MACHINE READABLE TRAVEL DOCUMENTS TECHNICAL REPORT

RF PROTOCOL AND APPLICATION TEST STANDARD FOR EMRTD - PART 5

TESTS FOR PKI OBJECTS

Version – 2.00 | August 2022

ISO/IEC JTC 1/SC 17/WG 3/TF 4

FOR THE INTERNATIONAL CIVIL AVIATION ORGANIZATION

Release Control

Release	Date	Description
0.20	March 2, 2017	Initial draft for discussion in the 54th WG3 meeting, Veridos
0.30	August 11, 2017	Draft for internal review, Veridos
0.40	September 5, 2017	Draft for review by ISO/IEC JTC 1 / SC 17 / WG3, Veridos • Considered results of the discussion in the 54th WG3 meeting • Considered Auctorizium and Secunet comments • Added further details for subjectPublicKeyInfo, CRLDistributionPoints, signatureAlgorithm, revokedCertificates, SignedAttributes
0.50	December 18, 2017	Draft considering the outcome of the discussion in the 55th WG3 Meeting, Veridos • Clarified all open questions and IDEMIA comments • Anticipated clarifications and changes in Doc9303-12; notes in the test specification indicate these clarifications and changes
0.51	January 17, 2018	Internal review, Veridos • Added editorial note in clause 2
1.00 RC1	March 15, 2018	Resolved the editorial note in clause 2 concerning compliant test suite implementations as discussed in the Tokyo TF5 meeting.
1.00 RC2	March 20, 2018	Resolved Auctorizium comments
1.10	April 20, 2022	Work in progress • Updated to ICAO Doc9303 8th Edition • Added test cases for VDS-NC Signer certificates, Trust List Signer certificates, the separate CA certificate, and the Trust List • Added test cases for DTC Signer certificates
1.20	August 05, 2022	Draft for review: • Added test cases for SPOC certificates • Considered outcome of July 2022 WG 3/TF 5 meeting: BCS signer certificates support only ECDSA
2.00	August 05, 2022	Changed version to 2.00 for publication

Table of contents

1 Introduction

1.1 Scope

[Doc9303-12] of ICAO specifies the Public Key Infrastructure (PKI) for Machine Readable Travel Documents including certificates, Certification Revocation Lists (CRLs) and Master Lists. The 8th Edition of Doc9303 is amended by

- the ICAO Technical Report [TR DTC] which specifies the PKI for the Digital Travel Credentials (DTC) in particular the DTC Signer certificate and
- the Technical Reports [TR VDS-NC] and [TR DTA] which specify the PKI for the Visible Digital Seals for non-constrained environments, in particular the Signer certificates, a separate CA certificate, and a Trust List.

This specification stipulates test cases for X.509v3 certificates, CRLs, Master Lists, Deviation Lists and Trust Lists according to the Doc9303 8th edition specifications including the ICAO Technical Reports that amend Doc9303. The following topics are out of the scope of this version of the test specification:

- Doc9303 7th and 6th edition
- Non-mandatory PKI requirements such as recommendations
- Tests that require all or the latest certificates, CRLs, Master Lists or Deviation Lists issued by a state or organization, e.g.
    - Tests that the serial number of a certificate issued by a given CSCA is unique
    - Test that the latest CSCA key has been used to sign the CRL of the state or organization
- The details of the `DeviationList` sequence in Deviation Lists [Doc9303-3], i.e. the encoding of categories of deviations and corresponding parameters.

1.2 Terminology

The key words “MUST”, “SHALL”, “REQUIRED”, “SHOULD”, “RECOMMENDED”, and “MAY” in this document are to be interpreted as described in [RFC2119].

MUST — This word, or the terms “REQUIRED” or “SHALL”, mean that the definition is an absolute requirement of the specification.

MUST NOT — This phrase, or the phrase “SHALL NOT”, mean that the definition is an absolute prohibition of the specification.

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

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

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

implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

1.3 Abbreviations

Abbreviation	
ASN.1	Abstract Syntax Notation One
CA	Certification Authority
CRL	Certificate Revocation List
CSCA	Country Signing Certification Authority
DER	Distinguished Encoding Rules
DSA	Digital Signature Algorithm
DTA	Digital Travel Authorization
DTC	Digital Travel Credential
ECDSA	Elliptic Curve DSA
ICAO	International Civil Aviation Organization
LDS2	Logical Data Structure version 2
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
OID	Object Identifier
PKI	Public Key Infrastructure
RSA	Rivest, Shamir and Adleman
SPOC	Single Point of Contact
TR	Technical Report
URI	Uniform Resource Identifier
VDS-NC	Visible Digital Seal for Non Constrained environments

1.4 Reference documentation

The following documentation served as reference for this technical report:

[Doc9303-3]	ICAO Doc 9303 Machine Readable Travel Documents, Eight Edition 2021, Part 3: Specifications Common to all MRTDs
[Doc9303-12]	ICAO Doc 9303 Machine Readable Travel Documents, Eight Edition 2021, Part 12: Public Key Infrastructure for MRTDs
[FIPS 186-4]	FIPS 186-4, Federal Information Processing Standards Publication, Digital Signature Standard (DSS), July 2013
[ISO/IEC 15946-1]	ISO/IEC 15946: 2002, Information technology — Security techniques — Cryptographic techniques based on elliptic curves: Part 1: General
[RFC2119]	S. Bradner, RFC 2119 Key words for use in RFCs to Indicate Requirement Levels, March 1997
[RFC3852]	R. Housley, RFC 3852 Cryptographic Message Syntax (CMS), July 2004
[RFC4055]	J. Schaad, B. Kaliski, R. Housley, RFC4055 Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, June 2005
[RFC4056]	J. Schaad, RFC4056 Use of the RSASSA-PSS Signature Algorithm

	in Cryptographic Message Syntax (CMS), June 2005
[RFC5246]	T. Dierks, E. Rescorla, RFC5246 The Transport Layer Security (TLS) Protocol Version 1.2, August 2008
[RFC5280]	D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008
[RFC5652]	R. Housley, RFC 5652 Cryptographic Message Syntax (CMS), September 2009
[RFC5754]	S. Turner, RFC 5754 Using SHA2 Algorithms with Cryptographic Message Syntax, January 2010
[RFC5758]	Q. Dang, S. Santesson, K. Moriarty, D. Brown, T. Polk, RFC5758 Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA, January 2010
[SP 800-89]	NIST Special Publication 800-89 Recommendation for Obtaining Assurances for Digital Signature Applications, November 2006
[TR VDS]	ICAO Technical Report Visible Digital Seals for Non-Electronic Documents – Visa, Version 1.1, July 24th, 2015
[TR DTA]	ICAO Technical Report Digital Travel Authorizations, Version 2.15, June 2021
[TR DTC]	ICAO Technical Report Digital Travel Credentials (DTC), Virtual Component Data Structure and PKI Mechanisms, Version 1.2, October 2020
[TR VDS-NC]	ICAO Technical Report Visible Digital Seals for non-constrained environments, Version 1.4, May 27, 2022
[X9.62]	X9.62, Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 7 January 1999

2 General test requirements

The test cases describe the comparison

- of a component of a given certificate, CRL, Master List or Deviation List with the mandatory requirements for this component
- of different components of a given certificate, CRL, Master List or Deviation List according to the mandatory requirements, e.g. the `subject` and `issuer` component of a CSCA Root certificate
- of a component of a given certificate, CRL, Master List or Deviation List with the component of another certificate, CRL, Master List or Deviation List according to the mandatory requirements, e.g. the `issuer` component of a Document Signer certificate with the `subject` component of the issuing CSCA Root certificate.

The test cases verify that the components follow the specified ASN.1 syntax, but this is not explicitly mentioned in the test case description. If the test object does not follow the specified ASN.1 syntax, the corresponding test case execution shall return an error. The test cases describe how to test the requirements specified in Doc9303 even if these requirements are already covered by the specified ASN.1 syntax.
A test suite implementation that is compliant to this Technical Report must implement all test cases as specified in this Technical Report. Please note that PKI test suites seem to be already available which implement tests based on the [Doc9303-12] (and [Doc9303-3]) requirements. While these test suites do not follow the structure of the test cases as specified in this Technical Report, these test suites implement more or less the same tests, but in a different way, i.e. using different test cases.

2.1 Profiles

The profile denotes the type of object to be tested.

