International Civil Aviation Organization

WORKING PAPER

TAG/MRTD/20-WP/7
01/08/11
English Only

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

TWENTIETH MEETING

Montréal, 7 to 9 September 2011

Agenda Item 2: Activities of the NTWG
Agenda Item 2.7: Technical Report – Logical Data Structure And Public Key Infrastructure Maintenance

TECHNICAL REPORT – LOGICAL DATA STRUCTURE AND PUBLIC KEY INFRASTRUCTURE MAINTENANCE

(Presented by the NTWG)

1. INTRODUCTION

1.1 The sixth edition of Part 1, Volume 2 of Doc 9303 — *Machine Readable Travel Documents*, published in September 2006, and the third edition of Part 3, Volume 2, published in 2008, contain the technical specifications of the Logical Data Structure (LDS) in Section III, and the Public Key Infrastructure (PKI) in Section IV.

1.2 Issues that arise within the scope of Doc 9303 are being addressed in the Supplement to Doc 9303, the purpose of which Supplement is to provide guidance, advice, updates, clarifications and amplifications for the travel document community to have timely and official direction with respect to the standards. The Supplement is published on a regular basis.

1.3 In this fast moving world it is necessary to evaluate the specifications in Doc 9303 from time to time to stay up to date, especially with respect to cryptographic security features and PKI.

1.4 Such evaluation activities were announced at the nineteenth meeting of the TAG/MRTD in December 2009 through Information Paper TAG/MRTD/19-IP/2. The results of the evaluation were detailed in a technical report providing updated specifications on relevant subjects.

1.5 At its meeting in Bern, Switzerland in May 2011, the NTWG approved this technical report for presentation at the twentieth meeting of the TAG/MRTD.

2. TECHNICAL REPORT

2.1 The technical report containing the revised specifications is entitled *LDS and PKI Maintenance* (version 1.0) and addresses the revised specifications detailed below.

2.2 LDS version information: The LDS version is indicated in a file called EF.COM, which is not electronically signed. Undetected manipulation of its contents is possible, and this may be of interest for an attacker, who aims to mask the presence of new security features in a specific LDS version. The Document Security Object has therefore been extended with a signed attribute, containing the LDS and Unicode version information. This information is protected by Passive Authentication.

2.3 Certificate profiles: Volume 2, Section IV, Normative Appendix 1 of Doc 9303 specifies certificate profiles for Country Signing CA certificates and Document Signer certificates. In practice, the assignment of qualifications such as mandatory and optional to various certificate extensions appears to be too strict in some cases and not strict enough in others, resulting in interoperability issues in the exchange of certificates. The specified profiles have now been revised.

2.4 Access Control: The present access control mechanism for electronic machine readable travel documents is Basic Access Control, which was evaluated in relation to future technology developments and e-passport validity periods. A revised access control mechanism has been developed, which is specified in the technical report *Supplemental Access Control for Machine Readable Travel Documents*, endorsed by TAG/MRTD/19.

2.5 Active Authentication: Although Doc 9303 specifies the use of various cryptographic algorithms, for Active Authentication the Seventh Supplement to Doc 9303 recommends the use of RSA and not ECDSA. The technical report provides a specification for the use of ECDSA in Active Authentication, in which a choice is made between the alternative methods of implementation.

2.6 Extended Length: Doc 9303 does not contain specifications for the use of Extended Length in the communications between an e-passport chip and an inspection system. Specifications on the use of Extended Length are under development within the International Organization for Standardization and the results, once finalized, will be incorporated into, or referenced in, Doc 9303.

3. ACTION BY THE TAG/MRTD

3.1 The TAG/MRTD is invited to:

a) recognize the necessity of regular evaluations of the specifications in Doc 9303 to preserve an appropriate level of accuracy and security; and

b) approve the technical report *LDS and PKI Maintenance* containing revised specifications for inclusion in Doc 9303.

