dynamic Authentication Data
	81	41		Mapping Data
			04	Uncompressed Point

			7A CF 3E FC 98 2E ... C2 CC 5E	x-coordinate
			54 45 52 DC B6 72 ... C4 92 2D	y-coordinate
L_e	00		Expected maximal byte length of the response data field is 256	
Response				
Data	Tag	Length	Value	Comment
	7C	43		Dynamic Authentication Data
	82	41		Mapping Data
			04	Uncompressed Point
			82 4F BA 91 C9 CB ... BA 3F 57	x-coordinate
			30 D8 C8 79 AA A9 ... D1 3C 54	y-coordinate
Status Bytes	90 00		Normal operation	

1.2.3 Perform Key Agreement

In the third step, chip and terminal perform an anonymous ECDH key agreement using the new domain parameters determined by the ephemeral group generator $\tilde{G}$ of the previous step. According to the Technical Report SAC, only the x-coordinate is required as shared secret since the KDF only uses the first coordinate to derive the session keys.

Terminal's Private Key	A73FB703 AC1436A1 8E0CFA5A BB3F7BEC 7A070E7A 6788486B EE230C4A 22762595
Terminal's Public Key	2DB7A64C 0355044E C9DF1905 14C625CB A2CEA487 54887122 F3A5EF0D 5EDD301C, 3556F3B3 B186DF10 B857B58F 6A7EB80F 20BA5DC7 BE1D43D9 BF850149 FBB36462
Chip's Private Key	107CF586 96EF6155 053340FD 633392BA 81909DF7 B9706F22 6F32086C 7AFF974A
Chip's Public Key	9E880F84 2905B8B3 181F7AF7 CAA9F0EF B743847F 44A306D2 D28C1D9E C65DF6DB, 7764B222 77A2EDDC 3C265A9F 018F9CB8 52E111B7 68B32690 4B59A019 3776F094
Shared Secret	28768D20 701247DA E81804C9 E780EDE5

	82A9996D B4A31502 0B273319 7DB84925

The key agreement is performed as follows:

T>C :	10 86 00 00 45 7C 43 83 41 04 2D B7 A6 4C 03 55 04 4E C9 DF 19 05 14 C6 25 CB A2 CE A4 87 54 88 71 22 F3 A5 EF 0D 5E DD 30 1C 35 56 F3 B3 B1 86 DF 10 B8 57 B5 8F 6A 7E B8 0F 20 BA 5D C7 BE 1D 43 D9 BF 85 01 49 FB B3 64 62 00
C>T :	7C 43 84 41 04 9E 88 0F 84 29 05 B8 B3 18 1F 7A F7 CA A9 F0 EF B7 43 84 7F 44 A3 06 D2 D2 8C 1D 9E C6 5D F6 DB 77 64 B2 22 77 A2 ED DC 3C 26 5A 9F 01 8F 9C B8 52 E1 11 B7 68 B3 26 90 4B 59 A0 19 37 76 F0 94 90 00

The encoding of the key agreement is examined in the following table.

Command				
CLA	10		Command chaining	
INS	86		General Authenticate	
P1/P2	00 00		Keys and protocol implicitly known	
L_c	45		Length of data	
Data	Tag	Length	Value	Comment
	7C	43	-	Dynamic Authentication Data
	83	41		Terminal's Ephemeral Public Key
			04	Uncompressed Point
			2D B7 A6 4C 03 55 ... DD 30 1C	x-coordinate
			35 56 F3 B3 B1 86 ... B3 64 62	y-coordinate
L_e	00		Expected maximal byte length of the response data field is 256	
Response				
Data	Tag	Length	Value	Comment
	7C	43		Dynamic Authentication Data
	84	41		Chip's Ephemeral Public Key
			04	Uncompressed Point
			9E 88 0F 84 29 05 ... 5D F6 DB	x-coordinate

			77 64 B2 22 77 A2 ... 76 F0 94	y-coordinate
Status Bytes	90 00		Normal operation	

By means of the KDF specified in the Technical Report SAC, the AES 128 session keys K_{Enc} and K_{MAC} are derived from the shared secret. These are

K_{Enc}	F5F0E35C 0D7161EE 6724EE51 3A0D9A7F
K_{MAC}	FE251C78 58B356B2 4514B3BD 5F4297D1

1.2.4 Mutual Authentication

The authentication tokens are derived by means of K_{MAC} using

Input Data for T_{PCD}	7F494F06 0A04007F 00070202 04020286 41049E88 0F842905 B8B3181F 7AF7CAA9 F0EFB743 847F44A3 06D2D28C 1D9EC65D F6DB7764 B22277A2 EDDC3C26 5A9F018F 9CB852E1 11B768B3 26904B59 A0193776 F094
Input Data for T_{PICC}	7F494F06 0A04007F 00070202 04020286 41042DB7 A64C0355 044EC9DF 190514C6 25CBA2CE A4875488 7122F3A5 EF0D5EDD 301C3556 F3B3B186 DF10B857 B58F6A7E B80F20BA 5DC7BE1D 43D9BF85 0149FBB3 6462

as input. The encoding of the input data is shown below

Tag	***Length***	***Value***	***ASN.1 Type***	***Comment***
7F49	4F		PUBLIC KEY	Input data for T_{PCD}
06	0A	04 00 7F 00 07 02 02 04 02 02	OBJECT IDENTIFIER	PACE with ECDH, generic mapping and AES 128 session keys
86	41		ELLIPTIC CURVE POINT	Chip's Ephemeral Public Point
		04		Uncompressed Point
		9E 88 0F 84 29 ... 5D F6 DB		x-coordinate
		77 64 B2 22 77 ... 76 F0 94		y-coordinate