Profile	Explanation
BCS	Bar Code Signer certificate
CA-VDS-NC	CA certificate other than the CSCA certificate used to issue barcode signer certificates for the VDS-NC format.
COMM	Communication Certificate
CRL	Certificate Revocation List
CSCA-Root	CSCA Root certificate (this does not comprise CSCA Link certificates)
CSCA-Root-New	CSCA Root certificate after CSCA key rollover
CSCA-Link	CSCA Link certificate
DL	Deviation List
DLS	Deviation List Signer certificate
DS	Document Signer certificate
DTA-S	DTA Signer certificate
DTC-S	DTC Signer certifiacte
LDS2-B	LDS2 Biometrics Signer certificate
LDS2-TS	LDS2 Travel Stamp Signer certificate
LDS2-V	LDS2 Visa Signer certificate
ML	Master List
MLS	Master List Signer certificate
PoR-S	Proof of Recovery Signer certificate

Profile	Explanation
PoT-S	Proof of Test Signer certificate
PoV-S	Proof of Vaccination Signer certificate
SPOC-C	SPOC Client Certificate
SPOC-CA	SPOC CA Certificate; this profile denotes a CA certificate different from the CSCA Root certificate which issues SPOC Client and / or SPOC Server certificates
SPOC-S	SPOC Server Certificate
TL	Trust List
TL-S	Trust List Signer certificate

Table 1 Profiles

The CSCA-Root-New profile is only used for the `NameChange` extension test cases. All test cases for the CSCA-Root Profile must also be executed for the CSCA-Root-New profile.

2.2 Assumptions

The test specification assumes that some common ASN.1 data types are well known. Based on this assumption it is clear how to verify that a component of a given certificate etc. follows the ASN.1 syntax of such a common data type.
Examples:
The data type `PrintableString` is well known. If Doc9303 requires that a component (such as a `countryName`) MUST be of type `PrintableString`, the test specification makes use of the test scenario: "The `countryName` MUST be a `PrintableString`." The test specification does not provide further information how to test whether the component is a `PrintableString` or not.

2.3 Preconditions

Preconditions in test cases serve two purposes:

- Preconditions specify optional components that must be present to execute the test case, e.g. "the optional `SubjectKeyIdentifier` extension is present in the certificate".
- Preconditions specify test cases that must be passed successfully to execute the test case, e.g. "The certificate has passed the test case CERT_SKI_1 successfully".

2.4 Information required

Table 2 lists the information required for the test execution for the different profiles.

Profile	Information required
BCS	Profile, see Table 1 Issuing CSCA Root certificate Name of issuing state or organization
CA-VDS-NC	Profile, see Table 1 Name of issuing state or organization
CSCA-Root	Profile, see Table 1 Name of issuing state or organization
CSCA-Root-New	Profile, see Table 1 The corresponding CSCA Link certificate The corresponding old CSCA Root certificate Name of issuing state or organization

Profile	Information required
CSCA-Link	Profile, see Table 1 Issuing CSCA Root certificate New CSCA Root certificate Name of issuing state or organization
COMM	Profile, see Table 1 Issuing CSCA Root certificate Name of issuing state or organization
DLS	Profile, see Table 1 Issuing CSCA Root certificate Name of issuing state or organization
DS	Profile, see Table 1 Issuing CSCA Root certificate Name of issuing state or organization
DTA-S	Profile, see Table 1 Issuing CSCA Root certificate certificate Name of issuing state or organization
LDS2-B	Profile, see Table 1 Issuing CSCA Root certificate Name of issuing state or organization
LDS2-TS	Profile, see Table 1 Issuing CSCA Root certificate Name of issuing state or organization
LDS2-V	Profile, see Table 1 Issuing CSCA Root certificate Name of issuing state or organization
MLS	Profile, see Table 1 Issuing CSCA Root certificate Name of issuing state or organization
PoR-S	Profile, see Table 1 Issuing CSCA Root certificate or issuing CA-VDS-NC certificate Name of issuing state or organization
PoT-S	Profile, see Table 1 Issuing CSCA Root certificate or issuing CA-VDS-NC certificate Name of issuing state or organization
PoV-S	Profile, see Table 1 Issuing CSCA Root certificate or issuing CA-VDS-NC certificate Name of issuing state or organization
SPOC-C	Profile, see Table 1 Information whether the certificate is issued by a CSCA Root or a SPOC CA Issuing CSCA Root certificate or SPOC CA certificate Name of issuing state or organization
SPOC-CA	Profile, see Table 1
SPOC-S	Profile, see Table 1

Profile	Information required
	Information whether the certificate is issued by a CSCA Root or a SPOC CA Issuing CSCA Root certificate or SPOC CA certificate Name of issuing state or organization Host part of the SPOC URL
TL-S	Profile, see Table 1 Issuing CSCA Root certificate Name of issuing state or organization
CRL	Profile, see Table 1 Issuing CSCA Root certificate
ML	Profile, see Table 1
DL	Profile, see Table 1 Issuing CSCA Root certificate
TL	Profile, see Table 1 Issuing CSCA Root certificate

Table 2 Information required for test execution

3 Certificate Tests

This clause covers all tests for certificates including their extensions. All tests for a given profile are mandatory, i.e. a certificate of that profile must pass these test cases successfully, unless marked as optional or conditional.

3.1 Certificate

Test-ID	CERT_CERT_1
Purpose	Verify that the certificate has an ASN.1 structure and is DER encoded.
Version	0.40
References	[Doc9303-12] clause 7 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	-
Test scenario	Verify the following properties: 1. The certificate MUST be DER encoded. 2. The certificate MUST have an ASN.1 structure. (Note: This test case does not require that the certificate follows the specified ASN.1 schema.)
Expected results	1. True 2. True

Test-ID	CERT_CERT_2
Purpose	Verify that the structure of the certificate is in conformance with the ICAO specifications.
Version	0.40
References	[Doc9303-12] Table 5 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_CERT_1 successfully.
Test scenario	Verify the following properties: 1. The `Certificate` sequence MUST contain the `tbsCertificate` field. 2. The `Certificate` sequence MUST contain the `signatureAlgorithm` field. 3. The `Certificate` sequence MUST contain the `signatureValue` field.
Expected results	1. True 2. True 3. True

Test-ID	CERT_CERT_3
Purpose	Verify that the certificate complies with the size restrictions imposed by the EF.Certificates file.
Version	1.10
References	[Doc9303-10] Table 83
Profile	LDS2-B, LDS2-TS, LDS2-V

Preconditions	1. The certificate has passed the test case CERT_CERT_1 successfully.
Test scenario	Verify the following properties: 1. The certificate size MUST be 900 bytes or less.
Expected results	1. True

3.2 signatureAlgorithm

Test-ID	CERT_ALG_1
Purpose	Verify that the `signatureAlgorithm` value is in conformance with Doc9303-12.
Version	0.40
References	[Doc9303-12] clause 4.1.6 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2 [RFC4055] clauses 3, 3.1, and 5 [RFC5758] clause 3.1 and 3.2
Profile	CSCA-Root, CSCA-Link, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S
Preconditions	1. The certificate has passed the test case CERT_CERT_2 successfully.
Test scenario	See clause 7.1.
Expected results	See clause 7.1.

For the profile CSCA-Root the test case CERT_ALG_2 is conditional. A CSCA Root certificate must pass this test case successfully if precondition 2 and 3 are fullfiled.

Test-ID	CERT_ALG_2
Purpose	In case of RSASSA-PSS verify that the `signatureAlgorithm` parameters match the parameters of the corresponding public key.
Version	0.30
References	[RFC4055] clause 3.3
Profile	CSCA-Root
Preconditions	1. The certificate has passed the test case CERT_ALG_1 successfully. 2. The certificate has passed the test case CERT_RSA_2 successfully. 3. The parameters are present in `subjectPublicKeyInfo`.
Test scenario	Verify the following properties: 1. The `hashAlgorithm` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST match the `hashAlgorithm` in the certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`. 2. The `maskGenAlgorithm` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST match the `maskGenAlgorithm` in the certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`. 3. The `saltLength` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST be greater or equal than the `saltLength` value in the certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`. 4. The `trailerField` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST match the `trailerField` in the certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`, i.e. MUST be absent.
Expected results	1. True 2. True

	3. True 4. True

For the profiles CSCA-Link, DS, MLS, DLS, TL-S, COMM, LDS2-B, LDS2-TS, LDS2-V, PoR-S, PoT-S, PoV-S, DTA-S, BCS, and DTC-S the test case CERT_ALG_3 is conditional. Such a certificate must pass this test case successfully if precondition 2 and 3 are fullfiled.