— — — — — — — —

MACHINE READABLE TRAVEL DOCUMENTS

TECHNICAL REPORT

LDS and PKI Maintenance

Version – **1.0**
Date – May 5, 2011

Published by authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION

File	: TR-LDS-PKI Maintenance V1.0.pdf
Author	: ISO/IEC JTC1 SC17 WG3/TF5 for ICAO-NTWG

Release Control

Release	Date	Description
0.1	16-06-2009	First draft for TF5
0.2	08-10-2009	Comments after TF5 Abu Dhabi incorporated
0.3	15-10-2009	Title changed
0.4	Jan 2010	Results of 13th TF5 meeting incorporated
0.5	Feb 2010	Added results of 13th TF5 meeting incorporated
0.51	March 2010	Minor editorial corrections
0.52	September 2010	TF5 amendments
0.8	September 2010	TF5 reviewed, version for NTWG
0.9	April 2011	TF5 final revision, addition of NameChange and DocumentType extensions, version for approval and publication
1.0	May 2011	Editorial corrections, Updated references to ISO/IEC 14443 and ISO/IEC 10373-6; NTWG approved version for TAG endorsement.

Table of contents

1. INTRODUCTION 4
1.1 ASSUMPTIONS 4
1.2 TERMINOLOGY 4
1.2.1 Technical report terminology 4
1.2.2 Abbreviations 4
1.3 REFERENCE DOCUMENTATION 4
2. LDS VERSIONING 7
2.1 PRESENT SPECIFICATION 7
2.2 REVISED SPECIFICATION 8
2.3 BACKWARDS COMPATIBILITY 10
2.4 IMPLEMENTATION STRATEGY 10
2.5 DOCUMENTATION 10
3. CERTIFICATE PROFILES 11
3.1 PRESENT SPECIFICATION 11
3.2 REVISED SPECIFICATION 11
3.2.1 Certificate Profiles 11
3.3 BACKWARDS COMPATIBILITY 14
3.4 IMPLEMENTATION STRATEGY 14
3.5 DOCUMENTATION 14
4. ACCESS CONTROL 16
4.1 PRESENT SPECIFICATION 16
4.2 REVISED SPECIFICATION 16
5. ACTIVE AUTHENTICATION 17
5.1 PRESENT SPECIFICATION 17
5.2 REVISED SPECIFICATION 17
5.2.1 The signature type returned by AA 17
5.2.2 Way to specify the HASH algorithm used 17
5.2.3 HASH calculation output versus ECDSA key length 18
5.3 BACKWARDS COMPATIBILITY 19
5.4 IMPLEMENTATION STRATEGY 19
5.5 DOCUMENTATION 19
6. EXTENDED LENGTH 20
6.1 PRESENT SPECIFICATION 20

1. Introduction

The specifications for the electronic part of Machine Readable Travel Documents have been in place since 2004. In this fast moving world it is necessary to evaluate these specifications from time to time to stay up to date, especially with respect to the cryptographic security features and PKI.
Therefore an evaluation work plan has been developed, addressing the various aspects that may need to be updated.
This Technical Report results from this evaluation, and provides updated specifications for relevant subjects.

1.1 Assumptions

It has been assumed that the reader is familiar with the concepts and mechanisms offered by public key cryptography and public key infrastructures.

It has been assumed that the reader is familiar with the contents of *ICAO Doc 9303-Machine Readable Travel Documents, part 1-Machine Readable Passports, Volume 2-Specifications for Electronically Enabled Passports with Biometric Identification Capability, sixth edition-2006*, e.g. *ICAO Doc 9303-Machine Readable Travel Documents, part 3-Machine Readable Official Travel Documents, Volume 2-Specifications for Electronically Enabled MRtds with Biometric Identification Capability, third edition-2008*, as well as *ICAO Supplement to Doc 9303, latest release*.