Tag	*Length*	*Value*	*ASN.1 Type*	*Comment*
7F49	4F		PUBLIC KEY	Input data for T_{PICC}
06	0A	04 00 7F 00 07 02 02 04 02 02	OBJECT IDENTIFIER	PACE with ECDH, generic mapping and AES 128 session keys
86	41		ELLIPTIC CURVE POINT	Terminal's Ephemeral Public Point
		04		Uncompressed Point
		2D B7 A6 4C 03 ... DD 30 1C		x-coordinate
		35 56 F3 B3 B1 ... B3 64 62		y-coordinate

The computed authentication tokens are

T_{PCD}	C2B0BD78 D94BA866
T_{PICC}	3ABB9674 BCE93C08

Finally, these tokens are exchanged and verified.

T>C :	00 86 00 00 0C 7C 0A 85 08 C2 B0 BD 78 D9 4B A8 66 00
C>T :	7C 0A 86 08 3A BB 96 74 BC E9 3C 08 90 00

2. DH-based Example

The second example is based on DH using the 1024-bit MODP Group with 160-bit Prime Order Subgroup specified by RFC 5114. The example is taken from the EAC 2 worked example (BSI 2010), making minor modifications. The parameters of the group are

Prime *p*	B10B8F96 A080E01D DE92DE5E AE5D54EC 52C99FBC FB06A3C6 9A6A9DCA 52D23B61 6073E286 75A23D18 9838EF1E 2EE652C0 13ECB4AE A9061123 24975C3C D49B83BF ACCBDD7D 90C4BD70 98488E9C 219A7372 4EFFD6FA E5644738 FAA31A4F F55BCCC0 A151AF5F 0DC8B4BD 45BF37DF 365C1A65 E68CFDA7 6D4DA708 DF1FB2BC 2E4A4371
Subgroup Generator *g*	A4D1CBD5 C3FD3412 6765A442 EFB99905 F8104DD2 58AC507F D6406CFF 14266D31 266FEA1E 5C41564B 777E690F 5504F213

	160217B4 B01B886A 5E91547F 9E2749F4 D7FBD7D3 B9A92EE1 909D0D22 63F80A76 A6A24C08 7A091F53 1DBF0A01 69B6A28A D662A4D1 8E73AFA3 2D779D59 18D08BC8 858F4DCE F97C2A24 855E6EEB 22B3B2E5
Prime Order *q* of *g*	F518AA87 81A8DF27 8ABA4E7D 64B7CB9D 49462353

The first section introduces the PACEInfo. Subsequently, the exchanged APDU's including all generated nonces and ephemeral keys are listed and examined

2.1 Diffie Hellman Parameters

The relevant information for PACE is given by the data structure PACEInfo.

PACEInfo	3012060A 04007F00 07020204 01020201 02020100

The detailed structure of PACEInfo is

Tag	***Length***	***Value***	***ASN.1 Type***	***Comment***
30	12		SEQUENCE	PACEInfo
06	0A	04 00 7F 00 07 02 02 04 01 02	OBJECT IDENTIFIER	OID: PACE with DH, generic mapping and AES 128 session keys
02	01	02	INTEGER	Version 2
02	01	00	INTEGER	Standardized 1024-bit Group specified by RFC 5114

2.2 Application flow of the DH-based example

To initialize PACE, the terminal sends the command MSE:AT to the chip.

T>C :	*00 22 C1 A4 0F 80 0A 04 00 7F 00 07 02 02 04 01 02 83 01 01*
C>T :	90 00

The encoding of the command is described in the next table.

Command		
CLA	00	Plain
INS	22	Manage security environment
P1/P2	C1 A4	Set Authentication Template for mutual authentication

L_c	0F		Length of data field	
Data	Tag	Length	Value	Comment
	80	0A	04 00 7F 00 07 02 02 04 01 02	OID: Cryptographic mechanism: PACE with DH, generic mapping and AES128
	83	01	01	Password: MRZ
Response				
Status Bytes	90 00		Normal operation	

2.2.1 Encrypted Nonce

Next, the terminal queries a nonce from the chip.

Decrypted Nonce s	FA5B7E3E 49753A0D B9178B7B 9BD898C8
Encrypted Nonce z	854D8DF5 827FA685 2D1A4FA7 01CDDDCA

The communication looks as follows.

T>C :	10 86 00 00 02 7C 00 00
C>T :	7C 12 80 10 85 4D 8D F5 82 7F A6 85 2D 1A 4F A7 01 CD DD CA 90 00

The encoding of the command APDU and the corresponding response is described in the following table.

