International Civil Aviation Organization

WORKING PAPER

TAG/MRTD/22-WP/4
16/04/14
English Only

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

TWENTY-SECOND MEETING

Montréal, 21 to 23 May 2014

Agenda Item 2: Activities of the NTWG

TECHNICAL REPORT
TRAVEL DOCUMENT DEVIATION LIST ISSUANCE

(Presented by the New Technologies Working Group)

1. INTRODUCTION

1.1 This Working Paper introduces the Technical Report “Travel Document Deviation List Issuance”.

1.2 The Technical report specifies a standardised means for issuing Sates to communicate on deviations in their Travel Documents and/or associated certificates.

1.3 It is based on principles established during the development of the CSCA Master List, in that a signed deviation list for each State’s non-conformities will be provided via the ICAO PKD or the Issuing Authority through a website or a LDAP-server.

2. BACKGROUND

2.1 As States worldwide continue to adopt Machine Readable Travel Documents (MRTDs), the increased complexity and the rise in deviations have led to a need for reporting deviations from standards or the normal practice of a State through a standardized mechanism.

2.2 Deviations are generally observed within Country Signing Certificate Authorities (CSCA) certificates or Document Signer Certificates (DSCs), but States have also indicated issues related to the LDS and MRZ fields within their MRTDs.

2.3 While travel documents may contain deviations, they may still be useable in border management systems. For documents that are otherwise valid, they may remain in use for several years.

2.4 Consequently, relying parties should identify their own processes for handling any published deviations.

3. CURRENT STATUS

3.1 Prior to the release of this Technical Report, the only method for managing deviations is through the general advice given by issuing States via diplomatic means.

3.2 The Technical Report includes deviations affecting large numbers of MRTDs that might be reported so as to assist borders in making a determination on whether travel documents are valid, forged, or the product of a substitution.

3.3 Deviations are categorized into four specific areas:

a) Keys and Certificates

b) Logical Data Structure (LDS)

c) Machine Readable Zone (MRZ)

d) Chip

4. ACTION BY THE TAG/MRTD

4.1 The TAG/MRTD is invited to:

a) endorse the Technical Report “Travel Document Deviation List Issuance” version 1.11; and

b) approve inclusion of this Technical Report into the seventh edition of Doc 9303.

— END —

MACHINE READABLE TRAVEL DOCUMENTS

TECHNICAL REPORT

Travel Document Deviation List issuance

Version – 1.11
Date –May 21, 2014
Published by authority of the Secretary General

ISO/IEC JTC1 SC17 WG3/TF5
FOR THE
INTERNATIONAL CIVIL AVIATION ORGANIZATION

File	: TR - Travel Document Deviation List Issuance v1.11.doc
Author	: ISO/IEC JTC1 SC17 WG3/TF5

Release Control

Release	Date	Description
0.1	Mar 2012	Initial Draft creating a separate document
0.2	1 Jan 2013	Revise all business language
0.3	8 Jan 2013	Correction and edits, and set up doc for review and Jan 20 technical meeting.
0.4	20 Jan 2013	Updates from Editing Group meeting Singapore
0.5	21 Jan 2013	Updates from Editing Group meeting accepted and additional changes added after TF5 meeting 21 Jan
0.6	09 Feb 2013	Accepted changes from Sharon, Jens and Alan to create a clean copy for review
0.7	15 Feb 2013	Accepted changes and added OID's pre NTWG
0.8	26 April 2013	Corrected Rajesh company name..
0.9	30 April 2013	Updated ASN.1 structure and changed reporting mechanism to be "Deviation List" throughout.
1.0	25 May 2013	Accepted changes from BR, JB, SB, AB
1.1	5 June 2013	Incorporated editorial and technical changes from the TF5 meeting
1.11	21 May 2014	Version for approval at TAG_22

Technical Report editorial group		
Alan Bennett	Australia	DFAT
Jens Bender	Germany	BSI
Sharon Boeyen	Canada	Entrust
Tom Kinneging	Netherlands	Morpho
Bill Russell	USA	Mount Airey Group
R.Rajeshkumar	Singapore	Auctorizium

Table of contents

1. Introduction

1.1 Background

As States worldwide continue to adopt Machine Readable Travel Documents (MRTDs), the increased complexity and the rise in deviations have led to a need for reporting deviations from standards or the normal practice of a state through a standardized mechanism. Deviations are defined as MRTDs that contain elements that do not precisely conform to the ICAO specifications and the governing ISO and RFC standards. Deviations are generally observed within Country Signing Certificate Authorities (CSCA) or Document Signer Certificate (DSCs). Nonetheless, States have also indicated issues related to the LDS and MRZ fields within their MRTDs. The purpose of this Technical Report (TR) is to detail the mechanism by which issuing States can publish their deviations.