Test-ID	CERT_ALG_3
Purpose	In case of RSASSA-PSS verify that the `signatureAlgorithm` parameters match the parameters of the corresponding public key.
Version	0.30
References	[RFC4055] clause 3.3
Profile	CSCA-Link, DS, MLS, DLS, TL-S COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S
Preconditions	1. The certificate has passed the test case CERT_ALG_1 successfully. 2. The issuing CSCA Root certificate has passed the test case CERT_RSA_2 successfully. 3. The parameters are present in the issuing CSCA Root certificate's `subjectPublicKeyInfo`.
Test scenario	Verify the following properties: 1. The `hashAlgorithm` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST match the `hashAlgorithm` in the issuing CSCA Root certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`. 2. The `maskGenAlgorithm` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST match the `maskGenAlgorithm` in the issuing CSCA Root certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`. 3. The `saltLength` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST be greater or equal than the `saltLength` value in the issuing CSCA Root certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`. 4. The `trailerField` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST match the `trailerField` in the issuing CSCA Root certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`, i.e. MUST be absent.
Expected results	1. True 2. True 3. True 4. True

Test-ID	CERT_ALG_4
Purpose	Verify that the `signatureAlgorithm` value is in conformance with the ICAO specifications.
Version	1.10
References	[Doc9303-12] clause 4.1.6 [TR VDS-NC] clause 3.6 [RFC5758] clause 3.2
Profile	CA-VDS-NC
Preconditions	1. The certificate has passed the test case CERT_CERT_2 successfully.
Test scenario	Verify the following properties:

	1. The `algorithm` in the `AlgorithmIdentifier` sequence MUST contain one of the OIDs listed in Table 7. 2. The `parameters` field MUST be absent.
Expected results	1. True 2. True

Test-ID	CERT_ALG_5
Purpose	Verify that the `signatureAlgorithm` value is in conformance with Doc9303-12.
Version	1.20
References	[Doc9303-12] clause 4.1.6 [RFC4055] clauses 3, 3.1, and 5 [RFC5758] clause 3.1 and 3.2
Profile	SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_CERT_2 successfully. 2. The issuing certificate is the CSCA-Root certificate.
Test scenario	See clause 7.1.
Expected results	See clause 7.1.

3.3 signatureValue

Test-ID	CERT_SIGV_1
Purpose	Verify the cryptographic signature of the certificate
Version	0.40
References	[Doc9303-12] Table 5
Profile	CSCA-Root
Preconditions	1. The certificate has passed the test case CERT_CERT_2 successfully. 2. The certificate has passed the test case CERT_PKI_2 successfully. 3. The certificate has passed the relevant test cases from clause 3.10.1, 3.10.2, or 3.10.3.
Test scenario	1. Verify the signature over the certificate using the signature from the certificate's `signatureValue` field the algorithm from the certificate's `signatureAlgorithm` field and the public key from the certificate's `subjectPublicKeyInfo` field the corresponding public key parameters. The signature MUST be valid.
Expected results	1. True

Test-ID	CERT_SIGV_2
Purpose	Verify the cryptographic signature of the certificate.
Version	1.10
References	[Doc9303-12] Table 5 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2
Profile	CSCA-Link, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_CERT_2 successfully. 2. The issuing Root certificate has passed the test case CERT_SIGV_1 or CERT_SIGV_3 successfully.

Test scenario	1. Verify the signature over the certificate using the signature from the certificate's `signatureValue` field the algorithm from the certificate's `signatureAlgorithm` field and the public key from the issuing Root certificate's `subjectPublicKeyInfo` field the corresponding public key parameters. The signature MUST be valid.
Expected results	1. True

Note: Test case CERT_SIGV_2 does not apply to SPOC Client and SPOC Server certificates issued by a SPOC CA.

Test-ID	CERT_SIGV_3
Purpose	Verify the cryptographic signature of the certificate
Version	1.10
References	[TR VDS-NC] clause 3.6
Profile	CA-VDS-NC
Preconditions	1. The certificate has passed the test case CERT_CERT_2 successfully. 2. The certificate has passed the test case CERT_PKI_3 successfully. 3. The certificate has passed the relevant test cases from clause 3.10.2.
Test scenario	1. Verify the signature over the certificate using the signature from the certificate's `signatureValue` field the algorithm from the certificate's `signatureAlgorithm` field and the public key from the certificate's `subjectPublicKeyInfo` field the corresponding public key parameters. The signature MUST be valid.
Expected results	1. True

3.4 version

Test-ID	CERT_VER_1
Purpose	Verify that the `version` field is present in `tbsCertificate`.
Version	0.40
References	[Doc9303-12] Table 5 and clause 7 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_CERT_2 successfully.
Test scenario	Verify the following properties: 1. The `tbsCertificate` sequence MUST contain the `version` field.
Expected results	1. True

Test-ID	CERT_VER_2
Purpose	Verify that the `version` value is in conformance with Doc9303-12.
Version	0.20
References	[Doc9303-12] Table 5 and clause 7 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM

	LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_VER_1 successfully.
Test scenario	Verify the following properties: 1. The `version` value MUST be `v3`.
Expected results	1. True

3.5 serialNumber

Test-ID	CERT_SER_1
Purpose	Verify that the `serialNumber` field is present in `tbsCertificate`.
Version	0.40
References	[Doc9303-12] Table 5 and clause 7 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_CERT_2 successfully.
Test scenario	Verify the following properties: 1. The `tbsCertificate` sequence MUST contain the `serialNumber` field.
Expected results	1. True

Test-ID	CERT_SER_2
Purpose	Verify that the `serialNumber` value is in conformance with Doc9303-12.
Version	0.40
References	[Doc9303-12] Table 5 and clause 7 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_SER_1 successfully.
Test scenario	Verify the following properties: 1. MUST be positive integer. 2. MUST be maximum 20 octets. 3. MUST be represented in the smallest number of octets.
Expected results	1. True 2. True 3. True

Note: The Doc9303-12 Table 5 requirement “MUST use 2’s complement encoding” is implicitly tested.

3.6 signature

Test-ID	CERT_SIG_1
Purpose	Verify that the `signature` field is present in `tbsCertificate`.
Version	0.40
References	[Doc9303-12] Table 5 and clause 7 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_CERT_2 successfully.
Test scenario	Verify the following properties: 1. The `tbsCertificate` sequence MUST contain the `signature` field.
Expected results	1. True

Test-ID	CERT_SIG_2
Purpose	Verify that the `signature` field is in accordance with the `signatureAlgorithm` field in the sequence `Certificate`.
Version	0.20
References	[Doc9303-12] Table 5 and clause 7 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_SIG_1 successfully.
Test scenario	Verify the following properties: 1. The `signature` field MUST contain the same algorithm identifier as the `signatureAlgorithm` field in the sequence `Certificate`.
Expected results	1. True

3.7 issuer

Test-ID	CERT_ISS_1
Purpose	Verify that the `issuer` field is present in `tbsCertificate`.
Version	0.40
References	[Doc9303-12] Table 5 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2 [RFC5280] clause 4.1.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_CERT_2 successfully.
Test scenario	Verify the following properties: 1. The `tbsCertificate` sequence MUST contain the `issuer` field.
Expected results	1. True

Test-ID	CERT_ISS_2
Purpose	Verify that the `issuer` field is in conformance with Doc9303-12.
Version	1.10
References	[Doc9303-12] Table 5 and clause 7.1.1.1 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_ISS_1 successfully.
Test scenario	Verify the following properties: 1. The `countryName` MUST be present. 2. The `countryName` value contains a code that MUST follow the format of two-letter codes, specified in [Doc9303-3]. 3. The `countryName` MUST be upper case. 4. The `countryName` MUST be a `PrintableString`. 5. The `commonName` MUST be present. 6. Other attributes that have `DirectoryString` syntax, if present, MUST be either `PrintableString` or `UTF8String`. 7. The `serialNumber`, if present, MUST be `PrintableString`.
Expected results	1. True 2. True 3. True 4. True 5. True 6. True 7. True

Test-ID	CERT_ISS_3
Purpose	Verify that the `issuer` and the `subject` values of a Root CA certificate match.
Version	0.40
References	[Doc9303-12] Table 5 and clause 7 [TR VDS-NC] clause 3.6
Profile	CSCA-Root, CA-VDS-NC SPOC-CA
Preconditions	1. The certificate has passed the test case CERT_ISS_1 successfully. 2. The certificate has passed the test case CERT_SUB_1 successfully.
Test scenario	Verify the following properties: 1. The `issuer` value MUST exactly match the `subject` value.
Expected results	1. True

Test-ID	CERT_ISS_4
Purpose	Verify that the country code belongs to the issuing state or organization.
Version	1.10
References	[Doc9303-12] Table 5 and clause 7.1.1.1 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS

	DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_ISS_1 successfully.
Test scenario	Verify the following properties: 1. The country code in the certificate's `issuer` field MUST be identical to the [Doc9303-3] two letter code of the specified issuing state or organization.
Expected results	1. True

Test-ID	CERT_ISS_5
Purpose	Verify that the certificate's `issuer` matches the `subject` of the issuing Root certificate.
Version	1.10
References	[RFC5280] clause 4.1.2.4
Profile	CSCA-Link, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_ISS_1 successfully. 2. The issuing Root certificate has passed the test case CERT_SUB_1 successfully.
Test scenario	Verify the following properties: 1. The certificate's `issuer` value MUST exactly match the `subject` value of the issuing Root certificate.
Expected results	1. True

3.8 validity

Test-ID	CERT_VAL_1
Purpose	Verify that the `validity` field is present in `tbsCertificate`.
Version	0.40
References	[Doc9303-12] Table 5 and clause 7 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_CERT_2 successfully.
Test scenario	Verify the following properties: 1. The `tbsCertificate` sequence MUST contain the `validity` field.
Expected results	1. True

Test-ID	CERT_VAL_2
Purpose	Verify that the `validity` field is in conformance with Doc9303-12.
Version	0.40
References	[Doc9303-12] Table 5 and clause 7 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2 [RFC5280] clause 4.1.2.5
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V

	PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_VAL_1 successfully.
Test scenario	Verify the following properties for the `notBefore` and `notAfter` components of the `validity`: See clause 7.2
Expected results	See clause 7.2

Test-ID	CERT_VAL_3
Purpose	Verify that the Root certificate's validity period includes the validity period of the issued certificate.
Version	1.10
References	[RFC5280] clause 6.1
Profile	CSCA-Link, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_VAL_1 successfully. 2. The issuing Root certificate has passed the test case CERT_VAL_1 successfully.
Test scenario	Verify the following properties: 1. The validity period of the certificate must not begin before the validity period of the issuing Root certificate, i.e. the certificate's `validity notBefore` date MUST be equal to or after the issuing Root certificate's `validity notBefore` date. 2. The validity period of the certificate must not exceed beyond the validity period of the issuing Root certificate, i.e. the certificate's `validity notAfter` date MUST be equal to or before the issuing Root certificate's `validity notAfter` date.
Expected results	1. True 2. True

3.9 subject

Test-ID	CERT_SUB_1
Purpose	Verify that the `subject` field is present in `tbsCertificate`.
Version	0.40
References	[Doc9303-12] Table 5 and clause 7 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2 [RFC5280] clause 4.1.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_CERT_2 successfully.
Test scenario	Verify the following properties: 1. The `tbsCertificate` sequence MUST contain the `subject` field.
Expected results	1. True

Test-ID	CERT_SUB_2
Purpose	Verify that the `subject` field is in conformance with Doc9303-12.
Version	1.10
References	[Doc9303-12] Table 5 and clause 7.1.1.1 [TR VDS-NC] clause 3.6
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM
Preconditions	1. The certificate has passed the test case CERT_SUB_1 successfully. 2. The certificate has passed the test case CERT_ISS_1 successfully.
Test scenario	Verify the following properties: 1. The `countryName` MUST be present. 2. The `countryName` MUST use the [Doc9303-3] two letter code as value. 3. The `countryName` MUST be upper case. 4. The `countryName` MUST be a `PrintableString`. 5. The `commonName` MUST be present. 6. Other attributes that have `DirectoryString` syntax, if present, MUST be either `PrintableString` or `UTF8String`. 7. The `serialNumber`, if present, MUST be a `PrintableString`. 8. The `countryName` value MUST be identical to the `countryName` value in the certificate's `issuer` field.
Expected results	1. True 2. True 3. True 4. True 5. True 6. True 7. True 8. True

Test-ID	CERT_SUB_3
Purpose	Verify that the `subject` field is in conformance with the ICAO specifications.
Version	1.10
References	[Doc9303-12] clause 7.1.2 [TR DTC] clause 2.2.2
Profile	LDS2-B, LDS2-TS, LDS2-V DTC-S
Preconditions	1. The certificate has passed the test case CERT_SUB_1 successfully. 2. The certificate has passed the test case CERT_ISS_1 successfully.
Test scenario	Verify the following properties: 1. The `countryName` MUST be present. 2. The `countryName` MUST use the [Doc9303-3] two letter code as value. 3. The countryName MUST be a `PrintableString`. 4. The `commonName` MUST be present. 5. The `commonName` value MUST NOT exceed 9 characters in length. 6. Other attributes MUST NOT be included. 7. The `countryName` value MUST be identical to the `countryName` value in the certificate's `issuer` field.
Expected results	1. True 2. True 3. True 4. True 5. True 6. True

	7. True

Test-ID	CERT_SUB_4
Purpose	Verify that the `subject` field is in conformance with the ICAO specifications.
Version	1.10
References	[Doc9303-12] clause 7.1.3 [TR VDS-NC] clause 3.6
Profile	PoR-S, PoT-S, PoV-S, DTA-S, BCS
Preconditions	1. The certificate has passed the test case CERT_SUB_1 successfully. 2. The certificate has passed the test case CERT_ISS_1 successfully.
Test scenario	Verify the following properties: 1. The `countryName` MUST be present. 2. The `countryName` MUST use the [Doc9303-3] two letter code as value. 3. The `countryName` MUST be upper case. 4. The `countryName` MUST be a `PrintableString`. 5. The `commonName` MUST be present. 6. The `commonName` MUST consist of two uppercase characters. 7. The `commonName` MUST be a `PrintableString`. 8. Other attributes MUST NOT be included. 9. The `countryName` value MUST be identical to the `countryName` value in the certificate's `issuer` field.
Expected results	1. True 2. True 3. True 4. True 5. True 6. True 7. True 8. True 9. True

Test-ID	CERT_SUB_5
Purpose	Verify that the `subject` field is in conformance with the ICAO specifications.
Version	1.20
References	[Doc9303-12] clause 7.2.1
Profile	SPOC-CA
Preconditions	1. The certificate has passed the test case CERT_SUB_1 successfully.
Test scenario	Verify the following properties: 1. The `countryName` MUST be present.
Expected results	1. True

Test-ID	CERT_SUB_6
Purpose	Verify that the `subject` field is in conformance with the ICAO specifications.
Version	1.20
References	[Doc9303-12] clause 7.2.1
Profile	SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_SUB_1 successfully.
Test scenario	Verify the following properties: 1. The `countryName` MUST be present. 2. The `countryName` MUST use the [Doc9303-3] two letter code as value. 3. The `countryName` MUST be upper case. 4. The `countryName` MUST be a PrintableString.

	5. The `commonName` MUST be present.
Expected results	1. True 2. True 3. True 4. True 5. True

3.10 subjectPublicKeyInfo

For the profiles CSCA-Root, CSCA-Link, DS, MLS, DLS, TL-S, COMM, and DTC-S the test cases specified in clause 3.10.1, 3.10.2, and 3.10.3 are conditional. A certificate must pass the relevant test cases either in clause 3.10.1, or in clause 3.10.2, or in clause 3.10.3. These clauses describe which test cases are relevant.

The CA-VDS-NC, LDS2-B, LDS2-TS, LDS2-V, PoR-S, PoT-S, PoV-S, DTA-S, and BCS certificates must pass the relevant test cases of clause 3.10.2.

For the profiles SPOC-C and SPOC-S the test cases specified in clause 3.10.2 and 3.10.3 are conditional. A certificate must pass the relevant test cases either in clause 3.10.2 or in clause 3.10.3. These clauses describe which test cases are relevant.

Test-ID	CERT_PKI_1
Purpose	Verify that the `subjectPublicKeyInfo` field is present in `tbsCertificate`.
Version	0.40
References	[Doc9303-12] Table 5 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2 [RFC5280] clause 4.1
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_CERT_2 successfully.
Test scenario	Verify the following properties: 1. The `tbsCertificate` sequence MUST contain the `subjectPublicKeyInfo` field.
Expected results	1. True

Test-ID	CERT_PKI_2
Purpose	Verify that the `subjectPublicKeyInfo` field specifies an allowed cryptographic algorithm.
Version	0.20
References	[Doc9303-12] clause 4 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2 [RFC3279] clauses 2.3.1 (RSASSA-PKCS1_v15), 2.3.2 (DSA), 2.3.5 (ECDSA) [RFC4055] clause 1.2 (RSASSA-PSS)
Profile	CSCA-Root, CSCA-Link, DS, MLS, DLS, TL-S, COMM DTC-S
Preconditions	1. The certificate has passed the test case CERT_PKI_1 successfully.