Command				
CLA	10		Command chaining	
INS	86		General Authenticate	
P1/P2	00 00		Keys and protocol implicitly known	
L_c	02		Length of data	
Data	Tag	Length	Value	Comment
	7C	00	-	Absent
L_e	00		Expected maximal byte length of the response data field is 256	
Response				
Data	Tag	Length	Value	Comment
	7C	12		Dynamic Authentication Data

	80	10	85 4D 8D F5 82 7F A6 85 2D 1A 4F A7 01 CD DD CA	Encrypted Nonce
Status Bytes	90 00		Normal operation	

2.2.2 Map Nonce

By means of the generic mapping, the nonce is mapped to an ephemeral group generator. For that purpose, the following ephemeral keys are randomly generated by terminal and chip.

Terminal's Private Key	24C3C0E0 A3280ECB 943345D9 DC2A7B72 539FDA6F FDF99AB7 B6CDDDD1 BE425AF3 D02C4ED0 CDD73EBB 4B2EDF8C 07FB3A35 903F72B8 4F3771F4 EBFB4952 0D61A8F7 C7FB8C9E 2ABC24BF 4FF9D8DD F381A193 80C85B62 3AB02ACB F6D220F5 12BF4065 8322AD20 9AC0BF9E 6F8DB602 D5197D25 2BF6D148 510CA1B7 40AF0F99 F33CA5F1
Terminal's Public Key	23FB3749 EA030D2A 25B278D2 A562047A DE3F01B7 4F17A154 02CB7352 CA7D2B3E B71C343D B13D1DEB CE9A3666 DBCFC920 B49174A6 02CB4796 5CAA73DC 702489A4 4D41DB91 4DE9613D C5E98C94 160551C0 DF86274B 9359BC04 90D01B03 AD54022D CB4F57FA D6322497 D7A1E28D 46710F46 1AFE710F BBBC5F8B A166F431 1975EC6C
Chip's Private Key	4EC025E4 0C6D10B2 AAF6FCAC 98C4244F 57481A49 61F3ADC3 72A95E40 E0CC3555 F73CCFC6 5E9DB956 DD61B143 E0C7DC51 9E7DD8ED D8E3E46A 094CF226 4FD193D0 BC4BC05C DE6CA443 19C2439F D04A4644 3C8D0494 487F6F2F E9AC8BE9 B9EE16A3 D242668C BA4FFD42 EEAC3650 9E16B4D1 E6E8EE00 25FF8244 B190F57D 441EC328
Chip's Public Key	78879F57 225AA808 0D52ED0F C890A4B2 5336F699 AA89A2D3 A189654A F70729E6 23EA5738 B26381E4 DA19E004 706FACE7 B235C2DB F2F38748 312F3C98 C2DD4882 A41947B3 24AA1259 AC22579D B93F7085 655AF308 89DBB845 D9E6783F E42C9F24 49400306 254C8AE8 EE9DD812 A804C0B6 6E8CAFC1 4F84D825 8950A91B 44126EE6
Shared secret H	5BABEBEF 5B74E5BA 94B5C063 FDA15F1F 1CDE9487 3EE0A5D3 A2FCAB49 F258D07F 544F13CB 66658C3A FEE9E727 389BE3F6 CBBBD321 28A8C21D D6EEA3CF 7091CDDF B08B8D00 7D40318D CCA4FFBF 51208790 FB4BD111 E5A968ED 6B6F08B2 6CA87C41 0B3CE0C3 10CE104E ABD16629 AA48620C 1279270C B0750C0D 37C57FFF E302AE7F

Mapped generator $\tilde{g}$	7C9CBFE9 8F9FBDDA 8D143506 FA7D9306 F4CB17E3 C71707AF F5E1C1A1 23702496 84D64EE3 7AF44B8D BD9D45BF 6023919C BAA027AB 97ACC771 666C8E98 FF483301 BFA4872D EDE9034E DFACB708 14166B7F 36067682 9B826BEA 57291B5A D69FBC84 EF1E7790 32A30580 3F743417 93E86974 2D401325 B37EE856 5FFCDEE6 18342DC5

The following APDU's are exchanged by terminal and chip to map the nonce.

T>C :	10 86 00 00 86 7C 81 83 81 81 80 23 FB 37 49 EA 03 0D 2A 25 B2 78 D2 A5 62 04 7A DE 3F 01 B7 4F 17 A1 54 02 CB 73 52 CA 7D 2B 3E B7 1C 34 3D B1 3D 1D EB CE 9A 36 66 DB CF C9 20 B4 91 74 A6 02 CB 47 96 5C AA 73 DC 70 24 89 A4 4D 41 DB 91 4D E9 61 3D C5 E9 8C 94 16 05 51 C0 DF 86 27 4B 93 59 BC 04 90 D0 1B 03 AD 54 02 2D CB 4F 57 FA D6 32 24 97 D7 A1 E2 8D 46 71 0F 46 1A FE 71 0F BB BC 5F 8B A1 66 F4 31 19 75 EC 6C 00
C>T :	7C 81 83 82 81 80 78 87 9F 57 22 5A A8 08 0D 52 ED 0F C8 90 A4 B2 53 36 F6 99 AA 89 A2 D3 A1 89 65 4A F7 07 29 E6 23 EA 57 38 B2 63 81 E4 DA 1 9E0 04 70 6F AC E7 B2 35 C2 DB F2 F3 87 48 31 2F 3C 98 C2 DD 48 82 A4 19 47 B3 24 AA 12 59 AC 22 57 9D B9 3F 70 85 65 5A F3 08 89 DB B8 45 D9 E6 78 3F E4 2C 9F 24 49 40 03 06 25 4C 8A E8 EE 9D D8 12 A8 04 C0 B6 6E 8C AF C1 4F 84 D8 25 89 50 A9 1B 44 12 6E E6 90 00