1.2 Terminology

1.2.1 Technical report 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.*

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

1.2.2 Abbreviations

Abbreviation	
C_{DS}	Document Signer Certificate
DER	Distinguished Encoding Rule
ICAO	International Civil Aviation Organization
LDS	Logical Data Structure
SO_D	Document Security Object

1.3 Reference documentation

The following documentation served as reference for Doc 9303, Technical Reports and the 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/IEC15444, *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)*

2. LDS Versioning

2.1 Present specification

ICAO Doc 9303 specifies in Volume 2, Section III, the LDS version 1.7. LDS version numbering and Unicode version numbering are specifies in the EF.COM, as follows:

Header. The Header contains the following information, which enables a receiving State or approved receiving organization locate and decode the various Data Groups and Data Elements contained within the block of data recorded by the issuing State or organization.

APPLICATION IDENTIFIER (AID)
LDS VERSION NUMBER
UNICODE VERSION NUMBER

LDS Version Number. The LDS Version Number defines the format version of the LDS. The exact format to be used for storing this value will be defined in the technology mapping annexes. Standardized format for an LDS Version Number is "aabb", where,

- "aa" = number (01 –99) identifying the Version of the LDS (i.e., Significant additions to the LDS)
- "bb" = number (01-99) identifying the Update of the LDS

Future upgrades to the standardized organization of the LDS have been anticipated and will be addressed through publication of Amendments to the specifications by ICAO. A Version Number will be assigned to each upgrade to ensure that receiving States and approved receiving organizations will be able to accurately decode all versions of the LDS.

Unicode Version Number. The Unicode Version Number identifies the coding method used when recording alpha, numeric and special characters, including national characters. The standardized format for a Unicode Version Number is “aabbcc”, where, The exact format to be used for storing this value will be defined in the technology mapping annexes.

- “aa” = number identifying the **Major version** of the Unicode Standard (i.e. Significant additions to the standard, published as a book);
- “bb” = number identifying the **Minor version** of the Unicode Standard (i.e. Character additions or more significant normative changes, published as a Technical Report); and
- “cc” = number identifying the **Update version** of the Unicode Standard (i.e. Any other changes to normative or important informative portions of the Standard that could change program behavior. These changes are reflected in new Unicode Character Database files and an update page).

Although future upgrades to the standardized organization of the LDS have been anticipated and the decoding of future LDS versions is supported by the LDS version number, this construction has a drawback.
The EF.COM file is not signed. Therefore undetected manipulation of its contents is possible. This may be of interest for an attacker, who aims at masking the presence of new security features in a specific LDS version.
Therefore it is desirable that the LDS version number is part of the signed information, and as such protected by Passive Authentication.

2.2 Revised specification

The Document Security Object has been extended with a signed attribute, containing the LDS and Unicode version information:

```
LDSVersionInfo ::= SEQUENCE {
      ldsVersion       PRINTABLE STRING
      unicodeVersion   PRINTABLE STRING }
```

The version number of the Document Security Object has been incremented from V0 to V1.

Specification of the Security Object V1 is as follows:
The Document Security object is implemented as a SignedData Type, as specified in RFC 3369, *R. Housley, Cryptographic Message Syntax (CMS), August 2002.* All security objects MUST be produced in Distinguished Encoding Rule (DER) format to preserve the integrity of the signatures within them.

Signed Data Type
The processing rules in RFC3369 apply.

m	mandatory – the field MUST be present
x	do not use – the field SHOULD NOT be populated
o	optional – the field MAY be present
c	choice – the field contents is a choice from alternatives

Value		Comments
SignedData		
version	m	Value = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	id-icao-mrtd-security-ldsSecurityObject
eContent	m	The encoded contents of an ldsSecurityObject
certificates	m	Nations SHALL include the Document Signer Certificate (C_{DS}) which can be used to verify the signature in the signerInfos field.
Crls	x	It is recommended that States do not use this field
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 RFC3369 Section 5.3 for rules regarding this field
Sid	m	
issuerandSerialNumber	c	It is recommended that nations support this field over subjectKeyIdentifier.
subjectKeyIdentifier	c	
digestAlgorithm	m	The algorithm identifier of the algorithm used to produce the hash value over encapsulatedContent and SignedAttrs.
signedAttrs	m	Producing nations may wish to include additional attributes for inclusion in the signature, however these do not have to be processed by receiving nations except to verify the signature value.
signatureAlgorithm	m	The algorithm identifier of the algorithm used to produce the signature value, and any associated parameters.