Test scenario	Verify the following properties: 1. The `AlgorithmIdentifier` MUST contain one of the following OIDs: `id-dsa` (1.2.840.10040.4.1) `id-ecPublicKey` (1.2.840.10045.2.1) `rsaEncryption` (1.2.840.113549.1.1.1) `id-RSASSA-PSS` (1.2.840.113549.1.1.10)
Expected results	1. True

Test-ID	CERT_PKI_3
Purpose	Verify that the `subjectPublicKeyInfo` field specifies an allowed cryptographic algorithm.
Version	1.10
References	[Doc9303-12] clause 4.1.7 [TR VDS-NC] clause 3.6 [RFC3279] clause 2.3.5
Profile	CA-VDS-NC LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S BCS
Preconditions	1. The certificate has passed the test case CERT_PKI_1 successfully.
Test scenario	Verify the following properties: 1. The `AlgorithmIdentifier` MUST contain the OID `id-ecPublicKey` (1.2.840.10045.2.1)
Expected results	1. True

Test-ID	CERT_PKI_4
Purpose	Verify that the `subjectPublicKeyInfo` field specifies an allowed cryptographic algorithm.
Version	1.20
References	[Doc9303-12] clause 4.2.2
Profile	SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_PKI_1 successfully.
Test scenario	Verify the following properties: 1. The `AlgorithmIdentifier` MUST contain one of the following OIDs: `id-ecPublicKey` (1.2.840.10045.2.1) or `rsaEncryption` (1.2.840.113549.1.1.1)
Expected results	1. True

3.10.1 **DSA Public Keys**

A CSCA-Root or CSCA-Link certificate that supports DSA must successfully pass the test cases:

- CERT_DSA_1, CERT_DSA_2, CERT_DSA_5, CERT_DSA_6

A DS, MLS, DLS, TL-S, COMM or DTC-S certificate that supports DSA must successfully pass the test cases:

- CERT_DSA_1
- CERT_DSA_3 if the issuing CSCA Root certificate supports DSA
- CERT_DSA_4 if the issuing CSCA Root certificate does not support DSA
- CERT_DSA_5 and CERT_DSA_6 if the parameters are present
- CERT_DSA_7 if the parameters are absent

This clause uses the following notation:

- p, q primes
- L the bit length of the prime p
- N the bit length of the prime q
- g the generator
- y the public key value

Test-ID	CERT_DSA_1
Purpose	Verify that the DSA public key in the `subjectPublicKeyInfo` field is encoded compliant to the specification.
Version	0.40
References	[RFC3279] clause 2.3.2
Profile	CSCA-Root, CSCA-Link, DS, MLS, DLS, TL-S, COMM DTC-S
Preconditions	1. The certificate has passed the test case CERT_PKI_2 successfully. 2. The `AlgorithmIdentifier` contains the `id-dsa` OID.
Test scenario	Verify the following properties: 1. The DSA public key MUST be encoded as specified in [RFC3279] clause 2.3.2.
Expected results	1. True

Test-ID	CERT_DSA_2
Purpose	Verify that the DSA parameters in the `subjectPublicKeyInfo` field are present and encoded compliant to the specification.
Version	0.40
References	[RFC3279] clause 2.3.2
Profile	CSCA-Root, CSCA-Link
Preconditions	1. The certificate has passed the test case CERT_PKI_2 successfully. 2. The `AlgorithmIdentifier` contains the `id-dsa` OID.
Test scenario	Verify the following properties: 1. The `parameters` component in the `AlgorithmIdentifier` MUST be included using the `Dss-Parms` data structure specified in [RFC3279] clause 2.3.2.
Expected results	1. True

Test-ID	CERT_DSA_3
Purpose	Verify that the DSA parameters in the `subjectPublicKeyInfo` field are encoded compliant to the specification.
Version	0.40
References	[RFC3279] clause 2.3.2
Profile	DS, MLS, DLS, TL-S, COMM DTC-S
Preconditions	1. The certificate has passed the test case CERT_PKI_2 successfully. 2. The `AlgorithmIdentifier` contains the `id-dsa` OID. 3. The issuing CSCA Root certificate contains the `id-dsa` OID in the `subjectPublicKeyInfo AlgorithmIdentifier`.
Test scenario	Verify the following properties: 1. The `parameters` component in the `AlgorithmIdentifier` MUST be either omitted entirely or MUST be included using the `Dss-Parms` data structure specified in [RFC3279] clause 2.3.2.
Expected results	1. True

Test-ID	CERT_DSA_4
Purpose	Verify that the DSA parameters in the `subjectPublicKeyInfo` field are present and encoded compliant to the specification.
Version	0.30
References	[RFC3279] clause 2.3.2
Profile	DS, MLS, DLS, TL-S, COMM DTC-S
Preconditions	1. The certificate has passed the test case CERT_PKI_2 successfully. 2. The `AlgorithmIdentifier` contains the `id-dsa` OID. 3. The issuing CSCA Root certificate does not contain the `id-dsa` OID in the `subjectPublicKeyInfo AlgorithmIdentifier`.
Test scenario	Verify the following properties: 1. The `parameters` component in the `AlgorithmIdentifier` MUST be included using the `Dss-Parms` data structure specified in [RFC3279] clause 2.3.2.
Expected results	1. True

Test-ID	CERT_DSA_5
Purpose	Validate the DSA parameters.
Version	0.40
References	[FIPS 186-4]
Profile	CSCA, CSCA-Link, DS, MLS, DLS, TL-S, COMM DTC-S
Preconditions	1. The certificate has passed either the test case CERT_DSA_2 or CERT_DSA_4 successfully or passed the test case CERT_DSA_3 successfully and the parameters are present.
Test scenario	Verify the following properties: 1. The bit lengths L of the parameter p and the bit length N of the parameter q MUST be one of the pairs specified in [FIPS 186-4] clause 4.2, i.e. L = 1024, N = 160 L = 2048, N = 224 L = 2048, N = 256 L = 3072, N = 256. 2. Primality test: The primes p and q MUST pass a probabilistic primality test according to [FIPS 186-4] clause C.3 or equivalent. 3. Validity of the generator: The generator MUST fulfil $2 \leq g \leq p-1$. 4. Validity of the generator: The generator MUST fulfil $g^q \equiv 1 \bmod p$.
Expected results	1. True 2. True 3. True 4. True

Test-ID	CERT_DSA_6
Purpose	Validate the DSA public key value
Version	0.40
References	[Doc9303-12] clause 4.1.6.2
Profile	CSCA, CSCA-Link, DS, MLS, DLS, TL-S, COMM DTC-S
Preconditions	1. The certificate has passed the test case CERT_DSA_1 successfully. 2. The certificate has passed the test case CERT_DSA_5 successfully.
Test scenario	Verify the following properties: 1. Correct representation and range: The key MUST fulfill $2 \leq y \leq p-2$.

	2. Correct order in the subgroup: The key MUST fulfill $y^q \equiv 1 \bmod p$. Note: The test scenario follows [SP 800-89] clause 5.3.1.
Expected results	1. True 2. True

Test-ID	CERT_DSA_7
Purpose	Validate the DSA public key value
Version	0.40
References	[Doc9303-12] clause 4.1.6.2
Profile	DS, MLS, DLS, TL-S, COMM DTC-S
Preconditions	1. The certificate has passed the test case CERT_DSA_1 successfully. 2. The certificate has passed the test case CERT_DSA_3 successfully and the parameters are not present. 3. The issuing CSCA Root certificate has passed the testcase CERT_DSA_5 successfully.
Test scenario	Verify the following properties using p and q from the issuing CSCA Root certificate: 1. Correct representation and range: The key MUST fulfill $2 \leq y \leq p-2$. 2. Correct order in the subgroup: The key MUST fulfill $y^q \equiv 1 \bmod p$. Note: The test scenario follows [SP 800-89] clause 5.3.1.
Expected results	1. True 2. True

3.10.2 **ECDSA Public Keys**

CSCA-Root, CSCA-Link, DS, MLS, DLS, TL-S, COMM, LDS2-B, LDS2-TS, LDS2-V, BCS, DTC-S, SPOC-C, and SPOC-S certificates that support ECDSA with prime fields must successfully pass the test cases CERT_ECDSA_1, CERT_ECDSA_2, CERT_ECDSA_4, and CERT_ECDSA_6.

CSCA-Root, CSCA-Link, DS, MLS, DLS, TL-S, COMM, LDS2-B, LDS2-TS, LDS2-V, BCS, DTC-S, SPOC-C, and SPOC-S certificates that support ECDSA with characteristic two fields must successfully pass the test cases CERT_ECDSA_1, CERT_ECDSA_3, CERT_ECDSA_5, and CERT_ECDSA_7.

