Machine Readable Travel Documents

GUIDANCE DOCUMENT

PKI for Machine Readable Travel Documents

Version -**1.0**
Date - 22 June, 2011

Table of Contents

1 Introduction 5

2 Structure of the document 5

3 Certificate Fields 5

3.1 Version 5

3.2 Serial Number 6

3.3 Signature 6

3.4 Issuer 6

3.5 Validity 7

3.5.1 UTCTime 7

3.5.2 GeneralizedTime 8

3.6 Subject 8

3.7 Subject Public Key Info 8

3.8 Unique Identifiers 9

3.9 Certificate Extensions 9

3.9.1 Authority Key Identifier 9

3.9.1.1 Authority Key Identifier - Document Signer/Masterlist Signer 9

3.9.2 Subject Key Identifier 9

3.9.2.1 Subject Key Identifier - Country Signing CA 10

3.9.3 Key Usage 10

3.9.3.1 Key Usage - Country Signing CA 10

3.9.3.2 Key Usage - Document Signer/Masterlist Signer 10

3.9.4 Private Key Usage Period 10

3.9.5 Certificate Policies 11

3.9.6 Policy Mappings 11

3.9.7 Subject Alternative Name 11

3.9.8 Issuer Alternative Names 11

3.9.9 Subject Directory Attributes 12

3.9.10 Basic Constraints 12

3.9.10.1 Basic Constraints - Country Signing CA 12

3.9.10.2 Basic Constraints - Document Signer/Masterlist Signer 12

3.9.11 Name Constraints 12

3.9.12 Policy Constraints 13
3.9.13 Extended Key Usage 13
3.9.13.1 Extended Key Usage - Contry Signing CA/Document Signer 13
3.9.13.2 Extended Key Usage - Master List Signer 13
3.9.14 CRL Distribution Points 14
3.9.15 Inhibit Any-Policy 14
3.9.16 Freshest CRL (a.k.a. Delta CRL Distribution Point) 14
3.9.17 Private Internet Extensions 15
3.9.18 NetScape Certificate Extensions 15
4 CRL fields 15
4.1 Version 15
4.2 Signature 16
4.3 Issuer 16
4.4 This Update 16
4.4.1 UTCTime 17
4.4.2 GeneralizedTime 17
4.5 Next Update 17
4.5.1 UTCTime 17
4.5.2 GeneralizedTime 18
4.6 Revoked Certificates 18
4.7 Extensions 18
4.7.1 Authority Key Identifier 18
4.7.2 Issuer Alternative Name 19
4.7.3 CRL Number 19
4.7.4 Delta CRL Indicator 20
4.7.5 Issuing Distribution Point 20
4.7.6 Freshest CRL (a.k.a. Delta CRL Distribution Point) 20
4.8 CRL Entry Extensions 20
4.8.1 Reason Code 20
4.8.2 Hold Instruction Code 21
4.8.3 Invalidity Date 21
4.8.4 Certificate Issuer 21
5 Master List fields 21
5.1 Content Type 21

5.2 Content 21
5.2.1 Version 21
5.2.2 Digest Algorithm 22
5.2.3 EncapsulatedContentInfo 22
5.2.3.1 eContent Type 22
5.2.3.2 eContent 23
5.2.4 Certificates 23
5.2.5 CRLs 23
5.2.6 Signer Infos 23
5.2.6.1 Version 23
5.2.6.2 Signer Identifier 23
5.2.6.3 Digest Algorithm 24
5.2.6.4 Signed Attributes 24
5.2.6.5 Signature Algorithm 24
5.2.6.6 Signature 24

1 Introduction

ICAO Doc 9303 specifies in Volume 2, Section IV, Normative Appendix 1 the certificate profiles for Country Signing CA certificates and Document Signer certificates. Additionally, ***CSCA countersigning and Master List issuance,*** Version – 1.**0,**Date – June 23, 2009 defines the profile for Master List Signer certificates and the Master List.

During the first years of operation there have been a number of changes to the ICAO PKI scheme to take into account omissions and errors in the original specification. These can be found in the current Supplement to Document 9303.

The ICAO PKI scheme is a subset of the general PKI scheme. It consists of two levels of trust. The highest level of trust is asserted by a self signed Country Signing CA certificate. The Document Signer Certificates are issued as end entity certificates. There are no intermediate certificates between the CSCA and the DS certificate. Additionally, Link certificates are used for distribution of new CSCA keys using the trust in the previous CSCA key. Link Certificates are not to be used to construct a validation path from a DSC issued by a new CSCA key to the old CSCA key. Rather, the new CSCA key is to be installed as a trust anchor in its own right and be used to verify signatures on DS certificates directly.