Value		Comments
signature	m	The result of the signature generation process.
unsignedAttrs	o	Producing States may wish to use this field, but it is not recommended and receiving nations may choose to ignore them.

ASN.1 Profile LDS Security Object

```
LDSSecurityObject {iso(2) identified-organization(23) icao(136)
mrtd(1) security(1) ldsSecurityObject(1)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- 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)
id-mod(0) id-pkix1-explicit(18) }

-- Constants

ub-DataGroups INTEGER ::= 16

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

-- LDS Security Object

LDSSecurityObjectVersion ::= INTEGER {V0(0), V1(1)
-- If LDSSecurityObjectVersion is V1, ldsVersionInfo MUST be present }

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

LDSSecurityObject ::= SEQUENCE {
     version               LDSSecurityObjectVersion,
     hashAlgorithm         DigestAlgorithmIdentifier,
     dataGroupHashValues   SEQUENCE SIZE (2..ub-DataGroups) OF
     DataGroupHash
     ldsVersionInfo        LDSVersionInfo OPTIONAL
     -- If present, version MUST be V1 }

DataGroupHash ::= SEQUENCE {
     dataGroupNumber       DataGroupNumber,
     dataGroupHashValue    OCTET STRING }

DataGroupNumber ::= INTEGER {
     dataGroup1       (1),
     dataGroup2       (2),
     dataGroup3       (3),
     dataGroup4       (4),
     dataGroup5       (5),
```

```
      dataGroup6       (6),
      dataGroup7       (7),
      dataGroup8       (8),
      dataGroup9       (9),
      dataGroup10     (10),
      dataGroup11     (11),
      dataGroup12     (12),
      dataGroup13     (13),
      dataGroup14     (14),
      dataGroup15     (15),
      dataGroup16     (16)}

LDSVersionInfo ::= SEQUENCE {
      ldsVersion      PRINTABLE STRING
      unicodeVersion  PRINTABLE STRING }

END
```

Note:
The field `dataGroupValue` contains the calculated hash over the complete contents of the Data group EF, specified by `dataGroupNumber`.

2.3 Backwards compatibility

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

2.4 Implementation strategy

With this change all information, present in the EF.COM, has been duplicated in the SO_D. This means that the EF.COM will be removed from the specifications from the next LDS version after V1.8.
It is RECOMMENDED that inspection systems that rely on the EF.COM will be modified to use the SO_D instead as soon as possible.

2.5 Documentation

Present documentation, affected by this change, is:

ICAO Doc 9303-Machine Readable Travel Documents, part 1-Machine Readable Passports, Volume 2-Specifications for Electronically Enabled Passports with Biometric Identification Capability, sixth edition-2006

- Normative Appendix 3 to Section IV - “Document Security Object”

ICAO Doc 9303-Machine Readable Travel Documents, part 3-Machine Readable Official Travel Documents, Volume 2-Specifications for Electronically Enabled MRtds with Biometric Identification Capability, third edition-2008

- Normative Appendix 3 to Section IV - “Document Security Object”

ICAO Supplement to Doc 9303, latest release

- R1-p1_v2_sIV_0006

3. Certificate Profiles

3.1 Present specification

ICAO Doc 9303 specifies in Volume 2, Section IV, Normative Appendix 1 the certificate profiles for Country Signing CA certificates and Document Signer certificates.
In practice the assignments of the qualifications **m**, **x**, **o**, and **c** to the various extensions appeared to be too strict in some cases, as well as not strict enough in others. This resulted in interoperability issues at the exchange of certificates. Therefore the specified profiles were reviewed.