The structure of the ADPU's can be described as follows:

Command				
CLA	10		Command chaining	
INS	86		General Authenticate	
P1/P2	00 00		Keys and protocol implicitly known	
L_c	86		Length of data	
Data	Tag	Length	Value	Comment
	7C	81 83	-	Dynamic Authentication Data
	81	81 80	23 FB 37 49 EA 03 ... 75 EC 6C	Mapping Data
L_e	00		Expected maximal byte length of the response data field is 256	
Response				
Data	Tag	Length	Value	Comment
	7C	81 83		Dynamic Authentication Data
	82	81 80	ED 0F C8 90 A4 B2 ... 12 6E E6	Mapping Data
Status Bytes	90 00		Normal operation	

2.2.3 Perform Key Agreement

Subsequently, chip and terminal perform an anonymous DH key agreement using the new domain parameters determined by the ephemeral group generator $\tilde{g}$ of the previous step.

Terminal's Private Key	4BD0E547 40F9A028 E6A515BF DAF96784 8C4F5F5F FF65AA09 15947FFD 1A0DF2FA 6981271B C905F355 1457B7E0 3AC3B806 6DE4AA40 6C1171FB 43DD939C 4BA16175 103BA3DE E16419AA 248118F9 0CC36A3D 6F4C3736 52E0C3CC E7F0F1D0 C5425B36 00F0F0D6 A67F004C 8BBA33F2 B4733C72 52445C1D FC4F1107 203F71D2 EFB28161
Terminal's Public Key	00907D89 E2D425A1 78AA81AF 4A7774EC 8E388C11 5CAE6703 1E85EECE 520BD911 551B9AE4 D04369F2 9A02626C 86FBC674 7CC7BC35 2645B616 1A2A42D4 4EDA80A0 8FA8D61B 76D3A154 AD8A5A51 786B0BC0 71470578 71A92221 2C5F67F4 31731722 36B7747D 1671E6D6 92A3C7D4 0A0C3C5C E397545D 015C175E B5130551 EDBC2EE5 D4
Chip's Private Key	020F018C 7284B047 FA7721A3 37EFB7AC B1440BB3 0C5252BD 41C97C30 C994BB78 E9F0C5B3 2744D840 17D21FFA 6878396A 6469CA28 3EF5C000 DAF7D261 A39AB886 0ED4610A B5343390 897AAB5A 7787E4FA EFA0649C 6A94FDF8 2D991E8E 3FC332F5 142729E7 040A3F7D 5A4D3CD7 5CBEE1F0 43C1CAD2 DD484FEB 4ED22B59 7D36688E
Chip's Public Key	075693D9 AE941877 573E634B 6E644F8E 60AF17A0 076B8B12 3D920107 4D36152B D8B3A213 F53820C4 2ADC79AB 5D0AEEC3 AEFB9139 4DA476BD 97B9B14D 0A65C1FC 71A0E019 CB08AF55 E1F72900 5FBA7E3F A5DC4189 9238A250 767A6D46 DB974064 386CD456 743585F8 E5D90CC8 B4004B1F 6D866C79 CE0584E4 9687FF61 BC29AEA1
Shared Secret	6BABC7B3 A72BCD7E A385E4C6 2DB2625B D8613B24 149E146A 629311C4 CA6698E3 8B834B6A 9E9CD718 4BA8834A FF5043D4 36950C4C 1E783236 7C10CB8C 314D40E5 990B0DF7 013E64B4 549E2270 923D06F0 8CFF6BD3 E977DDE6 ABE4C31D 55C0FA2E 465E553E 77BDF75E 3193D383 4FC26E8E B1EE2FA1 E4FC97C1 8C3F6CFF FE2607FD

The key agreement is performed as follows:

T>C :	10 86 00 00 86 7C 81 83 83 81 80 90 7D 89 E2 D4 25 A1 78 AA 81 AF 4A 77 74 EC 8E 38 8C 11 5C AE 67 03 1E 85 EE CE 52 0B D9 11 55 1B 9A E4 D0 43 69 F2 9A 02 62 6C 86 FB C6 74 7C C7 BC 35 26 45 B6 16 1A 2A 42 D4 4E DA 80 A0 8F A8 D6 1B

	76 D3 A1 54 AD 8A 5A 51 78 6B 0B C0 71 47 05 78 71 A9 22 21 2C 5F 67 F4 31 73 17 22 36 B7 74 7D 16 71 E6 D6 92 A3 C7 D4 0A 0C 3C 5C E3 97 54 5D 01 5C 17 5E B5 13 05 51 ED BC 2E E5 D4 00
C>T :	7C 81 83 84 81 80 07 56 93 D9 AE 94 18 77 57 3E 63 4B 6E 64 4F 8E 60 AF 17 A0 07 6B 8B 12 3D 92 01 07 4D 36 15 2B D8 B3 A2 13 F5 38 20 C4 2A DC 79 AB 5D 0A EE C3 AE FB 91 39 4D A4 76 BD 97 B9 B1 4D 0A 65 C1 FC 71 A0 E0 19 CB 08 AF 55 E1 F7 29 00 5F BA 7E 3F A5 DC 41 89 92 38 A2 50 76 7A 6D 46 DB 97 40 64 38 6C D4 56 74 35 85 F8 E5 D9 0C C8 B4 00 4B 1F 6D 86 6C 79 CE 05 84 E4 96 87 FF 61 BC 29 AE A1 90 00

