Certificate attributes checked as part of Doc9303 compliance check										
				RFC3280	Doc9303		CSCA Import	Operator Terminal (DSC)	Operator Terminal (CSCA Master List Signer)	Comments
1	TBSCertificate									
1.1		Version			Must be V3		Must be V3	Must be V3	Must be V3	
1.2		Serial number		-Must be positive. -2's complement encoding -Smallest number of Octets to represent the number -Max 20 Octets			-Must be positive. -2's complement encoding -Smallest number of Octets to represent the number -Max 20 Octets	-Must be positive. -2's complement encoding -Smallest number of Octets to represent the number -Max 20 Octets	-Must be positive. -2's complement encoding -Smallest number of Octets to represent the number -Max 20 Octets	
1.3		Signature		OID should match SignatureAlgorithm field(2)			OID should match SignatureAlgorithm field(2)	OID should match SignatureAlgorithm field(2)	OID should match SignatureAlgorithm field(2)	
1.4		Issuer		-Should all be UTF8String except country and SerialNumber which will be printablestring -Country code should be ISO3166 which should be uppercase.	Must be present		Countrycode must be present	Countrycode must be present. Subject country and issuer country must match	-Countrycode must be present. -Subject country and issuer country must match	Presence of specific fields are not mandated. But if country field is not present, we cannot decide the location of the entry in the directory. So, we mandate presence of country. Currently, we do not check "C" to be in uppercase. Also, some certs are using PrintableString, which are also accepted.
1.5		Validity								
1.6			UTCTime	-If date less than 2050. -No fractional seconds. -Should end with "Zulu"			check length=13 bytes Ends with zulu	check length=13 bytes Ends with zulu	-check length=13 bytes -Ends with zulu	
1.7			GeneralizedTime	-If date more than equal to 2050. -No fractional seconds. Should end with "Zulu"			check length=15 bytes First 4 bytes must decode to 2050 or greater Ends with zulu	check length=15 bytes First 4 bytes must decode to 2050 or greater Ends with zulu	-check length=15 bytes -First 4 bytes must decode to 2050 or greater -Ends with zulu	
1.8		Subject		-Same conditions as Issuer. -If selfsigned, Issuer and Subject should match -If CA asserted, subject not equal to issuer or subjectkeyidentifier not equal to authoritykeyidentifier, assume link cert.	Must be present		Countrycode must be present. If Link, then last two levels of DN should match	Countrycode must be present. Subject country and issuer country must match	-Countrycode must be present. -Subject country and issuer country must match	We check the subject DN to make sure it is really link cert and not cross cert. This is done by comparing the last two elements of the DN, to be identical.
1.9		Subject Public Key Info					Check Presence	Check Presence	Check Presence	
1.10		Unique Identifiers		Recommended not to use	Should not use		Must not be present	Must not be present	Must not be present	
1.11		Extensions								
1.11.1			Authority Key Identifier	-If issuer and subject do not match, mandatory -Minimum should have KeyIdentifier -Must not be critical			-If issuer and subject do not match, mandatory -Minimum should have KeyIdentifier -Must not be critical	-If issuer and subject do not match, mandatory -Minimum should have KeyIdentifier -Must not be critical	-If issuer and subject do not match, mandatory -Minimum should have KeyIdentifier -Must not be critical	
1.11.2			Subject Key Identifier	-Mandatory if issuer and subject match or CA is asserted(Link cert) -Must not be critical			-Mandatory if issuer and subject match or CA is asserted(Link cert) -Must not be critical	Don't care	Don't care	
1.11.3			Key Usage	-Mandatory,Critical	-For selfsigned and link, only KeyCertSign and CRLSign -for DSC, only Digital Signature		'-For selfsigned and link, only KeyCertSign and CRLSign -Must be critical	-for DSC, only Digital Signature -Must be critical	-for DSC, only Digital Signature -Must be critical	
1.11.4			Private Key Usage Period	-Must not be critical				-if present in CSCA, must be used during verification of DSC.	-if present in CSCA, must be used during verification of DSC.	
1.11.5			Certificate Policies	-If present, policy identifier must be present -If marked critical, path validation software must be able to interpret this extension			-If present, policy identifier must be present -Must not be critical	-If present, policy identifier must be present -Must not be critical	-If present, policy identifier must be present -Must not be critical	Since, there is no consistency in the interpretation of this extension for E-Passports, we only ensure it is not marked critical