3.2 Revised specification

The review of the certificate profiles resulted in the revised profiles shown in par. 3.2.1.

These profiles are based on the requirement that each issuing State or entity SHALL create a single CSCA for the purpose of signing all Doc 9303 compliant MRTDs/MRtds.

Also two additional certificate profiles were defined:

- for the CSCA Master List Signer
- for Communications, even though it is not strictly needed today. This is a future proofing step, the certificate may be used for access to the PKD or for LDAP/EMAIL/ HTTP communications between countries. It is recommended to position this under the CSCA.

3.2.1 Certificate Profiles

The profile uses the following terminology for each of the fields in the X.509 certificate:
m mandatory – the field MUST be present
x do not use – the field SHOULD NOT be populated
o optional – the field MAY be present
c critical – the extension is marked critical, receiving applications MUST be able to process this extension.

Certificate Body

Certificate Component	Section in RFC 5280	Certificates	Comments
Certificate	4.1.1	m	
TBSCertificate	4.1.1.1	m	see next part of the table
signatureAlgorithm	4.1.1.2	m	value inserted here dependent on algorithm selected
signatureValue	4.1.1.3	m	value inserted here dependent on algorithm selected
TBSCertificate	4.1.2		
version	4.1.2.1	m	MUST be v3
serialNumber	4.1.2.2	m	
signature	4.1.2.3	m	value inserted here MUST match the OID in signatureAlgorithm
issuer	4.1.2.4	m	See Note 3
validity	4.1.2.5	m	Implementations MUST specify using UTC time until 2049 from then on using GeneralizedTime
subject	4.1.2.6	m	See Note 3
subjectPublicKeyInfo	4.1.2.7	m	
issuerUniqueID	4.1.2.8	x	
subjectUniqueID	4.1.2.8	x	
extensions	4.1.2.9	m	see next table on which extensions should be present

Extensions

Extension name	Section in RFC 5280	Country Signing CA	Document Signer	Master List Signer	Communication	Comments
AuthorityKeyIdentifier	**4.2.1.1**	**m**	**m**	**m**	**m**	
keyIdentifier		m	m	m	m	
authorityCertIssuer		o	o	o	o	
authorityCertSerialNumber		o	o	o	o	
SubjectKeyIdentifier	**4.2.1.2**	**m**	**o**	**o**	**o**	
subjectKeyIdentifier		m	m	m	m	
KeyUsage	**4.2.1.3**	**mc**	**mc**	**mc**	**mc**	
digitalSignature		x	m	m	m	
nonRepudiation		x	x	x	x	
keyEncipherment		x	x	x	o	
dataEncipherment		x	x	x	x	
keyAgreement		x	x	x	o	
keyCertSign		m	x	x	x	
cRLSign		m	x	x	x	
encipherOnly		x	x	x	x	
decipherOnly		x	x	x	x	
PrivateKeyUsagePeriod		**m**	**m**	**m**	**m**	This would be the issuing period of the private key (ref. RFC3280, section 4.2.1.4
CertificatePolicies	**4.2.1.4**	**o**	**o**	**o**	**o**	
PolicyInformation		m	m	m	m	
policyIdentifier		m	m	m	m	
policyQualifiers		o	o	o	o	
PolicyMappings	**4.2.1.5**	**x**	**x**	**x**	**x**	
SubjectAltName	**4.2.1.6**	**m**	**m**	**m**	**m**	See Note 4
IssuerAltName	**4.2.1.7**	**m**	**m**	**m**	**m**	
SubjectDirectoryAttributes	**4.2.1.8**	**x**	**x**	**x**	**x**	
Basic Constraints	**4.2.1.9**	**mc**	**x**	**x**	**x**	
cA		m	x	x	x	
PathLenConstraint		m	x	x	x	In Country Signing CA Certificates PathLenConstraint MUST always be ‘0’
NameChange		**o**	**x**	**x**	x	See Note 5
DocumentType		**x**	**m**	**x**	x	See Note 6
NameConstraints	**4.2.1.10**	**x**	**x**	**x**	x	
PolicyConstraints	**4.2.1.11**	**x**	**x**	**x**	x	
ExtKeyUsage	**4.2.1.12**	**x**	**x**	**mc**	**mc**	
CRLDistributionPoints	**4.2.1.13**	**m**	**m**	**m**	**o**	MUST be ldap, http or https,
distributionPoint		m	m	m	m	
reasons		x	x	x	x	
cRLIssuer		x	x	x	x	
InhibitAnyPolicy	**4.2.1.14**	**x**	**x**	**x**	**x**	
FreshestCRL	**4.2.1.15**	**x**	**x**	**x**	**x**	
privateInternetExtensions	**4.2.2**	**o**	**o**	**o**	**o**	