Command				
CLA	10		Command chaining	
INS	86		General Authenticate	
P1/P2	00 00		Keys and protocol implicitly known	
L_c	86		Length of data	
Data	Tag	Length	Value	Comment
	7C	81 83	-	Dynamic Authentication Data
	83	81 80	90 7D 89 E2 D4 25 ... 2E E5 D4	Terminal's Ephemeral Public Key
L_e	00		Expected maximal byte length of the response data field is 256	
Response				
Data	Tag	Length	Value	Comment
	7C	81 83		Dynamic Authentication Data
	84	81 80	07 56 93 D9 AE 94 ... 29 AE A1	Chip's Ephemeral Public Key
Status Bytes	90 00		Normal operation	

The AES 128 session keys K_{Enc} and K_{MAC} are derived from the shared secret using the KDF specified in the Technical Report SAC.

K_{Enc}	2F7F46AD CC9E7E52 1B45D192 FAFA9126
K_{MAC}	805A1D27 D45A5116 F73C5446 9462B7D8

2.2.4 Mutual Authentication

The authentication tokens are constructed from the following input data.

Input Data for T_{PCD}	7F49818F 060A0400 7F000702 02040102 84818007 5693D9AE 94187757 3E634B6E 644F8E60 AF17A007 6B8B123D 9201074D

	36152BD8 B3A213F5 3820C42A DC79AB5D 0AEEC3AE FB91394D A476BD97 B9B14D0A 65C1FC71 A0E019CB 08AF55E1 F729005F BA7E3FA5 DC418992 38A25076 7A6D46DB 97406438 6CD45674 3585F8E5 D90CC8B4 004B1F6D 866C79CE 0584E496 87FF61BC 29AEA1
Input Data for T_{PICC}	7F49818F 060A0400 7F000702 02040102 84818090 7D89E2D4 25A178AA 81AF4A77 74EC8E38 8C115CAE 67031E85 EECE520B D911551B 9AE4D043 69F29A02 626C86FB C6747CC7 BC352645 B6161A2A 42D44EDA 80A08FA8 D61B76D3 A154AD8A 5A51786B 0BC07147 057871A9 22212C5F 67F43173 172236B7 747D1671 E6D692A3 C7D40A0C 3C5CE397 545D015C 175EB513 0551EDBC 2EE5D4

The encoding of the input data is shown below

Tag	***Length***	***Value***	***ASN.1 Type***	***Comment***
7F49	81 8F		PUBLIC KEY	Input data for T_{PCD}
06	0A	04 00 7F 00 07 02 02 04 01 02	OBJECT IDENTIFIER	PACE with DH, generic mapping and AES 128 session keys
84	81 80	07 56 93 D9 AE ... 29 AE A1	UNSIGNED INTEGER	Chip's Ephemeral Public Key

Tag	***Length***	***Value***	***ASN.1 Type***	***Comment***
7F49	81 8F		PUBLIC KEY	Input data for T_{PICC}
06	0A	04 00 7F 00 07 02 02 04 01 02	OBJECT IDENTIFIER	PACE with DH, generic mapping and AES 128 session keys
84	81 80	90 7D 89 E2 D4 ... 2E E5 D4	UNSIGNED INTEGER	Terminal's Ephemeral Public Key

The computed authentication tokens are

T_{PCD}	B46DD9BD 4D98381F
T_{PICC}	917F37B5 C0E6D8D1

Finally, these tokens are exchanged and verified.

T>C :	00 86 00 00 0C 7C 0A 85 08 B4 6D D9 BD 4D 98 38 1F 00

C>T :	7C 1B 86 08 91 7F 37 B5 C0 E6 D8 D1 87 0F 44 45 54 45 53 54 43 56 43 41 30 30 30 30 33

Command				
CLA	00		Plain	
INS	86		General Authenticate	
P1/P2	00 00		Keys and protocol implicitly known	
L_c	0C		Length of data	
Data	Tag	Length	Value	Comment
	7C	0A	-	Dynamic Authentication Data
	85	08	B4 6D D9 BD 4D 98 38 1F	Terminal's Authentication Token
L_e	00		Expected maximal byte length of the response data field is 256	
Response				
Data	Tag	Length	Value	Comment
	7C	0A		Dynamic Authentication Data
	86	08	91 7F 37 B5 C0 E6 D8 D1	Chip's Authentication Token
Status Bytes	90 00		Normal operation	

G.2. Integrated Mapping

Introduction

This section provides two examples for the PACE protocol with Integrated Mapping, as described in [1] with the revisions of [6]. The first one is based on Elliptic Curve Diffie-Hellman (ECDH) and the second one on Diffie-Hellman (DH). The document does not detail how to obtain encryption keys from the MRZ, the key K used the key from the PACE examples of [2].