1.11.6			Policy Mappings	-Must not be critical	-Should not be present	If present, should not be marked critical	If present, should not be marked critical	If present, should not be marked critical		
1.11.7			Subject Alternative Name	-If subject is empty, should be marked critical -If present, should have non-null entries	-Should not be present	If present, should not be marked critical	If present, should not be marked critical	If present, should not be marked critical		Since Subject is Manadatory according to Doc9303, this extension if present should not be critical
1.11.8			Issuer Alternative Name	-Should not be critical	-Should not be present	If present, should not be marked critical	If present, should not be marked critical	If present, should not be marked critical		
1.11.9			Subject Directory Attributes	-Must not be marked critical	-Should not be present	If present, should not be marked critical	If present, should not be marked critical	If present, should not be marked critical		
1.11.10			Basic Constraints	-Mandatory, Critical for CSCA/Link -CA must be true for CSCA/Link -If CA not asserted, may be critical	-Pathlength must be zero	-Must be present and critical -CA must be asserted -Pathlength must be zero	-Ensure CA not asserted. No other checks	-Ensure CA not asserted. No other checks		
1.11.11			Name Constraints	-If present, critical -Not applicable if issuer=subject	-must not be used	Don't care	Don't care	Don't care		Since pathlength=0, this constraint does not matter
1.11.12			Policy Constraints		-must not be used	Don't care	Don't care	Don't care		Since pathlength=0, this constraint does not matter
1.11.13			Extended Key Usage		-must not be used	Must not be present	Must not be present	Must be present and must be critical		
1.11.14			CRL Distribution Points		-if present, not critical -Must have ICAO PKD as a distribution point	If present, should not be marked critical	If present, should not be marked critical	If present, should not be marked critical		Since, the PKD as a distribution point is not well defined, we don't check it.
1.11.15			Inhibit Any-Policy	-Must be critical	-Must not be present	Don't care	Don't care	Don't care		Since pathlength=0, this constraint does not matter
1.11.16			Freshest CRL		-Must not be present	Don't care	Don't care	Don't care		
1.11.17			Netscape Extensions			Must not be present	Must not be present	Must not be present		Netscape extensions have the same effects as EKU. Hence, they are not allowed to be present in a certificate.
		Internet Certificate Extensions			-must not be present	Don't care	Don't care	Don't care		
		Other Private extensions			-Must not be critical	Don't care	Don't care	Don't care		
2	signatureAlgorithm			-Must match 1.3		-Must match 1.3	-Must match 1.3	-Must match 1.3		