Extension name	Section in RFC 5280	Country Signing CA	Document Signer	Master List Signer	Communication	Comments
other private extensions	**N/A**	**o**	**o**	**o**	**o**	

Note 1 - Link Certificates:
Link Certificates follow the profile for CSCA certificates.

Note 2 - Algorithms:
Refer to Doc 9303 for approved algorithms.

Note 3 – Certificate and Naming conventions
The following naming and addressing convention for Issuer and Subject fields are REQUIRED.

- country. (country codes MUST follow the format of two letter country codes, specified in ISO 3166-1: 2006, *Codes for the representation of names of countries and their subdivisions — Part 1: Country codes*)
- common name.

Other attributes MAY be used at the discretion of the issuing State.

Note 4 - AlternativeName:
AlternativeName serves two functions.

First function is to provide contact information of the subject and/or issuer of the certificate. For that purpose it SHOULD include at least one of the following:

- rfc822Name;
- dNSName;
- uniform ResourceIdentifier

Second function is to provide a directory string made of ICAO assigned country codes. For this purpose certificates issued using this profile MUST additionally include a directory name that is constructed as follows:

- localityName that contains the ICAO country code as it appears in the MRZ;
- if this country code does not uniquely define the issuing State or entity, the attribute stateOrProvinceName SHALL be used to indicate the ICAO assigned three letter code for the issuing State or entity.

Other attributes are disallowed.

Note 5 - NameChange extension:
When a CSCA key rollover occurs a certificate MUST be issued that links the new key to the old key to provide a secure transition for relying parties. Generally this is achieved through the issuance of a self-issued certificate where the issuer and subject fields are identical but the key used to verify the signature represents the old key pair and the certified public key represents the new key pair.

It is RECOMMENDED that CSCAs do not change their DN unnecessarily as there is an adverse impact on relying parties (other states must retain both the old and new names as valid CSCAs for the same state until all ePassports signed under the old name have expired). However, if a name change is necessary this can be conveyed to relying parties through the issuance of a certificate where the issuer is the old DN and the subject is the new DN. This certificate can also convey a key rollover in the same way as the self-issued certificate where the key used to verify the signature represents the old key pair and the certified public key represents the new key pair. Certificates that convey both a CSCA name change and

a key rollover for that CSCA SHOULD also include the NameChange extension to identify the certificate as such. The NameChange extension in name change certificates MUST be set to non-critical. This has no effect on PathLengthConstraint; it remains '0'.

ASN.1 for Name Change extension:

```
nameChange  EXTENSION  ::=  {
    SYNTAX           NULL
    IDENTIFIED BY    id-icao-mrtd-security-extensions-nameChange}

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}
```

Note 6 – DocumentType extension
The DocumentType extension MUST be used to indicate the document types as they appear in the MRZ that the corresponding Document Signer is allowed to produce. The extension is identified below.