Keeping this in mind, the document " ICAO Doc 9303 Volume 2, Section IV, Normative Appendix 1 " defines the certificate profiles and CRL profiles fit for usage in an ICAO PKI scheme. These draw upon the underlying specifications for X.509 and Distinguished Encoding rules, with specific guidance for certain attributes for use in the ICAO PKI scheme.

It has been recognised that due to the complex nature of the PKI schemes in general and the implementation differences in various commercial toolkits, from time to time countries will create certificates that do not precisely conform to the ICAO specifications or the governing ISO and IETF RFCs. These certificates would be deemed to be “non conforming”. These non-conforming certificates are likely to create issues related to security or interoperability.

This document details the attributes of the ICAO PKI scheme and their mandated requirements. It is intended as a guide for entities that issue or validate E-Passports.

2 Structure of the document

A separate section is detailed for Certificates, CRLs and Master Lists. In each section, the attributes are defined with a reference to the underlying standards or documents governing the attribute. If there is difference between the way an attribute is treated for say a CSCA and a DSC, then these are presented separately.

3 Certificate Fields

3.1 Version

Requirement	References
Must be present and must be '3'.	RFC 5280: Section 4.1.2.1 When extensions are used, as expected in this profile, version

	MUST be 3 (value is 2).

3.2 Serial Number

Requirement	References
Must be present	RFC5280 Section 4.1.2.2
Must be Positive	RFC5280 Section 4.1.2.2 The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA (i.e., the issuer name and serial number identify a unique certificate). CAs MUST force the serialNumber to be a non-negative integer.
Must use 2's Complement Encoding	X.690 Sectrion 8.3.3 The contents octets shall be a two's complement binary number equal to the integer value, and consisting of bits 8 to 1 of the first octet, followed by bits 8 to 1 of the second octet, followed by bits 8 to 1 of each octet in turn up to and including the last octet of the contents octets.
Smallest Number of Octets Representation	X.690 Section 8.3.2 If the contents octets of an integer value encoding consist of more than one octet, then the bits of the first octet and bit 8 of the second octet: a) shall not all be ones; and b) shall not all be zero. NOTE – These rules ensure that an integer value is always encoded in the smallest possible number of octets.
Max 20 Octets	RFC 5280 Section 4.1.2.2 Given the uniqueness requirements above, serial numbers can be expected to contain long integers. Certificate users MUST be able to handle serialNumber values up to 20 octets. Conformant CAs MUST NOT use serialNumber values longer than 20 octets.

3.3 Signature

Requirement	References
Must be present	RFC 5280 Section 4.1.2.3
Match Signature Algorithm field in Certificate	RFC 5280 Section 4.1.1.2 This field MUST contain the same algorithm identifier as the signatureAlgorithm field in the sequence Certificate

3.4 Issuer

Requirement	References

Must be present	RFC 5280 Section 4.1.2.4
Country and Serial Number(SN) Must Be Printable String	RFC5280 Appendix A.1 X520countryName ::= PrintableString (SIZE (2)) X520SerialNumber ::= PrintableString (SIZE (1..ub-serial-number))
Other Than Country and SN, The Rest Must be UTF8	CAs conforming to this profile MUST use either the PrintableString or UTF8String encoding of DirectoryString,
At Least Have Country Code	The following Attributes SHOULD be used: • country. (country codes MUST follow the format of two letter country codes, specified in [R16], ISO/IEC 3166, Codes for the representation of names of countries and their subdivisions – 1997.) • organization. • organizational-unit. • common name. Additionally some countries MAY use: • serial number. *Note: The presence of Country Code is not mandated in Doc 9303, but as the Issuer field is intended to identify the issuer of the travel document, the country code must be present.*
Country Code Must Be Caps	ISO/IEC 3166 recommendation

3.5 Validity

Requirement	References
Must be present	RFC 5280: Section 4.1.2.5
Dates through 2049 Must be in UTCTime, Dates in 2050 and beyond must be in Generalised Time.	RFC 5280 Section 4.1.2.5 Both notBefore and notAfter may be encoded as UTCTime or GeneralizedTime. CAs conforming to this profile MUST always encode certificate validity dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime.