While travel documents may contain deviations, they may still be useable in border management systems. For documents that are otherwise valid, they may remain in use for several years. Consequently, relying parties should identify their own processes for handling any published deviations.

1.2 Operational Experiences

Prior to the release of this Technical Report, the only method for managing deviations is through the general advice given by issuing States via diplomatic means. This TR includes deviations affecting large numbers of MRTDs that might be reported so as to assist borders in making a determination on whether travel documents are valid, forged, or the product of a substitution. Some examples of operational errors include MRZ, LDS, and PKI deviations.

While the MRZ has been in use for many years some recent examples of known MRZ errors are:

- MRZ *Date of Birth* does not match VIZ page *Date of Birth*.
- MRZ *Citizenship* incorrectly reports the country of birth rather than citizenship

In most cases travel documents with a non-conforming MRZ will be recalled by the issuing State. Since there is a gap between issuance and the subsequent reissuance, travellers may be forced to use their deviating MRTD. During this time, a published deviation may alleviate potential problems for travellers.[1]

For LDS and PKI deviations, some could go undetected for long periods of time, as many States are not yet performing Passive and Active Authentication as specified by Doc 9303. However, issuing States are strongly encouraged to publish deviations in order assist the global community in the technical adoption of MRTDs.[2]

[1] Non Conformities that affect single documents or a small numbers of eMRTD’s will not be addressed by this TR, it is up to the issuing state to recall and re-issue individual documents.

[2] For any instance where there has been a security issue related to a PKI certificate, the proper response is revocation as described in Doc 9303. Further guidance is outside the scope of this TR.

1.3 Deviation List Approach

The approach described in this TR aims to provide an standardised means for issuing States to publish and distribute a Travel Document Deviation List. It is based on principles established during the development of the CSCA Master List, in that a signed deviation list for each State's non-conformities will be provided via the ICAO PKD or the Issuing Authority through a website or a LDAP-server. The PKD is used to support the dissemination of information relevant to the management of deviations.

Deviations are categorized into four specific areas:

- Keys and Certificates
- Logical Data Structure (LDS)
- Machine Readable Zone (MRZ)
- Chip

For each of these categories deviations will be describe to one level only, for example:

Category:	LDS
Error	DG2

Additional information will be provided via an operational parameter as made available by each State and/or a free text field in the reporting framework allowing the notifying State to add any descriptive text required. The notifying State can include links to additional information within the free text field. For certificate errors, the issuer will have the option to issue a new certificate, but this will not be mandatory.

The decision to advise relying parties of a non-conformity remains soley with the Issuing State. In deciding whether to create a Deviation List, States should take into consideration that as traveller self-processing border solutions become more common, failure to communicate information relevant to non-conforming travel documents may cause delays and inconvenience for travellers, which will reflect poorly on both the issuing state and the border process as a whole.

As stated in Section 1.1, the intention of this Technical Report is to provide a means of reporting deviations affecting 1000's of travel documents rather than a few or a few hundred. It is appropriate for States to manage small numbers of non-conforming travel documents directly.

1.4 Assumptions

- It is assumed that the reader is familiar with the contents of [R2], ICAO Doc 9303, "Machine Readable Travel Documents", and any other official documents issued by ICAO regarding Machine Readable Travel Documents.
- It is assumed that the reader is familiar with the concepts and mechanisms offered by public key cryptography and public key infrastructures.

At any time a state may create deviations that will affect the passage of its citizens through border control, and though inconvenient these deviations are generally administrative. While most deviations related to the MRZ will require at least a limited recall of travel documents by the issuing State, other non-MRZ deviations will not require a recall. In the case of PKI certificates, some deviations are minor and therefore do not require a certificate revocation. [R2]ICAO Doc 9303, "Machine Readable Travel Documents"

1.5 Terminology

1.5.1 Technical report terminology

The key words "MUST", “MUST NOT”, "SHALL", “SHALL NOT”, "REQUIRED", "SHOULD", “SHOULD NOT”, "RECOMMENDED", "MAY", and “OPTIONAL” in this document are to be interpreted as described in [R1], RFC 2119, S. Bradner, "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

In case OPTIONAL features are implemented, they MUST be implemented as described in this Technical Report.