References

All the documents referenced in this specification are listed in the following document:

REFERENCE	DOCUMENT
[1]	I. J. S. WG3/TF5, "Supplemental Access Control for Machine Readable Travel

REFERENCE	DOCUMENT
	Documents, version 1.01," 2010.
[2]	B. f. S. i. d. Informationstechnik, "EAC 2 Worked Example," 2010.
[3]	M. Lochter and J. Merkle, "FRC 5639: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation," 2010.
[4]	M. Lepinski and S. Kent, "RFC 5114: Additional Diffie-Hellman Groups for Use with IETF Standards," 2008.
[5]	M. Lepinski and S. Kent, "RFC 5114: Additional Diffie-Hellman Groups for Use with IETF Standards," 2008.
[6]	I. J. S. WG3/TF1, "Supplement to Doc 9303 – Release 10" 2011.

Conventions

- **Hexadecimal Notation**

The values expressed in hexadecimal are between simple hooks (‘ ’). For example, the decimal value 27509 is noted ‘6B 75’ in hexadecimal.

- **Decimal Notation**

The decimal values are expressed in rough format. For example the hexadecimal-noted value ‘08’ is noted 8 in decimal.

- **Binary Notation**

The binary values are followed by a “b” in lower case. For example, the value 8 is noted 00001000b in binary.

- **Various Notations**

The free or not fixed values are noted ‘XX … XX’ (several bytes) or ‘XX’ (only one byte). The symbol “ || ” is used to represent the concatenation of two elements.

M/O - M for Mandatory and O for Optional.

1 ECDH-based Example

This example is based on the BrainpoolP256r1 elliptic curve, as defined in [3]. The block cipher used in this example is AES-128. For reminder, the curve parameters are the following:

Prime p	A9FB57DB A1EEA9BC 3E660A90 9D838D72 6E3BF623 D5262028 2013481D 1F6E5377
Parameter a	7D5A0975 FC2C3057 EEF67530 417AFFE7 FB8055C1 26DC5C6C E94A4B44 F330B5D9
Parameter b	26DC5C6C E94A4B44 F330B5D9 BBD77CBF 95841629 5CF7E1CE 6BCCDC18 FF8C07B6
x-coordinate of the group generator G	8BD2AEB9 CB7E57CB 2C4B482F FC81B7AF B9DE27E1 E3BD23C2 3A4453BD 9ACE3262
y-coordinate of the group generator G	547EF835 C3DAC4FD 97F8461A 14611DC9 C2774513 2DED8E54 5C1D54C7 2F046997
Group order n	A9FB57DB A1EEA9BC 3E660A90 9D838D71 8C397AA3 B561A6F7 901E0E82 974856A7
Cofactor f	01

The encryption key is the following:

K_π	591468CD A83D6521 9CCCB856 0233600F

1.1 Encrypted Nonce

A nonce s is randomly chosen by the chip and encrypted using K_π. The encrypted nonce z is then sent to the terminal.

Decrypted Nonce s	2923BE84 E16CD6AE 529049F1 F1BBE9EB
Encrypted Nonce z	143DC40C 08C8E891 FBED7DED B92B64AD

1.2 Map Nonce

A nonce t is randomly chosen and sent in clear. t and s are then used to compute the Integrated Mapping. First, the pseudo-random function R_p, derived from AES, is applied to s and t. Then, the point encoding f_G is used on the result to compute the Mapped Generator $\hat{G}=f_G(R_p(s,t))$.

Nonce t	5DD4CBFC 96F5453B 130D890A 1CDBAE32
Pseudo-random R(s,t)	E2340305 C1CC37B5 08B3F320 AA8C4E15 1288FBBC 452FDD1B 00D5D585 7344F116 0FC1A115 EF560E0F 3A5946FE D0D1FC0E
$R_p(s,t)$	A2F8FF2D F50E52C6 599F386A DCB595D2 29F6A167 ADE2BE5F 2C3296AD D5B7430E
x-coordinate of the Mapped Generator $\hat{G}$	8E82D315 59ED0FDE 92A4D049 8ADD3C23 BABA94FB 77691E31 E90AEA77 FB17D427
y-coordinate of the Mapped Generator $\hat{G}$	4C1AE14B D0C3DBAC 0C871B7F 36081693 64437CA3 0AC243A0 89D3F266 C1E60FAD

1.3 Perform Key Agreement

The chip and the terminal perform an anonymous Diffie-Hellman key agreement using their secret keys and the mapped generator $\hat{G}$. The shared secret K is the x-coordinate of agreement.

Chip's private key SK_{PICC}	107CF586 96EF6155 053340FD 633392BA 81909DF7 B9706F22 6F32086C 7AFF974A
Chip's public key PK_{PICC}	67F78E5F 7F768608 2B293E8D 087E0569 16D0F74B C01A5F89 57D0DE45 691E51E8 932B69A9 62B52A09 85AD2C0A 271EE6A1 3A8ADDDC D1A3A994 B9DED257 F4D22753

Terminal's private key SK_{PCD}	A73FB703 AC1436A1 8E0CFA5A BB3F7BEC 7A070E7A 6788486B EE230C4A 22762595
Terminal's public key PK_{PCD}	89CBA23F FE96AA18 D824627C 3E934E54 A9FD0B87 A95D1471 DC1C0ABF DCD640D4 6755DE9B 7B778280 B6BEBD57 439ADFEB 0E21FD4E D6DF4257 8C13418A 59B34C37
Shared secret K	4F150FDE 1D4F0E38 E95017B8 91BAE171 33A0DF45 B0D3E18B 60BA7BEA FDC2C713