3.5.1 UTCTime

Requirement	References
Terminate With Zulu (Z)	X.690 Section 11.8.1 The encoding shall terminate with "Z", as described in the ITU-T X.680 | ISO/IEC 8824-1 clause on UTCTime.
The seconds element must be present	X.690 Section 11.8.2 The seconds element shall always be present
Must be represented as YYMMDDHHMMSSZ	x.690 Section 11.8

3.5.2 GeneralizedTime

Requirement	References
Terminate With Zulu (Z)	X.690 Section 11.7.1 The encoding shall terminate with a "Z", as described in the ITU-T Rec. X.680 | ISO/IEC 8824-1 clause on **GeneralizedTime**.
The seconds element must be present	X.690 Section 11.7.2 The seconds element shall always be present
Must not have fractional seconds	RFC 5280 Section 4.1.2.5.2 GeneralizedTime values MUST NOT include fractional seconds.
Must be represented as YYYYMMDDHHMMSSZ	RFC 5280 Section 4.1.2.5.2 For the purposes of this profile, GeneralizedTime values MUST be expressed Greenwich Mean Time (Zulu) and MUST include seconds (i.e., times are YYYYMMDDHHMMSSZ), even where the number of seconds is zero.

3.6 Subject

Requirement	References
Must be present	RFC 5280 Section 4.1.2.6
Country and Serial Number(SN) Must Be Printable String	RFC5280 Appendix A.1 X520countryName ::= PrintableString (SIZE (2)) X520SerialNumber ::= PrintableString (SIZE (1..ub-serial-number))
Other Than Country and SN, The Rest UTF8	CAs conforming to this profile MUST use either the PrintableString or UTF8String encoding of DirectoryString, .
At Least Have Country Code	The following Attributes SHOULD be used: • country. (country codes MUST follow the format of two letter country codes, specified in [R16], ISO/IEC 3166, Codes for the representation of names of countries and their subdivisions – 1997.) • organization. • organizational-unit. • common name. Additionally some countries MAY use: • serial number. *Note: The presence of Country Code is not mandated in Doc 9303, but as the subject field is intended to identify the issuer of the travel document, the country code must be present.*
Country Code Must Be Caps	ISO/IEC 3166 recommendation
Subject Country Code and Issuer Country code must match	*Note: Security consideration*

3.7 Subject Public Key Info

Requirement	References
Must be present.	RFC 5280: Section 4.1.2.7

3.8 Unique Identifiers

Requirement	References
Must not be present.	RFC 5280: Section 4.1.2.8 CAs conforming to this profile MUST NOTgenerate certificates with unique identifiers.

3.9 Certificate Extensions

Requirement	References
Must be present.	RFC 5280: Section 4.2
Default Values must not be encoded	X.690 Section 11.5 The encoding of a set value or sequence value shall not include an encoding for any component value which is equal to its default value.

3.9.1 Authority Key Identifier

Requirement	**References**
Must Not Be Critical	RFC 5280 Section 4.2.1.1
Must Have Key Identifier	ICAO Doc 9303 specifies in Volume 2, Section IV, Normative Appendix 1 If this extension is used keyIdentifier MUST be supported as a minimum

3.9.1.1 Authority Key Identifier - Document Signer/Masterlist Signer

Requirement	References
Must be present	RFC 5280 Section 4.2.1.1 The keyIdentifier field of the authorityKeyIdentifier extension MUST be included in all certificates generated by conforming CAs to facilitate certification path construction. There is one exception; where a CA distributes its public key in the form of a "self-signed" certificate, the authority key identifier MAY be omitted.

3.9.2 Subject Key Identifier

Requirement	References
Must Not Be Critical	RFC5280 Section 4.2.1.2

3.9.2.1 Subject Key Identifier - Country Signing CA

Requirement	References
Must be present	RFC 5280 Section 4.2.1.2 To facilitate certification path construction, this extension MUST appear in all conforming CA certificates, that is, all certificates including the basic constraints extension (section 4.2.1.9) where the value of cA is TRUE.

3.9.3 Key Usage

Requirement	References
Must be Present	RFC5280 Section 4.2.1.3 The usage restriction might be employed when a key that could be used for more than one operation is to be restricted.
Must Be Critial	RFC5280 Section 4.2.1.3

3.9.3.1 Key Usage - Country Signing CA

Requirement	**References**
cRLSign and keyCertSign must be asserted	The cRLSign bit is asserted when the subject public key is used for verifying a signature on certificate revocation list (e.g., a CRL, delta CRL, or an ARL). This bit MUST be asserted in certificates that are used to verify signatures on CRLs. The keyCertSign bit is asserted when the subject public key is used for verifying a signature on public key certificates..