2. Method

2.1 Deviation Elements

The elements that make up an MRTD range from paper to RFID chips, with each element protected in some way by security features that can be defined and thus tested by inspection systems during the life of the travel document. Security features employed on the physical travel document are both overt and covert. This TR considers only deviation elements within the MRZ, LDS and PKI.

The MRZ is a fixed-dimensional area located on the MRTD data page, containing mandatory and optional data formatted for machine reading using OCR methods. Doc 9303 Part 1 Volume 1 provides the specifications for the MRZ, including:

- Purpose;
- Constraints;
- Transliteration and;
- Data Structure of the upper and lower lines.

The conformity of the MRZ is routinely tested by inspection systems via data comparison with the corresponding VIZ page data and recalculation of the MRZ Check digits.

The authenticity and integrity of data stored on MRTD RFID chip is protected by Passive Authentication. This security mechanism is based on digital signatures and Public Key Infrastructure (PKI).

The structure of the MRTD LDS is defined by Doc 9303. While there are no specific tests to establish conformity, the data stored within the LDS is in part a subset of data available from the MRZ or VIZ page of the MRTD. Consequently, the same tests apply for the digital MRZ and VIZ data as would be applied to the MRZ and VIZ page. Authenticity of the LDS is provided through the correct application of Passive Authentication by inspection systems, while Active Authentication is performed by the chip. A brief description is below:

Passive Authentication (PA) is based on digital signatures and consists of the following Public Key Infrastructure (PKI) components:

1. **Country Signing CA (CSCA):** Every State establishes a CSCA as its national trust point in the context of ePassports. The CSCA issues public key certificates for one or more (national)

Document Signers. In addition each CSCA issues Certificate Revocation Lists (CRLs) of all revoked certificates.[3]

2. **Document Signers (DS):** A Document Signer digitally signs data to be stored on MRTDs; this signature is stored in the Document Security Object for each document.
3. **Active Authentication (AA):** Where AA is implemented, each chip contains its own AA Key Pair. The private Key is stored in the chip's secure memory with the Public Key stored at Data Group 15.

2.2 Issuing Deviation Lists

Deviation Lists MUST NOT be issued directly by a CSCA, instead the CSCA SHALL authorize a Deviation List Signer to compile, sign, and publish Deviation Lists. The Deviation List Signer SHALL use the same Certificate Profile as the Master List Signer, with the exception being that the ExtendedKeyUsage SHALL be set to `id-icao-cscaDeviationListSigningKey`.

The procedures to be performed for issuing a Deviation List SHOULD be reflected in the published certification policies of the issuing CSCA.

2.3 Deviation List Signer Certificate revocation

The issuing CSCA handles the Deviation List Signer certificate as it handles Document Signers. Revoked Deviation List Signer certificates will be published in a CRL, issued by the CSCA.

2.4 Receiving a Deviation List

Every Receiving State defines its own policies under which it accepts a Deviation List and how deviations are handled during the inspection of documents. Those policies are, in general, private information.

The Receiving State will at its sole discretion choose to allow MRTDs with a deviation to be utilized.

2.5 Categories of Deviations

2.5.1 Keys and Certificates

Certificate and key deviations are restricted to the following:

Issue	Comment
Certificate	Described to the Field or Extension
Keys	Described to the Field or Extension
AA	Described to the error/problem only

Note: Where a reporting state decides to issue a new certificate, the certificate MUST NOT be included in the Deviation List, but could be pointed to via the free text field.

2.5.2 Logical Data Structure (LDS)

LDS deviations are restricted to the Following

Issue	Comment

[3] Since CRLs are a security reporting mechanism and are constantly reissued, no defects reporting is necessary for them and are therefore outside the scope of this TR.

Issue	Comment
EF.Com	Described to the encoding error
DG's	Described to the Data Group
EF.sod	Described to the issue (eg DSC)

2.5.3 Machine Readable Zone (MRZ)

MRZ deviations are restricted to the following:

Issue	Comment
Match to VIZ	Described to the field
Check Digits	Described to the responsible check digit
Wrong Information encoded	Described to the MRZ field

2.6 Deviation Type Definitions

Categories of deviations and corresponding parameters may be extended over time, and will be maintained in supplements to Document 9303.