The CA-VDS-NC certificate must either successfully pass the test cases

- CERT_ECDSA_1, CERT_ECDSA_2, CERT_ECDSA_4, CERT_ECDSA_6 or
- CERT_ECDSA_1, CERT_ECDSA_3, CERT_ECDSA_5, and CERT_ECDSA_7 or
- CERT_ECDSA_8 and CERT_ECDSA_9.

The PoR-S, PoT-S, PoV-S, and DTA-S certificates must successfully pass the test cases CERT_ECDSA_8 and CERT_ECDSA_9.

This clause uses the following notation:

- F(p) finite prime field consisting of exactly p elements
- $F(2^m)$ finite field consisting of exactly 2^m elements
- a, b parameters of the elliptic curve
- 0_E the point at infinity
- G base point / generator with x-coordinate x_G and y-coordinate y_G

- n order of the base point / generator G
- Q public key point with x-coordinate x_Q and y-coordinate y_Q

Test-ID	CERT_ECDSA_1
Purpose	Verify that the ECDSA parameters and the ECDSA public key in the `subjectPublicKeyInfo` field are compliant to the specification.
Version	1.10
References	[Doc9303-12] clause 4.1.6.3 [RFC3279] clause 2.3.5
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V BCS DTC-S SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_PKI_2, CERT_PKI_3, or CERT_PKI_4 successfully. 2. The `AlgorithmIdentifier` contains the `id-ecPublicKey` OID.
Test scenario	Verify the following properties: 1. The `parameters` in the `AlgorithmIdentifier` MUST be of type `ECParameters`, see [RFC3279] clause 2.3.5. 2. The `ecParameters version` MUST be set to 1. 3. The `fieldType` OID in the `ecParameters fieldID` MUST use one of the OIDs listed in Table 8. 4. These ec`Parameters` MUST include the optional co-factor. 5. These ec`Parameters` MUST use the `ECPoint` in uncompressed format. 6. The ECDSA public key MUST be encoded as specified in [RFC3279] clause 2.3.5 using the uncompressed format.
Expected results	1. True 2. True 3. True 4. True 5. True 6. True

Test-ID	CERT_ECDSA_2
Purpose	Verify that the `fieldID` (as part of the ECDSA parameters) contains correct encoded parameters in case of prime fields.
Version	0.40
References	[RFC3279] clause 2.3.5
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V BCS DTC-S SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_ECDSA_1 successfully. 2. The `ecParameters fieldType` contains the `prime-field` OID.
Test scenario	Verify the following properties: 1. The fieldID `parameters` are of type `Prime-p`.
Expected results	1. True

Test-ID	CERT_ECDSA_3
Purpose	Verify that the `fieldID` (as part of the ECDSA parameters) contains the correct

	encoded parameters in case of characteristic two fields.
Version	0.40
References	[RFC3279] clause 2.3.5
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V BCS DTC-S SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_ECDSA_1 successfully. 2. The `ecParameters fieldType` contains the `characteristic-two-field` OID.
Test scenario	Verify the following properties: 1. The fieldID `parameters` are of type `Characteristic-two`. 2. The `basis` in the `Characteristic-two` parameters MUST use one of the OIDs listed in Table 9. 3. The `parameters` in the `Characteristic-two` MUST be of the type specified for the corresponding `basis` OID, see Table 9.
Expected results	1. True 2. True 3. True

Test-ID	CERT_ECDSA_4
Purpose	Validate the ECDSA parameters in case of prime fields.
Version	0.40
References	[Doc9303-12] clause 4.1.6.3 [TR VDS-NC] clause 3.6
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V BCS DTC-S SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_ECDSA_2 successfully.
Test scenario	For the given parameters verify the following properties (or equivalent): 1. $p > 3$ MUST be prime. 2. a, b, x_G, y_G MUST be elements of F(p). 3. $(4a^3 + 27b^2) \neq 0$ in F(p) 4. $y_G^2 = x_G^3 + ax_G + b$ in F(p) 5. The order n of the base point G MUST be prime and fulfil $n > 4\ (p^{1/2})$. 6. $nG = 0_E$ (the point at infinity) 7. Calculate the largest integer less or equal to $((p^{1/2} + 1)^2 / n)$; the result MUST equal the cofactor. Note: The parameter validation follows [ISO/IEC 15946-1]; the following steps are omitted: • the verification that a and b were suitably derived from a seed if the curve was randomly generated, • the check to exclude known weak curves.
Expected results	1. True 2. True 3. True 4. True

	5. True 6. True 7. True

Test-ID	CERT_ECDSA_5
Purpose	Validate the ECDSA parameters in case of characteristic two fields.
Version	0.40
References	[Doc9303-12] clause 4.1.6.3
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V BCS DTC-S SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_ECDSA_3 successfully.
Test scenario	For the given parameters verify the following properties (or equivalent): 1. $q = 2^m$ for some m 2. a, b, x_G, and y_G MUST be bit strings of length m bits. 3. $b \neq 0$ 4. $y_G^2 + x_G y_G = x_G^3 + a x_G^2 + b$ in $F(2^m)$ 5. n MUST be prime and $n > 4\ (2^m)^{1/2}$ 6. $nG = 0_E$ (the point at infinity) 7. Calculate the largest integer less or equal to $(((2^m)^{1/2} + 1)^2 / n)$; the result MUST equal the cofactor. 8. Verify the basis as specified in [X9.62]. Note: The parameter validation follows [ISO/IEC 15946-1] with the exception of step 8; the following steps are omitted: • the verification that a and b were suitably derived from a seed if the curve was randomly generated, • the check to exclude known weak curves.
Expected results	1. True 2. True 3. True 4. True 5. True 6. True 7. True 8. True

Test-ID	CERT_ECDSA_6
Purpose	Validate the ECDSA public key in case of prime fields.
Version	0.40
References	[Doc9303-12] clause 4.1.6.3
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S COMM LDS2-B, LDS2-TS, LDS2-V BCS DTC-S SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_ECDSA_4 successfully.
Test scenario	For the claimed public key Q verify the following properties (or equivalent): 1. Q MUST NOT be the point at infinity 0_E.

	2. The x coordinate of Q (denoted as x_Q) and the y coordinate of Q (denoted as y_Q) MUST be elements of F(p). 3. $y_Q^2 = x_Q^3 + ax_Q + b$ in F(p) 4. $nQ = 0_E$ Note: The public key validation follows [ISO/IEC 15946-1].
Expected results	1. True 2. True 3. True 4. True

Test-ID	CERT_ECDSA_7
Purpose	Validate the ECDSA public key in case of characteristic two fields.
Version	0.40
References	[Doc9303-12] clause 4.1.6.3
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V BCS DTC-S SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_ECDSA_5 successfully.
Test scenario	For the claimed public key Q verify the following properties (or equivalent): 1. Q MUST NOT be the point at infinity 0_E. 2. The x coordinate of Q (denoted as x_Q) and the y coordinate of Q (denoted as y_Q) MUST be elements of $F(2^m)$. 3. $y_Q^2 + x_Q y_Q = x_Q^3 + ax_Q^2 + b$ in $F(2^m)$ 4. $nQ = 0_E$ Note: The public key validation follows [ISO/IEC 15946-1].
Expected results	1. True 2. True 3. True 4. True

Test-ID	CERT_ECDSA_8
Purpose	Verify that the ECDSA parameters and the ECDSA public key in the `subjectPublicKeyInfo` field are compliant to the specification.
Version	1.10
References	[TR VDS-NC] clause 3.6 [RFC3279] clause 2.3.5
Profile	CA-VDS-NC PoR-S, PoT-S, PoV-S, DTA-S
Preconditions	1. The certificate has passed the test case CERT_PKI_3 successfully.
Test scenario	Verify the following properties: 1. The `parameters` in the `AlgorithmIdentifier` MUST be of type `namedCurve`, see [RFC3279] clause 2.3.5. 2. The `namedCurve` MUST encode an OID for a curve listed in [TR VDS-NC] clause 3.6.5. 3. The ECDSA public key MUST be encoded as specified in [RFC3279] clause 2.3.5 using the uncompressed format.
Expected results	1. True 2. True

	3. True

Test-ID	CERT_ECDSA_9
Purpose	Validate the ECDSA public key in case of prime fields.
Version	1.10
References	[Doc9303-12] clause 4.1.6.3
Profile	CA-VDS-NC PoR-S, PoT-S, PoV-S, DTA-S
Preconditions	1. The certificate has passed the test case CERT_ECDSA_8 successfully.
Test scenario	For the claimed public key Q verify the following properties (or equivalent): 1. Q MUST NOT be the point at infinity 0_E. 2. The x coordinate of Q (denoted as x_Q) and the y coordinate of Q (denoted as y_Q) MUST be elements of F(p). 3. $y_Q^2 = x_Q^3 + ax_Q + b$ in F(p) 4. $nQ = 0_E$ Note: The public key validation follows [ISO/IEC 15946-1].
Expected results	1. True 2. True 3. True 4. True

3.10.3 **RSA Public Keys**

CSCA-Root, CSCA-Link, DS, MLS, DLS, TL-S, COMM, DTC-S, SPOC-C, and SPOC-S certificates that support RSA (OID `rsaEncryption`) must successfully pass the test cases CERT_RSA_1 and CERT_RSA_3.
CSCA-Root, CSCA-Link, DS, MLS, DLS, TL-S, COMM, and DTC-S certificates that support RSA (OID `id-RSASSA-PSS`) must successfully pass the test cases CERT_RSA_2 and CERT_RSA_3.