3.9.3.2 Key Usage - Document Signer/Masterlist Signer

Requirement	**References**
digitalSignature must be asserted	The digitalSignature bit is asserted when the subject public key is used with a digital signature mechanism to support security services other than certificate signing (bit 5), or CRL signing (bit 6)....

3.9.4 Private Key Usage Period

Requirement	**References**
If present, Must Not Be Critical	RFC 3280 Section 4.2.1.4 CAs conforming to this profile MUST NOT generate certificates with private key usage period extensions unless at least one of the two components is present and the extension is non-critical.
If present, at least one of notBefore or notAfter must be present	RFC 3280 Section 4.2.1.4 CAs conforming to this profile MUST NOT generate certificates with private key usage period extensions unless at least one of the two components is present and the extension is non-critical.

notBefore and notAfter Must be encoded as generalisedTime.	RFC 3280 Section 4.2.1.4 Where used, notBefore and notAfter are represented as GeneralizedTime and MUST be specified and interpreted as defined in section 4.1.2.5.2.

3.9.5 Certificate Policies

Requirement	References
If present, Must Not Be Critical	RFC 5280 Section 4.2.1.4 If this extension is critical, the path validation software MUST be able to interpret this extension (including the optional qualifier), or MUST reject the certificate. ICAO Doc 9303 specifies in Volume 2, Section IV, Normative Appendix 1 *Note: In E-Passport scheme, Certificate Policies may be interpreted or ignored. Marking it critical forces the Certificate Policy to be interpreted or the certificate to be rejected if the policy cannot be interpreted.*

3.9.6 Policy Mappings

Requirement	References
Must not be present	RFC 5280 Section 4.2.1.5 This extension is used in CA certificates. It lists one or more pairs of OIDs; each pair includes an issuerDomainPolicy and a subjectDomainPolicy. The pairing indicates the issuing CA considers its issuerDomainPolicy equivalent to the subject CA's subjectDomainPolicy. ICAO Doc 9303 specifies in Volume 2, Section IV, Normative Appendix 1 *Note: In E-Passport scheme, there are no intermediate CAs.*

3.9.7 Subject Alternative Name

Requirement	References
Should not be present If present, Must Not Be Critical	ICAO Doc 9303 specifies in Volume 2, Section IV, Normative Appendix 1

3.9.8 Issuer Alternative Names

Requirement	References
Should not be present If present, Must Not Be Critical	ICAO Doc 9303 specifies in Volume 2, Section IV, Normative Appendix 1

3.9.9 Subject Directory Attributes

Requirement	References
Should not be present If present, Must Not Be Critical	ICAO Doc 9303 specifies in Volume 2, Section IV, Normative Appendix 1

3.9.10 Basic Constraints

3.9.10.1 Basic Constraints - Country Signing CA

Requirement	References
Must be present	RFC 5280 Section 4.2.1.9 The basic constraints extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate
Must Be Critical	RFC 5280 Section 4.2.1.9 Conforming CAs MUST include this extension in all CA certificates that contain public keys used to validate digital signatures on certificates and MUST mark the extension as critical in such certificates.
CA Bit Asserted	RFC 5280 Section 4.2.1.9 The cA boolean indicates whether the certified public key belongs to a CA. If the cA boolean is not asserted, then the keyCertSign bit in the key usage extension MUST NOT be asserted. ICAO Doc 9303 specifies in Volume 2, Section IV, Normative Appendix 1
Path Length Must Be Zero	ICAO Doc 9303 specifies in Volume 2, Section IV, Normative Appendix 1 0 for New Country Signing CA Certificate

3.9.10.2 Basic Constraints - Document Signer/Masterlist Signer

Requirement	References
Must not be present	ICAO Doc 9303 specifies in Volume 2, Section IV, Normative Appendix 1

3.9.11 Name Constraints

Requirement	References

Must Not Be Present	RFC 5280 4.2.1.10 The name constraints extension, which MUST be used only in a CAcertificate, indicates a name space within which all subject names insubsequent certificates in a certification path MUST be located. *Note: In the E-Passport model, there are no certification paths between a CA and end entity certificates. Hence, it must not be used.*