Each deviation is described by a `deviationDescription` element. The deviation is identified by an Object Identifier `deviationType` and may be further detailed by `parameters`. The field `description` MAY contain further information, such as how the nature of the deviation cannot be adequately described by the governing `deviationType`.

`deviationType`	`parameters`	Description
Certificate/Key Deviation		
`id-Deviaion-CertOrKey`	None	A generic certificate or key related deviation not covered by the more detailed deviations below.
`id-Deviation-CertOrKey-DSSignature`	None	The signature of the Document Signer Certificate is wrong.
`id-Deviation-CertOrKey-DSEncoding CertField`	`CertField`	The Document Signer Certificate contains a coding error.
`id-Deviation-CertOrKey-CSCAEncoding`	`CertField`	The Country Signing CA Certificate contains a coding error.
`id-Deviation-CertOrKey-AAKeyCompromised`	None	The key for Active Authentication may be compromised and should not be reilied upon.
LDS Deviation		
`id-Deviation-LDS`	None	A generic LDS related deviation not covered by the more detailed deviations below.
`id-Deviation-LDS-DGMalformed`	`Datagroup`	The TLV encoding of the given datagroup is corrupted.
`id-Deviation-LDS-DGHashWrong`	`Datagroup`	The hash value of the given datagroup in the EF.SOD is wrong
`id-Deviation-LDS-SODSignatureWrong`	None	The signature contained in EF.SOD is wrong.
`id-Deviation-LDS-COMinconsistent`	None	EF.COM and EF.SOD are incosistent.
MRZ Deviation		
`id-Deviation-MRZ`	None	A generic MRZ related deviation not covered by

		the more detailed deviation below.
`id-Deviation-MRZ-WrongData`	`MRZField`	The given field of the MRZ contains wrong data (e.g.. inconsistent with VIZ), but the derived BAC key is usable to open the chip. If the derived BAC key is not usable, additionally `id-Deviation-Chip` SHALL be included in the Deviation List.
`id-Deviation-MRZ-WrongCheckDigit`	`MRZField`	The check digit ot given field of the MRZ is calculated wrong.
Chip Deviation		
`id-Deviation-Chip`	None	The Chip is not usable, e.g. wrong BAC key, broken antenna or other physical defect.

Maintenance of the list type of defects will be via the Supplement to Document 9303.

2.7 Identification of Deviant Documents

Documents affected by a deviation MAY be identified by several different means:

- by the Document Signer Certificate used to sign these documents; the Document Signer can be either identified by
  - the Distinguished Name of the Issuer in combination with the Serial Number of the certificate (`issuerAndSerialNumber`),
  - the `subjectKeyIdentifier` uniquely identify the Document Signer, or
  - the hash of the Document Signer certificate (`certificateHash`); the hash function to be used is the same as used in the signature of the Deviation List.
- by a range of issuing dates (`startIssuingDate`, `endIssuingDate`)
- by a list of document numbers (`listOfDocNumbers`).

Each method has advantages and disadvanges for the issuer of a Deviation List as well for the receiver of a Deviation List. These include:

- Identification by Document Signer allows recognition of a deviation by the inpsection systems only after Passive Authentication was performed. Additionally, identification by Document Signer might be too coarse to accurately identify only defect documents, i.e. the deviation affects only part of the documents signed by a given Document Signer.
- The Issuing Date is not part of the machine readable zone, and also in general not available in the electronic LDS. Therefore this is not suitable for automated processing. Additionally, depending on the Issuing State, the Issuing Date might not be the actual date of passport personalization, but the application date, and therefore not accurate enough to identify only affected documents.
- A list of document numbers is difficult to compile if document numbers are not issued sequentially. A list of document numbers grows quick quite quickly to unmanagable size if many documents are affected by a defect.

It is RECOMMENDED to give as much identifying information on affected documents as possible. If several methods for identification are given, the conditions MUST be met simultaneaously to identify a document. It is at the discretion of the Relying State to decide which means of identification given in a Defect List entry are used to identify affected documents.

3. Publication

Deviation Lists can be published via the ICAO PKD and/or the Issuing Authority through a website or LDAP server. The primary distribution point for Defect Lists is the PKD.

Defect Lists	
Primary Distribution	PKD
Secondary Distribution	Website/LDAP

3.1 Publication by the Issuing State

Deviation Lists can be published via a website or an LDAP-server of the Issuing Authority.

3.2 Publication on the PKD

The PKD operates as a central repository for Deviation Lists.