Test-ID	CERT_RSA_1
Purpose	Verify that the RSASSA-PKCS1_v15 parameters and the RSA public key in the `subjectPublicKeyInfo` field are compliant to the specification.
Version	0.30
References	[RFC4055] clause 1.2
Profile	CSCA-Root, CSCA-Link, DS, MLS, DLS, TL-S, COMM DTC-S SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_PKI_2 or CERT_PKI_4 successfully. 2. The `AlgorithmIdentifier` contains the `rsaEncryption` OID.
Test scenario	Verify the following properties: 1. The `parameters` in the `AlgorithmIdentifier` MUST be NULL. 2. The RSA public key MUST be encoded as specified in [RFC4055] clause 1.2.
Expected results	1. True 2. True

Test-ID	CERT_RSA_2
Purpose	Verify that the RSASSA-PSS parameters and the RSA public key in the `subjectPublicKeyInfo` field are compliant to the specification.
Version	0.30

References	[Doc9303-12] clause 4.1.6.4[RFC4055] clauses 1.2 and 3.1
Profile	CSCA-Root, CSCA-Link, DS, MLS, DLS, TL-S, COMM DTC-S
Preconditions	1. The certificate has passed the test case CERT_PKI_2 successfully. 2. The `AlgorithmIdentifier` contains the `id-RSASSA-PSS` OID.
Test scenario	Verify the following properties: 1. The `parameters` in the `AlgorithmIdentifier` MUST be either absent or of type `RSASSA-PSS-params` using the following values: a. The `hashAlgorithm` MUST use one of the OIDs listed in Table 11. b. The `maskGenAlgorithm` MUST use one of the algorithm identifiers listed in Table 6. c. The `trailerField` MUST be absent. 2. The RSA public key MUST be encoded as specified in [RFC4055] clause 1.2.
Expected results	1. True a. True b. True c. True 2. True

Test-ID	CERT_RSA_3
Purpose	Partial Public Key Validation for RSA
Version	0.40
References	[Doc9303-12] clause 4.1.6.1
Profile	CSCA-Root, CSCA-Link, DS, MLS, DLS, TL-S, COMM DTC-S SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_RSA_1 or CERT_RSA_2 successfully.
Test scenario	Verify at least the following properties (or equivalent): 1. The modulus and the public exponent MUST be odd numbers. 2. The modulus MUST be composite, but MUST NOT be a power of a prime. 3. The modulus MUST have no factors smaller than 752. (Note: Testing for additional factors is allowed.) Note: The test scenario uses the relevant steps from [SP 800-89] clause 5.3.3 which also provides information on how these steps could be implemented.
Expected results	1. True 2. True 3. True

3.11 issuerUniqueID

Test-ID	CERT_IUID_1
Purpose	Verify that the `issuerUniqueID` field is not present in `tbsCertificate`.
Version	0.40
References	[Doc9303-12] Table 5 and clause 7 [RFC5280] clause 4.1.2.8 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V

	PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_CERT_2 successfully.
Test scenario	Verify the following properties: 1. The `tbsCertificate` sequence MUST NOT contain the `issuerUniqueID` field.
Expected results	1. True

3.12 subjectUniqueID

Test-ID	CERT_SUID_1
Purpose	Verify that the `subjectUniqueID` field is not present in `tbsCertificate`.
Version	0.40
References	[Doc9303-12] Table 5 and clause 7 [RFC5280] clause 4.1.2.8 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_CERT_2 successfully.
Test scenario	Verify the following properties: 1. The `tbsCertificate` sequence MUST NOT contain the `subjectUniqueID` field.
Expected results	1. True

3.13 extensions

Test-ID	CERT_EXT_1
Purpose	Verify that the `extensions` field is present in `tbsCertificate`.
Version	0.40
References	[Doc9303-12] Table 5 and clause 7 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_CERT_2 successfully.
Test scenario	Verify the following properties: 1. The `tbsCertificate` sequence MUST contain the `extensions` field.
Expected results	1. True

Test-ID	CERT_EXT_2
Purpose	Verify that extensions which must not be used according to the ICAO specifications are absent in the `extensions` field.
Version	0.20
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6

Profile	CSCA-Root, CSCA-Link, DS, MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully.
Test scenario	Verify the following properties: 1. The `extensions` sequence MUST NOT contain extensions that are marked as 'do not use (x)' for the type of certificate in Doc9303-12 Table 6. Notes: The Doc 9303-12 Table 6 provisions for the • MLS profile apply to the TL-S profile, • COMM profile apply to the SPOC-C and SPOC-S profile.
Expected results	1. True

Test-ID	CERT_EXT_3
Purpose	Verify that extensions which must not be used according to the ICAO specifications are absent in the `extensions` field.
Version	1.10
References	[Doc9303-12] Table 7 and clause 7.1.2
Profile	LDS2-B, LDS2-TS, LDS2-V
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully.
Test scenario	Verify the following properties: The `extensions` sequence MUST NOT contain extensions that are not listed in Doc9303-12 Table 7.
Expected results	1. True

Test-ID	CERT_EXT_4
Purpose	Verify that extensions which must not be used according to the ICAO specifications are absent in the `extensions` field.
Version	1.10
References	[Doc9303-12] Table 8 and clause 7.1.3 [TR VDS-NC] clause 3.6
Profile	PoR-S, PoT-S, PoV-S, DTA-S, BCS
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully.
Test scenario	Verify the following properties: The `extensions` sequence MUST NOT contain extensions that are not listed in Doc9303-12 Table 8.
Expected results	1. True

Test-ID	CERT_EXT_5
Purpose	Verify that extensions which must not be used according to the ICAO specifications are absent in the `extensions` field.
Version	1.10
References	[TR DTC] clause 2.2.2
Profile	DTC-S
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully.
Test scenario	Verify the following properties: The `extensions` sequence MUST NOT contain extensions that are not listed in [TR DTC] clause 2.2.2.
Expected results	1. True

Test-ID	CERT_EXT_6
Purpose	Verify that extensions which must not be used according to the ICAO specifications are absent in the `extensions` field.

Version	1.10
References	[Doc9303-12] Table 6 [TR VDS-NC] clause 3.6
Profile	CA-VDS-NC
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully.
Test scenario	Verify the following properties: 1. The extensions sequence MUST NOT contain extensions that are marked as 'do not use (x)' for the CSCA profile in Doc9303-12 Table 6 with the exception of the Extended Key Usage extension.
Expected results	1. True

3.13.1 **AuthorityKeyIdentifier Extension**

Test-ID	CERT_AKI_1
Purpose	Verify that the `AuthorityKeyIdentifier` extension is present.
Version	0.40
References	[Doc9303-12] Table 6, 7 and 8 and clause 7 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2 [RFC5280] clause 4.2
Profile	CSCA-Link, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully.
Test scenario	Verify the following properties: 1. The `extensions` MUST contain exactly 1 instance of the `AuthorityKeyIdentifier` extension.
Expected results	1. True

For the profiles CSCA-Root and CA-VDS-NC the test cases CERT_AKI_2 to CERT_AKI_ 5 are conditional. A CSCA Root / CA-VDS-NC certificate must pass these test cases successfully if an `AuthorityKeyIdentifier` extension is present.
For the profile SPOC-CA the test cases CERT_AKI_2 to CERT_AKI_3 are conditional. A SPOC CA certificate must pass these test cases successfully if an `AuthorityKeyIdentifier` extension is present.