3.9.12 Policy Constraints

Requirement	References
Must Not be present	RFC 5280 Section 4.2.1.11 The policy constraints extension can be used in certificates issued to CAs. The policy constraints extension constrains path validation in two ways. It can be used to prohibit policy mapping or require that each certificate in a path contain an acceptable policy identifier. *Note:In the E-Passport model, there are no additional certificates in the certification paths between a CA and end entity certificates. Hence, it must not be used.*

3.9.13 Extended Key Usage

3.9.13.1 Extended Key Usage - Contry Signing CA/Document Signer

Requirement	References
Must Not Be Present	RFC 5280 Section 4.2.1.12 This extension indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension. *Note: There is no additional purpose other than the basic purposes defined in the key usage extension. Hence, extended Key Usage Must not be present.*

3.9.13.2 Extended Key Usage - Master List Signer

Requirement	References
Must Be Present	RFC 5280 Section 4.2.1.12 This extension indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension. *Note:The additional purpose defined is the signing of Master List.*

OID 2.23.136.1.1.3	CSCA countersigning and Master List issuance Version – 1.0 Date – June 23, 2009
Must be marked Critical	CSCA countersigning and Master List issuance Version – 1.0 Date – June 23, 2009 *Note:The Master List Signer Must only be used to sign Master Lists. It should not be used to sign Passports. Hence, this extension Must be marked critical.*

3.9.14 CRL Distribution Points

Requirement	**References**
Must Not Be Critical	RFC 2280 Section 4.2.1.13 ICAO Doc 9303 specifies in Volume 2, Section IV, Normative Appendix 1 *Note: This extension may be ignored by receiving states, and hence Must not be critical.*

3.9.15 Inhibit Any-Policy

Requirement	**References**
Must Not Be Present	RFC 5280 Section 4.2.1.14 The inhibit anyPolicy extension indicates that the special anyPolicy OID, with the value { 2 5 29 32 0 }, is not considered an explicit match for other certificate policies except when it appears in an intermediate self-issued CA certificate. The value indicates the number of additional non-self-issued certificates that may appear in the path before anyPolicy is no longer permitted. *Note: In the E-Passport model, there are no additional certificates in the certification path between a CA and end entity certificates. Hence, it must not be used*

3.9.16 Freshest CRL (a.k.a. Delta CRL Distribution Point)

Requirement	**References**

Must Not Be Present	RFC 5280 Section 4.2.1.15 The freshest CRL extension identifies how delta CRL information is obtained. *Note: E-Passport implementation does not allow the concept of Delta CRLs, and hence this extension Must not be used.*

3.9.17 Private Internet Extensions

Requirement	References
If Present, Must Not be critical	RFC 5280 Section 4.2.2 These extensions may be used to direct applications to on-line information about the issuing CA or the subject. *Note: These extensions are informational only. They may be ignored by validating entity. If they were to be marked Critical, they cannot be ignored.*

3.9.18 NetScape Certificate Extensions

Requirement	References
Must Not be Present	Netscape Certificate Management System - Administrator's guide (hosted at http://www.redhat.com/docs/manuals/cert-system/admin/app_ext.htm#15213) The Netscape Certificate Type extension can be used to limit the purposes for which a certificate can be used. It has been replaced by the X.509 v3 extensions extKeyUsage and basicConstraints. *Note: Netscape Cert Extensions are the equivalent of Extended Key Usages. The only EKU allowed in the E-Passport domain if for Master List Signer. Since EKUs are not allowed for any other purposes, so are Netscape extensions not allowed.*

4 CRL fields

4.1 Version

Requirement	References
Must be present	RFC 5280 Section 5.1.2.1
Must Be V2	RFC 5280 Section 5.1.2.1 This optional field describes the version of the encoded CRL. When extensions are used, as required by this profile, this field MUST be present and MUST specify version 2 (the integer value is 1).