CRL attributes checked as part of Doc9303 compliance check

					RFC3280	Doc9303		Operator Terminal	Comments
1	TBS Cert List								
1.1		Version			MUST be v2	MUST be v2		MUST be v2	
1.2		Signature			OID should match SignatureAlgorithm field(2)	Must be present			
1.3		Issuer			-Should all be UTF8String except country and SerialNumber which will be printablestring -Country code should be ISO3166 which should be uppercase.	UTF8 Encoding. Must be present		Countrycode must be present.	We do not enforce UTF8 checking, as many countries are still using printablestring.
1.4		This Update				Must be present			
1.4.1			UTCTime		-If date less than 2050. -No fractional seconds. -Should end with "Zulu"	check length=13 bytes Ends with zulu		-check length=13 bytes -Ends with zulu	
1.4.2			GeneralizedTime		-If date more than equal to 2050. -No fractional seconds. Should end with "Zulu"	check length=15 bytes First 4 bytes must decode to 2050 or greater Ends with zulu		-check length=15 bytes -First 4 bytes must decode to 2050 or greater -Ends with zulu	
1.5		Next Update				Must be present			
1.5.1			UTCTime		-If date less than 2050. -No fractional seconds. -Should end with "Zulu"	check length=13 bytes Ends with zulu		-check length=13 bytes -Ends with zulu	
1.5.2			GeneralizedTime		-If date more than equal to 2050. -No fractional seconds. Should end with "Zulu"	check length=15 bytes First 4 bytes must decode to 2050 or greater Ends with zulu		-check length=15 bytes -First 4 bytes must decode to 2050 or greater -Ends with zulu	
1.6		Revoked Certificates			When there are no revoked certificates, the revoked certificates list MUST be absent. The date on which the revocation occurred is specified. DateTime follow format of This Update	Must be present		If present, must not be empty.	
1.7		Extensions				Must be present			
1.7.1			Authority Key Identifier		-If issuer and subject do not match, mandatory -Should have KeyIdentifier at minimum -Must not be critical	Must be present		-Must be present -Should have KeyIdentifier at minimum	
1.7.2			Issuer Alternative Name		-Should not be critical	Must not be present		If present, must not be critical.	
1.7.3			CRL Number		-Contains long integers. -CRL verifiers MUST be able to handle CRLNumber values up to 20 octets. -Conformant CRL issuers MUST NOT use CRLNumber values longer than 20 octets.	Must be present		-Must be present. -2's complement encoding -Smallest number of Octets to represent the number -Max 20 Octets.	
1.7.4			Delta CRL Indicator			Must not be present		Must not be present	
1.7.5			Issuing Distributing Pt			Must not be present		Must not be present	
1.7.6			Freshest CRL			Must not be present		Must not be present	
1.8		CRL Entry Extension							
1.8.1			Reason Code			Must not be present		If present, must not be critical.	
1.8.2			Hold Instruction Code			Must not be present		If present, must not be critical.	
1.8.3			Invalidity Date			Must not be present		If present, must not be critical. Should end with "Zulu"	
1.8.4			Certificate Issuer			Must not be present		Must not be present	
2	signatureAlgorithm				-Must match 1.2			-Must match 1.2	
3	signature								

CSCA Master List attributes checked as part of Doc9303 compliance check

					RFC3852	Doc9303		Operator Terminal	Comments
1	Signed Data								
1.1		Version			Dependent on content of Signed Data	MUST be v3		MUST be v3	
1.2		digest Algorithm			A collection of disgest Algorithm	Must be present		Must be present	
1.3		encap Content Info							
1.3.1			eContent Type			id-icao-cscaMasterList		id-icao-cscaMasterList	
1.3.2			eContent					Corresponding CSCA to masterlist signer must be present	
1.4		Certificates			Collection of certs that is sufficient to contain certification path from recognised 'root' to all signers	Master List Signer Cert must be included		-Master List Signer Cert must be included -Check signer for Doc9303 compliance as define in CSCA_DSC. -If extended key usage is present, must be critical and oid = 2.23.136.1.1.3	
1.5		crls				Must not be present		Must not be present	
1.6		signer Infos				Must be present		Must be present	
1.7	Signer Info								
1.7.1		Version			If issuer&SerialNumber used value = 1 if subjectkeyidentifier used value = 3	If issuer&SerialNumber used value = 1 if subjectkeyidentifier used value = 3		If issuer&SerialNumber used value = 1 if subjectkeyidentifier used value = 3	
1.7.2		SID			Dependent on version number If 1 refer to issuer&SerialNumber if 3 refer to subjectkeyidentifier	Dependent on version number If 1 refer to issuer&SerialNumber if 3 refer to subjectkeyidentifier		Dependent on version number If 1 refer to issuer&SerialNumber if 3 refer to subjectkeyidentifier	
1.7.2.1			Subject Key Identifier						
1.7.3		disgest Algorithm			Must be one of those listed in Signed Data disgest algorithm	Must be present		Must be present	
1.7.4		signed Attr				Must be present. Must have signing time		Must be present. Must have signing time	
1.7.5		signature Algorithm				Must be present		Must be present	
1.7.6		signature				Must be present		Must be present	
1.7.7		unsigned Attrs				ignore		ignore	