The procedure for publishing a Deviation List is as follows:

1. Deviation Lists are sent to the write PKD, as part of the usual certificate upload process as defined in the PKD Interface Specification and PKD Procedures Manual.
2. The ICAO PKD office validates the signatures of uploaded Deviation Lists as specified in the PKD Procedures Manual.
3. Valid Deviation Lists are moved to the read PKD.
4. The distributing state will determine if their Deviation List will be publically available, or restricted to PKD member states.

3.3 Relying Parties

To be able to verify a Deviation List, a relying party needs to have received the corresponding CSCA certificate of the issuing State by out of band communications. It is up to the Relying Party to decide how to handle MRTDs with a corresponding entry in the Issuing State's Deviation List.

4. Technical specifications

4.1 Deviation List specification

The Deviation List is implemented as a SignedData type, as specified in [R3], RFC 3852 - Cryptographic Message Syntax - July 2004. All Deviation Lists MUST be produced in DER format to preserve the integrity of the signatures within them.

The range of deviations will be bounded by:

- Date Range (including both the Issue and Expiry date);
- Issuer Name and Serial Number;
- Subject Key Identifier of DSC;
- List of eMRTD numbers.

Appropriate combinations of these values will be used to accurately bind the range of MRTDs affected. When combining values, they are to be processed as joined by “AND”. There is no option to process values as joined using “OR”.

4.1.1 SignedData Type

The processing rules in RFC3852 apply.

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

Value		Comments
SignedData		
version	m	Value = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	id-DefectList
eContent	m	The encoded contents DefectList
certificates	m	States MUST include the /Defect List Signer certificate and SHOULD include the CSCA certificate, which can be used to verify the signature in the signerInfos field.
crls	x	
signerInfos	m	It is RECOMMENDED that States only provide 1 signerinfo within this field.
SignerInfo	m	
version	m	The value of this field is dictated by the sid field. See RFC3852 Section 5.3 for rules regarding this field
sid	m	
subjectKeyIdentifier	r	It is RECOMMENDED that States support this field over issuerandSerialNumber.
digestAlgorithm	m	The algorithm identifier of the algorithm used to produce the hash value over encapsulatedContent and SignedAttrs.
signedAttrs	m	Producing States may wish to include additional

Value		Comments
		attributes for inclusion in the signature, however these do not have to be processed by receiving States except to verify the signature value. signedAttrs MUST include signing time (ref. PKCS#9).
signatureAlgorithm	m	The algorithm identifier of the algorithm used to produce the signature value, and any associated parameters.
signature	m	The result of the signature generation process.
unsignedAttrs	x	