4.2 Signature

Requirement	References
Mandatory	RFC 3280 Section 5.1.2.2
Match Signature Algorithm in Signature Algorithm Sequence	RFC 3280 Section 5.1.1.2 This field MUST contain the same algorithm identifier as the signature field in the sequence CertificateList

4.3 Issuer

Must be present	RFC 5280 Section 5.1.2.3
Country and Serial Number(SN) Must Be Printable String	RFC5280 Appendix A.1 X520countryName ::= PrintableString (SIZE (2)) X520SerialNumber ::= PrintableString (SIZE (1..ub-serial-number))
Other Than Country and SN, The Rest UTF8	CAs conforming to this profile MUST use either the PrintableString or UTF8String encoding of DirectoryString,
At Least Have Country Code	ICAO Doc 9303 specifies in Volume 2, Section IV, Normative Appendix 1 The following Attributes SHOULD be used: • country. (country codes MUST follow the format of two letter country codes, specified in [R16], ISO/IEC 3166, Codes for the representation of names of countries and their subdivisions – 1997.) • organization. • organizational-unit. • common name. Additionally some countries MAY use: • serial number. *Note: The presence of Country Code is not mandated in Doc 9303, but as the subject field is intended to identify the issuer of the travel document, the country code must be present.*
Country Code Must Be Caps	ISO/IEC 3166 recommendation

4.4 This Update

Requirement	References
Must be present	RFC 5280: Section 5.1.2.4
Dates through 2049 Must be in UTCTime, Dates in 2050 and beyond must be in Generalised Time.	RFC 5280 Section 5.1.2.4 CRL issuers conforming to this profile MUST encode thisUpdate as UTCTime for dates through the year 2049. CRL issuers conforming to this profile MUST encode thisUpdate as GeneralizedTime for dates in the year 2050 or later.

4.4.1 UTCTime

Requirement	References
Terminate With Zulu (Z)	X.690 Section 11.8.1 The encoding shall terminate with "Z", as described in the ITU-T X.680 | ISO/IEC 8824-1 clause on UTCTime.
The seconds element must be present	X.690 Section 11.8.2 The seconds element shall always be present
Must be represented as YYMMDDHHMMSSZ	x.690 Section 11.8

4.4.2 GeneralizedTime

Requirement	References
Terminate With Zulu (Z)	X.690 Section 11.7.1 The encoding shall terminate with a "Z", as described in the ITU-T Rec. X.680 | ISO/IEC 8824-1 clause on **GeneralizedTime**.
The seconds element must be present	X.690 Section 11.7.2 The seconds element shall always be present
Must not have fractional seconds	RFC 5280 Section 4.1.2.5.2 GeneralizedTime values MUST NOT include fractional seconds.
Must be represented as YYYYMMDDHHMMSSZ	RFC 5280 Section 4.1.2.5.2 For the purposes of this profile, GeneralizedTime values MUST be expressed Greenwich Mean Time (Zulu) and MUST include seconds (i.e., times are YYYYMMDDHHMMSSZ), even where the number of seconds is zero.

4.5 Next Update

Requirement	References
Must be present	RFC 5280: Section 5.1.2.5
Dates through 2049 Must be in UTCTime, Dates in 2050 and beyond must be in Generalised Time.	RFC 5280 Section 5.1.2.5 CRL issuers conforming to this profile MUST encode nextUpdate as UTCTime for dates through the year 2049. CRL issuers conforming to this profile MUST encode nextUpdate as GeneralizedTime for dates in the year 2050 or later.

4.5.1 UTCTime

Requirement	References
Terminate With Zulu (Z)	X.690 Section 11.8.1 The encoding shall terminate with "Z", as described in the ITU-T X.680 | ISO/IEC 8824-1 clause on UTCTime.

The seconds element must be present	X.690 Section 11.8.2 The seconds element shall always be present
Must be represented as YYMMDDHHMMSSZ	x.690 Section 11.8

4.5.2 GeneralizedTime

Requirement	References
Terminate With Zulu (Z)	X.690 Section 11.7.1 The encoding shall terminate with a "Z", as described in the ITU-T Rec. X.680 | ISO/IEC 8824-1 clause on **GeneralizedTime**.
The seconds element must be present	X.690 Section 11.7.2 The seconds element shall always be present
Must not have fractional seconds	RFC 5280 Section 4.1.2.5.2 GeneralizedTime values MUST NOT include fractional seconds.
Must be represented as YYYYMMDDHHMMSSZ	RFC 5280 Section 4.1.2.5.2 For the purposes of this profile, GeneralizedTime values MUST be expressed Greenwich Mean Time (Zulu) and MUST include seconds (i.e., times are YYYYMMDDHHMMSSZ), even where the number of seconds is zero.

4.6 Revoked Certificates

Requirement	**References**
If Present, Must not be Empty	RFC5280 Section 5.1.2.6 When there are no revoked certificates, the revoked certificates list MUST be absent. Otherwise, revoked certificates are listed by their serial numbers.