Using the specifications from [1], the session keys KENC and KMAC are derived from K using the hash function SHA1: KENC=SHA1(K||0x00000001) and KMAC=SHA1(K||0x00000002). Then, only the first 16 octets of the digest are used with the following result:

K_{ENC}	0D3FEB33 251A6370 893D62AE 8DAAF51B
K_{MAC}	B01E89E3 D9E8719E 586B50B4 A7506E0B

1.4 Mutual Authentication

The authentication tokens are computed using a CMAC on the following inputs with the key K_{MAC}.

Input data for T_{PICC}	7F494F06 0A04007F 00070202 04040286 410489C BA23FFE96 AA18D824 627C3E93 4E54A9FD 0B87A95D 1471DC1C 0ABFDCD6 40D46755 DE9B7B77 8280B6BE BD57439A DFEB0E21 FD4ED6DF 42578C13 418A59B3 4C37
Input data for T_{PCD}	7F494F06 0A04007F 00070202 04040286 410467F7 8E5F7F76 86082B29 3E8D087E 056916D0 F74BC01A 5F8957D0 DE45691E

	51E8932B 69A962B5 2A0985AD 2C0A271E E6A13A8A DDDCD1A3 A994B9DE D257F4D2 2753

The corresponding authentication tokens are:

TPICC	75D4D96E 8D5B0308
TPCD	450F02B8 6F6A0909

2 DH-based Example

This example is based on the 1024-bit MODP Group with 160-bit Prime Order Subgroup introduced in [4]. The PACE example from [2] is used and modified to enable Integrated Mapping. The block cipher used in this example is AES-128.

The group parameters are:

Prime p	B10B8F96 A080E01D DE92DE5E AE5D54EC 52C99FBC FB06A3C6 9A6A9DCA 52D23B61 6073E286 75A23D18 9838EF1E 2EE652C0 13ECB4AE A9061123 24975C3C D49B83BF ACCBDD7D 90C4BD70 98488E9C 219A7372 4EFFD6FA E5644738 FAA31A4F F55BCCC0 A151AF5F 0DC8B4BD 45BF37DF 365C1A65 E68CFDA7 6D4DA708 DF1FB2BC 2E4A4371
Subgroup generator g	A4D1CBD5 C3FD3412 6765A442 EFB99905 F8104DD2 58AC507F D6406CFF 14266D31 266FEA1E 5C41564B 777E690F 5504F213 160217B4 B01B886A 5E91547F 9E2749F4 D7FBD7D3 B9A92EE1 909D0D22 63F80A76 A6A24C08 7A091F53 1DBF0A01 69B6A28A

	D662A4D1 8E73AFA3 2D779D59 18D08BC8 858F4DCE F97C2A24 855E6EEB 22B3B2E5
Prime order q of g	F518AA87 81A8DF27 8ABA4E7D 64B7CB9D 49462353

The following encryption key is used:

K_π	591468CD A83D6521 9CCCB856 0233600F

2.1 Encrypted Nonce

A nonce s is randomly chosen by the chip and encrypted using K_π. The encrypted nonce z is then sent to the terminal.

Decrypted Nonce s	FA5B7E3E 49753A0D B9178B7B 9BD898C8
Encrypted Nonce z	9ABB8864 CA0FF155 1E620D1E F4E13510

2.2 Map Nonce

A nonce t is randomly chosen and sent in clear. t and s are then used to compute the Integrated Mapping. First, the pseudo-random function R_p, derived from AES, is applied to s and t. Then, the point encoding f_g is used on the result.

Nonce t	B3A6DB3C 870C3E99 245E0D1C 06B747DE
Pseudo-random R(s,t)	EAB98D13 E0905295 2AA72990 7C3C9461 84DEA0FE 74AD2B3A F506F0A8 3018459C 38099CD1 F7FF4EA0 A078DB1F AC136550 5E3DC855 00EF95E2 0B4EEF2E 88489233 BEE0546B 472F994B 618D1687 02406791 DEEF3CB4 810932EC 278F3533 FDB860EB 4835C36F A4F1BF3F A0B828A7 18C96BDE

	88FBA38A 3E6C35AA A1095925 1EB5FC71 0FC18725 8995944C 0F926E24 9373F485
$R_p(s,t)$	A0C7C50C 002061A5 1CC87D25 4EF38068 607417B6 EE1B3647 3CFB800D 2D2E5FA2 B6980F01 105D24FA B22ACD1B FA5C8A4C 093ECDFA FE6D7125 D42A843E 33860383 5CF19AFA FF75EFE2 1DC5F6AA 1F9AE46C 25087E73 68166FB0 8C1E4627 AFED7D93 570417B7 90FF7F74 7E57F432 B04E1236 819E0DFE F5B6E77C A4999925 328182D2
Mapped Generator $\hat{g}= f_g(R_p(s,t))$	1D7D767F 11E333BC D6DBAEF4 0E799E7A 926B9697 3550656F F3C83072 6D118D61 C276CDCC 61D475CF 03A98E0C 0E79CAEB A5BE2557 8BD4551D 0B109032 36F0B0F9 76852FA7 8EEA14EA 0ACA87D1 E91F688F E0DFF897 BBE35A47 2621D343 564B262F 34223AE8 FC59B664 BFEDFA2B FE7516CA 5510A6BB B633D517 EC25D4E0 BBAA16C2

2.3 Perform Key Agreement

The chip and the terminal perform an anonymous Diffie-Hellman key agreement using their secret keys and the mapped generator $\hat{g}$.