ASN.1 for Document Type List extension:

```
documentTypeList  EXTENSION  ::=  {
    SYNTAX           DocumentTypeListSyntax
    IDENTIFIED BY    id-icao-mrtd-security-extensions-documentTypeList}

DocumentTypeListSyntax ::= SEQUENCE {
    version          DocumentTypeListVersion,
    docTypeList SET OF DocumentType }

DocumentTypeListVersion ::= INTEGER {v0(0)}

-- Document Type as contained in MRZ, e.g. "P" or "ID" where a
-- single letter denotes all document types starting with that letter
DocumentType ::= PrintableString(1..2)

id-icao-mrtd-security-extensions-documentTypeList OBJECT IDENTIFIER ::=
{id-icao-mrtd-security-extensions 2}
```

3.3 Backwards compatibility

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

3.4 Implementation strategy

Issuers are RECOMMENDED to start issuing certificates conforming this new profile starting at their next CSCA roll-over.

3.5 Documentation

Present documentation, affected by this change, is:

ICAO Doc 9303-Machine Readable Travel Documents, part 1-Machine Readable Passports, Volume 2-Specifications for Electronically Enabled Passports with Biometric Identification Capability, sixth edition-2006

- Normative Appendix 1 to Section IV - "Certificate Profile"

ICAO Doc 9303-Machine Readable Travel Documents, part 3-Machine Readable Official Travel Documents, Volume 2-Specifications for Electronically Enabled MRtds with Biometric Identification Capability, third edition-2008

- Normative Appendix 1 to Section IV - “Certificate Profile”

ICAO Supplement to Doc 9303, latest release

- R3-p1_v2_sIV_0038

4. Access Control

4.1 Present specification

The present access control mechanism for eMRTDs is Basic Access Control.

4.2 Revised specification

The revised access control mechanisms are described in the ICAO Technical Report `Supplemental Access Control for Machine Readable Travel Documents`.

5. Active Authentication

5.1 Present specification

ICAO Doc 9303 specifies in section IV, par. 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, par. 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 par. 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 (see issue **R7-p1_v2_sIV_0057**).

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.

5.2 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.

5.2.1 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

5.2.2 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-icao-mrtd-security-aaProtocolObject,
      version INTEGER  -- MUST be 1
      signatureAlgorithm OBJECT IDENTIFIER
}

-- 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-mrtd-security-aaProtocolObject OBJECT IDENTIFIER ::=
                                        {id-icao-mrtd-security 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.

5.2.3 HASH calculation output versus ECDSA key length

Because the calculation of the hash value from the message to be signed is part of the 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.

5.3 Backwards compatibility

n/a

5.4 Implementation strategy

n/a

5.5 Documentation

Present documentation, affected by this change, is:

ICAO Doc 9303-Machine Readable Travel Documents, part 1-Machine Readable Passports, Volume 2-Specifications for Electronically Enabled Passports with Biometric Identification Capability, sixth edition-2006

- Section IV - par. 7.2.2
- Section IV - par. 8.1
- Section IV - Normative Appendix 4

ICAO Doc 9303-Machine Readable Travel Documents, part 3-Machine Readable Official Travel Documents, Volume 2-Specifications for Electronically Enabled MRtds with Biometric Identification Capability, third edition-2008

- Section IV - par. 7.2.2
- Section IV - par. 8.1
- Section IV - Normative Appendix 4

ICAO Supplement to Doc 9303, latest release

- R7-p1_v2_sIV_0057
- R7-p3_v2_sIV_0010

6. Extended Length

6.1 Present specification

ICAO Doc 9303 currently does not contain specifications for the use of Extended Length APDUs. Specifications with respect to using Extended Length are under development within ISO/IEC JTC1 SC17 WG4.

Results of these developments will be incorporated into, or referenced in, Doc 9303 once finalized.