4.7 Extensions

Requirement	**References**
Must be present.	RFC 5280: Section 5.2 Conforming CRL issuers are REQUIRED to include the authority key identifier (Section 5.2.1) and the CRL number (Section 5.2.3) extensions in all CRLs issued.
Default Values must not be encoded	X.690 11.5 The encoding of a set value or sequence value shall not include an encoding for any component value which is equal to its default value.

4.7.1 Authority Key Identifier

Requirement	**References**
Must be present	RFC 5280 Section 5.2.1 Conforming CRL issuers MUST use the key identifier method, and MUST include this extension in all CRLs issued.
Must Not Be Critical	RFC 5280 Section 4.2.1.1

Must Have Key Identifier	RFC 5280 Section 5.2.1 Conforming CRL issuers MUST use the key identifier method, and MUSTinclude this extension in all CRLs issued.

4.7.2 Issuer Alternative Name

Requirement	References
If present , Must Not Be Critical	RFC 3280 Section 5.2.2 Conforming CRL issuers SHOULD mark the issuerAltName extension as non-critical.

4.7.3 CRL Number

Requirement	References
Must be present	RFC 5280 Section 5.2.3 CRL issuers conforming to this profile MUST include this extension in all CRLs and MUST mark this extension as non-critical.
Positive	RFC 5280 Section 5.2.3 CRLNumber ::= INTEGER (0..MAX)
2's Complement Encoding	X.690 Section 8.3.3 The contents octets shall be a two's complement binary number equal to the integer value, and consisting of bits 8 to 1 of the first octet, followed by bits 8 to 1 of the second octet, followed by bits 8 to 1 of each octet in turn up to and including the last octet of the contents octets.
Smallest Number of Octets Representation	X.690 Section 8.3.2 If the contents octets of an integer value encoding consist of more than one octet, then the bits of the first octet and bit 8 of the second octet: a) shall not all be ones; and b) shall not all be zero. NOTE – These rules ensure that an integer value is always encoded in the smallest possible number of octets.

Max 20 Octects	RFC 3280 Section 5.2.3 Given the requirements above, CRL numbers can be expected to contain long integers. CRL verifiers MUST be able to handle CRLNumber values up to 20 octets. Conforming CRL issuers MUST NOT use CRLNumber values longer than 20 octets.
Must Not Be Critical	RFC 5280 Section 5.2.3 CRL issuers conforming to this profile MUST include this extension in all CRLs and MUST mark this extension as non-critical.

4.7.4 Delta CRL Indicator

Requirement	References
Must Not Be Present	ICAO Doc 9303 specifies in Volume 2, Section IV, Normative Appendix 1 *Note: In E-Passport PKI scheme, all CRLs are complete CRLs.*

4.7.5 Issuing Distribution Point

Requirement	References
Must Not Be Present	RFC 5280 Section 5.2.5 The issuing distribution point is a critical CRL extension that identifies the CRL distribution point and scope for a particular CRL, and it indicates whether the CRL covers revocation for end entity certificates only, CA certificates only, attribute certificates only, *Note: In E-Passport PKI scheme, there is only one type of CRL, which includes both end entity and CA certificates.*

4.7.6 Freshest CRL (a.k.a. Delta CRL Distribution Point)

Requirement	References
Must Not Be Present	RFC 5280 Section 5.2.6 The freshest CRL extension identifies how delta CRL information for this complete CRL is obtained. *NOTE: E-Passport implementation does not allow the concept of Delta CRLs, and hence this extension Must not be used.*

4.8 CRL Entry Extensions

4.8.1 Reason Code

Requirement	References

Should not be present	ICAO Doc 9303 specifies in Volume 2, Section IV, Normative Appendix 2

4.8.2 Hold Instruction Code

Requirement	References
Should not be present l	ICAO Doc 9303 specifies in Volume 2, Section IV, Normative Appendix 2

4.8.3 Invalidity Date

Requirement	References
Should not be present	ICAO Doc 9303 specifies in Volume 2, Section IV, Normative Appendix 2

4.8.4 Certificate Issuer

Requirement	References
Must not be present	RFC 5280 Section 5.3.4 This CRL entry extension identifies the certificate issuer associated with an entry in an indirect CRL, that is, a CRL that has the indirectCRL indicator set in its issuing distribution point extension. *NOTE: In E-Passport PKI scheme, indirect CRLs are not allowed*