4.1.2 ASN.1 specification

```
DeviationList
{ iso-itu-t(2) international-organization(23) icao(136) mrtd(1) security(1)
deviationlist(7)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

     -- Imports from RFC 3280 [PROFILE], Appendix A.1
         AlgorithmIdentifier
            FROM PKIX1Explicit88
                   { iso(1) identified-organization(3) dod(6)
                     internet(1) security(5) mechanisms(5) pkix(7)
                     mod(0) pkix1-explicit(18) }

     -- Imports from RFC 3852
         SubjectKeyIdentifier, Digest, IssuerAndSerialNumber
              FROM CryptographicMessageSyntax2004
                   { iso(1) member-body(2) us(840) rsadsi(113549)
                     pkcs(1) pkcs-9(9) smime(16) modules(0)
                     cms-2004(24) };

DeviationListVersion ::= INTEGER {v0(0)}

DeviationList ::= SEQUENCE {
  version         DeviationListVersion,
  digestAlgorithm AlgorithmIdentifier OPTIONAL,
  deviations      SET OF Deviation
}

Deviation ::= SEQUENCE{
  documents       DeviationDocuments,
  descriptions    SET OF DeviationDescription
}

DeviationDescription ::= SEQUENCE{
  description          PrintableString  OPTIONAL,
  deviationType        OBJECT IDENTIFIER,
  parameters           [0] ANY DEFINED BY deviationType OPTIONAL,
  nationalUse          [1] ANY OPTIONAL

  -- The nationalUse field is for internal State use, and is not governed
  -- by an ICAO specification.
}

DeviationDocuments ::= SEQUENCE {
  documentType         [0] PrintableString (SIZE(2)) OPTIONAL,
      -- per MRZ, e.g. 'P'
  dscIdentifier         DocumentSignerIdentifier OPTIONAL,
  issuingDate           [4] IssuancePeriod OPTIONAL,
  documentNumbers       [5] SET OF PrintableString OPTIONAL
}

DocumentSignerIdentifier ::= CHOICE{
  issuerAndSerialNumber [1] IssuerAndSerialNumber,
  subjectKeyIdentifier  [2] SubjectKeyIdentifier,
  certificateDigest     [3] Digest        -- if used, digestAlgorithm must
be present in DeviationList
}

IssuancePeriod ::= SEQUENCE {
  firstIssued          GeneralizedTime,
  lastIssued           GeneralizedTime
}

-- CertField is used to define which part of a certificate is
-- affected by a coding error. Parts of the Body are identified by
-- the corresponding value of CertificateBodyField, extensions
-- by the corresponding OID identifying the extension.

CertField ::= CHOICE {
  body      CertificateBodyField,
  extension OBJECT IDENTIFIER
}
CertificateBodyField ::= INTEGER {
  generic(0), version(1),  serialNumber(2), signature(3), issuer(4),
  validity(5), subject(6), subjectPublicKeyInfo(7),
  issuerUniqueID(8), subjectUniqueID(9)
}

Datagroup ::= INTEGER
              {dg1(1), dg2(2), dg3(3), dg4(4), dg5(5), dg6(6),
               dg7(7), dg8(8), dg9(9), dg10(10), dg11(11),
               dg12(12), dg13(13), dg14(14), dg15(15), dg16(16),
               sod(20), com(21)}

MRZField ::= INTEGER
             {generic(0), documentCode(1), issuingState(2), personName(3),
              documentNumber(4), nationality(5), dateOfBirth(6),
              sex(7), dateOfExpiry(8), optionalData(9)}

-- Base Object Identifiers

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}
id-icao-DeviationList OBJECT IDENTIFIER ::= {id-icao-mrtd-security 7}
id-icao-DeviationListSigningKey OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 8}

-- Deviation Object Identifiers and Parameter Definitions

id-Deviation-CertOrKey OBJECT IDENTIFIER ::= {id-icao-DeviationList 1}
id-Deviation-CertOrKey-DSSignature OBJECT IDENTIFIER ::= {id-Deviation-
CertOrKey 1}
id-Deviation-CertOrKey-DSEncoding OBJECT IDENTIFIER ::= {id-Deviation-
CertOrKey 2}
id-Deviation-CertOrKey-CSCAEncoding OBJECT IDENTIFIER ::= {id-Deviation-
CertOrKey 3}
id-Deviation-CertOrKey-AAKeyCompromised OBJECT IDENTIFIER ::= {id-
Deviation-CertOrKey 4}
id-Deviation-LDS OBJECT IDENTIFIER ::= {id-icao-DeviationList 2}
id-Deviation-LDS-DGMalformed OBJECT IDENTIFIER ::= {id-Deviation-LDS 1}
```

```
id-Deviation-LDS-DGHashWrong OBJECT IDENTIFIER ::= {id-Deviation-LDS 2}
id-Deviation-LDS-SODSignatureWrong OBJECT IDENTIFIER ::= {id-Deviation-LDS
3}
id-Deviation-LDS-COMInconsistent OBJECT IDENTIFIER ::= {id-Deviation-LDS 4}

id-Deviation-MRZ OBJECT IDENTIFIER ::= {id-icao-DeviationList 3}
id-Deviation-MRZ-WrongData OBJECT IDENTIFIER ::= {id-Deviation-MRZ 1}
id-Deviation-MRZ-WrongCheckDigit OBJECT IDENTIFIER ::= {id-Deviation-MRZ 2}

id-Deviation-Chip OBJECT IDENTIFIER ::= {id-icao-DeviationList 4}

END
```

Annex A Reference documentation

The following documentation served as reference for this Technical Report:

[R1] RFC 2119, S. Bradner, "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

[R2] ICAO Doc 9303, “Machine Readable Travel Documents“

[R3] RFC 3852 - Cryptographic Message Syntax - July 2004

[R4] 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

[R5] ISO/IEC 3166, Codes for the representation of names of countries and their subdivisions – 1997

[R6] ICAO Supplement to Doc 9303

Annex B Abbreviations

Abbreviation	
CA	Certification Authority
CRL	Certificate Revocation List
CSCA	Country Signing Certification Authority
DER	Distinguished Encoding Rule
DS	Document Signer
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
LDS	Logical Data Structure
MRTD	Machine Readable Travel Document
PKI	Public Key Infrastructure
PKD	Public Key Directory
SO_D	Document Security Object