Chip's private key SK_{PICC}	020F018C 7284B047 FA7721A3 37EFB7AC B1440BB3 0C5252BD 41C97C30 C994BB78

	E9F0C5B3 2744D840 17D21FFA 6878396A 6469CA28 3EF5C000 DAF7D261 A39AB886 0ED4610A B5343390 897AAB5A 7787E4FA EFA0649C 6A94FDF8 2D991E8E 3FC332F5 142729E7 040A3F7D 5A4D3CD7 5CBEE1F0 43C1CAD2 DD484FEB 4ED22B59 7D36688E
Chip's public key PK_{PICC}	928D9A0F 9DBA450F 13FC859C 6F290D1D 36E42431 138A4378 500BEB4E 0401854C FF111F71 CB6DC1D0 335807A1 1388CC8E AA87B079 07AAD9FB A6B169AF 6D8C26AF 8DDDC39A DC3AD2E3 FF882B84 D23E9768 E95A80E4 746FB07A 9767679F E92133B4 D379935C 771BD7FB ED6C7BB4 B1708B27 5EA75679 524CDC9C 6A91370C C662A2F3
Terminal's private key SK_{PCD}	4BD0E547 40F9A028 E6A515BF DAF96784 8C4F5F5F FF65AA09 15947FFD 1A0DF2FA 6981271B C905F355 1457B7E0 3AC3B806 6DE4AA40 6C1171FB 43DD939C 4BA16175 103BA3DE E16419AA 248118F9 0CC36A3D 6F4C3736 52E0C3CC E7F0F1D0 C5425B36 00F0F0D6 A67F004C 8BBA33F2 B4733C72 52445C1D FC4F1107 203F71D2 EFB28161
Terminal's public key PK_{PCD}	0F0CC629 45A80292 51FB7EF3 C094E12E C68E4EF0 7F27CB9D 9CD04C5C 4250FAE0 E4F8A951 557E929A EB48E5C6 DD47F2F5

	CD7C351A 9BD2CD72 2C07EDE1 66770F08 FFCB3702 62CF308D D7B07F2E 0DA9CAAA 1492344C 85290691 9538C98A 4BA4187E 76CE9D87 832386D3 19CE2E04 3C3343AE AE6EDBA1 A9894DC5 094D22F7 FE1351D5
Shared secret K	419410D6 C0A17A4C 07C54872 CE1CBCEB 0A2705C1 A434C8A8 9A4CFE41 F1D78124 CA7EC52B DE7615E5 345E48AB 1ABB6E7D 1D59A57F 3174084D 3CA45703 97C1F622 28BDFDB2 DA191EA2 239E2C06 0DBE3BBC 23C2FCD0 AF12E0F9 E0B99FCF 91FF1959 011D5798 B2FCBC1F 14FCC24E 441F4C8F 9B08D977 E9498560 E63E7FFA B3134EA7

Using the specifications from [1], the session keys KENC and KMAC are derived from K using the hash function SHA1: KENC=SHA1(K||0x00000001) and KMAC=SHA1(K||0x00000002). Then, only the first 16 octets of the digest are used with the following result:

K_{ENC}	01AFC10C F87BE36D 8179E873 70171F07
K_{MAC}	23F0FBD0 5FD6C7B8 B88F4C83 09669061

2.4 Mutual Authentication

The authentication tokens are computed using a CMAC on the following inputs with the key K_{MAC}.

Input data for T_{PICC}	7F49818F 060A0400 7F000702 02040302 8481800F 0CC62945 A8029251 FB7EF3C0 94E12EC6 8E4EF07F 27CB9D9C D04C5C42

	50FAE0E4 F8A95155 7E929AEB 48E5C6DD 47F2F5CD 7C351A9B D2CD722C 07EDE166 770F08FF CB370262 CF308DD7 B07F2E0D A9CAAA14 92344C85 29069195 38C98A4B A4187E76 CE9D8783 2386D319 CE2E043C 3343AEAE 6EDBA1A9 894DC509 4D22F7FE 1351D5
Input data for T_{PCD}	7F49818F 060A0400 7F000702 02040302 84818092 8D9A0F9D BA450F13 FC859C6F 290D1D36 E4243113 8A437850 0BEB4E04 01854CFF 111F71CB 6DC1D033 5807A113 88CC8EAA 87B07907 AAD9FBA6 B169AF6D 8C26AF8D DDC39ADC 3AD2E3FF 882B84D2 3E9768E9 5A80E474 6FB07A97 67679FE9 2133B4D3 79935C77 1BD7FBED 6C7BB4B1 708B275E A7567952 4CDC9C6A 91370CC6 62A2F3

The corresponding authentication tokens are:

T_{PICC}	C2F04230 187E1525
T_{PCD}	55D61977 CBF5307E