5 Master List fields

5.1 Content Type

Requirement	References
Must be present	RFC 3852 Section 3
Must be SignedData Type (OID 1.2.840.113549.1.7.2)	CSCA countersigning and Master List issuance Section 3.1

5.2 Content

5.2.1 Version

Requirement	References
Must be present	RFC 3852 Section 5.1

Must Be V3	RFC 3852 Section 5.1
	version is the syntax version number. The appropriate value depends on certificates, eContentType, and SignerInfo. The version MUST be assigned as follows:
	IF ((certificates is present) AND
	(any certificates with a type of other are present)) OR
	((crls is present) AND
	(any crls with a type of other are present))
	THEN version MUST be 5
	ELSE
	IF (certificates is present) AND
	(any version 2 attribute certificates are present)
	THEN version MUST be 4
	ELSE
	IF ((certificates is present) AND
	(any version 1 attribute certificates are present)) OR
	(any SignerInfo structures are version 3) OR
	(encapContentInfo eContentType is other than id-data)
	THEN version MUST be 3
	ELSE version MUST be 1

5.2.2 Digest Algorithm

Requirement	**References**
Must be present	RFC 3852 Secion 5.4 digestAlgorithms is a collection of message digest algorithm identifiers. There MAY be any number of elements in the collection, including zero. Each element identifies the message digest algorithm, along with any associated parameters, used by one or more signer. The collection is intended to list the message digest algorithms employed by all of the signers, in any order, to facilitate one-pass signature verification.

5.2.3 EncapsulatedContentInfo

5.2.3.1 eContent Type

Requirement	**References**
Must be present	RFC 3852 Section 5.2
OID id-icao cscaMasterlist	CSCA countersigning and Master List issuance Section 3.1.1

5.2.3.2 eContent

Requirement	References
Must be present	RFC 3852 Section 5.2
Corresponding CSCA Must Be Present	CSCA countersigning and Master List issuance Section 2.2.1 The Master List issuer MUST include the issuing State's CSCA certificates in the CSCA Master List.
All Content Must Be X.509 Certificates	CSCA countersigning and Master List issuance Section 3.1.1 "CSCA Master List - A signed list of CSCA certificates" - which should be X 509 certificates

5.2.4 Certificates

Requirement	References
Must be present	RFC3852 Section 5.1
Master List Signer Certificate Must Be Present	RFC3852 Section 5.1 It is intended that the set of certificates be sufficient to contain certification paths from a recognized "root" or "top-level certification authority" to all of the signers in the signerInfos field.

5.2.5 CRLs

Requirement	References
Must Not Be Present	CSCA countersigning and Master List issuance Section 3.1.1

5.2.6 Signer Infos

5.2.6.1 Version

Requirement	References
Must be present	RFC 3852 Section 5.3
If Issuer & SN Used, V=1 If Ski Used, V =3	RFC 3852 Section 5.3 If the SignerIdentifier is the CHOICE issuerAndSerialNumber, then the version MUST be 1. If the SignerIdentifier is subjectKeyIdentifier, then the version MUST be 3.

5.2.6.2 Signer Identifier

Requirement	References

Must be present	RFC 3852 Section 5.3 sid specifies the signer's certificate (and thereby the signer's public key). The signer's public key is needed by the recipient to verify the signature. SignerIdentifier provides two alternatives for specifying the signer's public key. The issuerAndSerialNumber alternative identifies the signer's certificate by the issuer's distinguished name and the certificate serial number; the subjectKeyIdentifier identifies the signer's certificate by a key identifier. When an X.509 certificate is reference, the key identifier matches the X.509 subjectKeyIdentifier extension value.

5.2.6.3 Digest Algorithm

Requirement	**References**
Must be present	RFC 3852 Section 5.3

5.2.6.4 Signed Attributes

Requirement	**References**
Must be present	CSCA countersigning and Master List issuance Section 3.1.1 RFC 3852 Section 5.3 The field is optional, but it MUST be present if the content type of the EncapsulatedContentInfo value being signed is not id-data.
Must Have Signing Time	CSCA countersigning and Master List issuance Section 3.1.1 signedAttrs MUST include signing time (ref.PKCS#9). *Note: The Master List does not have a monotonically increasing Serial Number, and the Signing time is the mechanism to identify the latest Master List.*

5.2.6.5 Signature Algorithm

Requirement	**References**
Must be present	RFC 3852 Section 5.3

5.2.6.6 Signature

Requirement	**References**
Must be present	RFC 3852 Section 5.3