Test-ID	CERT_AKI_2
Purpose	Verify that at most 1 instance of the `AuthorityKeyIdentifier` extension is present.
Version	0.40
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6 [RFC5280] clause 4.2
Profile	CSCA-Root, CA-VDS-NC SPOC-CA
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully. 2. The optional `AuthorityKeyIdentifier` extension is present.
Test scenario	Verify the following properties: 1. The `extensions` MUST contain exactly 1 instance of the `AuthorityKeyIdentifier` extension.
Expected results	1. True

Test-ID	CERT_AKI_3
Purpose	Verify that the `AuthorityKeyIdentifier` extension's criticality is in conformance with Doc9303-12.
Version	0.40
References	[Doc9303-12] Table 5 and Table 6, 7 and 8 and clause 7 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2 [RFC5280] clause 4.2.1.1
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_AKI_1 or CERT_AKI_2 successfully.
Test scenario	Verify the following properties: 1. The `critical` field MUST be absent.
Expected results	1. True

Test-ID	CERT_AKI_4
Purpose	Verify that the `AuthorityKeyIdentifier` extension contains the `keyIdentifier`.
Version	0.40
References	[Doc9303-12] Table 6, 7 and 8 and clause 7 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_AKI_1 or CERT_AKI_2 successfully.
Test scenario	Verify the following properties: 1. The `keyIdentifier` MUST be present in the `AuthorityKeyIdentifier` extension.
Expected results	1. True

Test-ID	CERT_AKI_5
Purpose	Verify that the `AuthorityKeyIdentifier` extension is in conformance with Doc9303-12.
Version	1.10
References	[RFC5280] clause 4.2.1.1
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_AKI_4 successfully. 2. The issuing Root certificate has passed the test case CERT_SKI_4 successfully.
Test scenario	Verify the following properties of the certificate's `AuthorityKeyIdentifier` extension: 1. The `keyIdentifier` value MUST be identical to the

	`subjectKeyIdentifier` value of the issuing Root certificate's `SubjectKeyIdentifier` extension. Notes: • For the CSCA-Root profile, the issuing CSCA Root certificate is the CSCA Root certificate itself. • For the CA-VDS-NC profile, the issuing Root certificate is the VDS-NC Root CA certificate itself
Expected results	1. True

3.13.2 **SubjectKeyIdentifier Extension**

Test-ID	CERT_SKI_1
Purpose	Verify that the `SubjectKeyIdentifier` extension is present.
Version	0.40
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2 [RFC5280] clause 4.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC DTC-S SPOC-CA
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully.
Test scenario	Verify the following properties: 1. The `extensions` MUST contain exactly 1 instance of the `SubjectKeyIdentifier` extension.
Expected results	1. True

For the profiles DS, MLS, DLS, TL-S, COMM, SPOC-C, and SPOC-S the test cases CERT_SKI_2 to CERT_SKI_ 4 are conditional. A DS, MLS, DLS, TL-S, COMM, SPOC Client or SPOC Server certificate must pass these test cases successfully if a `SubjectKeyIdentifier` extension is present.

Test-ID	CERT_SKI_2
Purpose	Verify that at most 1 instance of the `SubjectKeyIdentifier` extension is present.
Version	0.40
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6 [RFC5280] clause 4.2
Profile	DS, MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully. 2. The optional `SubjectKeyIdentifier` extension is present.
Test scenario	Verify the following properties: 1. The `extensions` MUST contain exactly 1 instance of the `SubjectKeyIdentifier` extension.
Expected results	1. True

Test-ID	CERT_SKI_3
Purpose	Verify that the `SubjectKeyIdentifier` extension's criticality is in conformance with the ICAO specifications.
Version	0.40

References	[Doc9303-12] Table 5 and Table 6 and clause 7 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2 [RFC5280] clause 4.1 and 4.2.1.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_SKI_1 or CERT_SKI_2 successfully.
Test scenario	Verify the following properties: 1. The `critical` field MUST be absent.
Expected results	1. True

Test-ID	CERT_SKI_4
Purpose	Verify that the `SubjectKeyIdentifier` extension contains a `subjectKeyIdentifier`.
Version	0.40
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_SKI_1 or CERT_SKI_2 successfully.
Test scenario	Verify the following properties: 1. The `SubjectKeyIdentifier` extension MUST contain a `subjectKeyIdentifier`.
Expected results	1. True

3.13.3 **KeyUsage Extension**

Test-ID	CERT_BKU_1
Purpose	Verify that the `KeyUsage` extension is present.
Version	0.40
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2 [RFC5280] clause 4.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM DTC-S SPOC-CA, SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully.
Test scenario	Verify the following properties: 1. The `extensions` MUST contain exactly 1 instance of the `KeyUsage` extension.
Expected results	1. True

Test-ID	CERT_BKU_2
Purpose	Verify that the `KeyUsage` extension's criticality is in conformance with the ICAO specifications.
Version	0.20
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6

	[TR DTC] clause 2.2.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM DTC-S SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_BKU_1 successfully.
Test scenario	Verify the following properties: 1. The `critical` field MUST be set to TRUE.
Expected results	1. True

Test-ID	CERT_BKU_3
Purpose	Verify that the `KeyUsage` bits are set in conformance with Doc9303-12.
Version	1.20
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_BKU_1 successfully.
Test scenario	Verify the following properties: 1. The `KeyUsage` bits marked as "mandatory" (m) for the type of certificate in [Doc9303-12] Table 6 MUST be set in the certificate. 2. The `KeyUsage` bits marked as "do not use" (x) for the type of certificate in [Doc9303-12] Table 6 MUST NOT be set in the certificate. 3. The `KeyUsage` bits marked as "optional" (o) for the type of certificate in [Doc9303-12] Table 6 MAY be set in the certificate. Notes: The Doc 9303-12 Table 6 provisions • for the CSCA-Root profile apply to the CA-VDS-NC profile, • for the MLS profile apply to the TL-S profile, • for the COMM profile apply to the SPOC-C and SPOC-S profile. (This clause specifies further SPOC-C and SPOC-S test cases for the `KeyUsage` bits marked as "optional" (o).)
Expected results	1. True 2. True 3. True

Test-ID	CERT_BKU_4
Purpose	Verify that the `KeyUsage` bits are set in conformance with the ICAO specifications.
Version	1.10
References	[TR DTC] clause 2.2.2
Profile	DTC-S
Preconditions	1. The certificate has passed the test case CERT_BKU_1 successfully.
Test scenario	Verify the following properties: 1. The `KeyUsage` bits marked as "mandatory" (m) for the type of certificate in [TR DTC] clause 2.2.2 MUST be set in the certificate. 2. The `KeyUsage` bits marked as "do not use" (x) for the type of certificate in [TR DTC] clause 2.2.2 MUST NOT be set in the certificate. 3. The `KeyUsage` bits marked as "optional" (o) for the type of certificate in [TR DTC] clause 2.2.2 MAY be set in the certificate.
Expected results	1. True

	2. True 3. True

Test-ID	CERT_BKU_5
Purpose	Verify that the `KeyUsage` bits are set in conformance with the ICAO specifications.
Version	1.20
References	[Doc9303-12] clause 7.2.1 [RFC5280] clause 4.2.1.3
Profile	SPOC-CA
Preconditions	1. The certificate has passed the test case CERT_BKU_1 successfully.
Test scenario	Verify the following properties: 1. The `keyCertSign` bit MUST be set in the certificate.
Expected results	1. True

Test-ID	CERT_BKU_6
Purpose	Verify that the `KeyUsage` bits are set in conformance with RFC5246.
Version	1.20
References	[RFC5246] clause 7.4.2 and 7.4.6
Profile	SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_BKU_1 successfully. 2. The certificate has passed the test case CERT_PKI_4 successfully. 3. The `AlgorithmIdentifier` in the `subjectPublicKeyInfo` field contains the `id-ecPublicKey` OID.
Test scenario	Verify the following properties: 1. The `digitalSignature` bit MUST be set in the certificate.
Expected results	1. True

Test-ID	CERT_BKU_7
Purpose	Verify that the `KeyUsage` bits are set in conformance with RFC5246.
Version	1.20
References	[RFC5246] clause 7.4.2
Profile	SPOC-S
Preconditions	1. The certificate has passed the test case CERT_BKU_1 successfully. 2. The certificate has passed the test case CERT_PKI_4 successfully. 3. The `AlgorithmIdentifier` in the `subjectPublicKeyInfo` field contains the `rsaEncryption` OID.
Test scenario	Verify the following properties: 1. The `digitalSignature` bit, or the `keyEncipherment` bit, or both bits MUST be set in the certificate.
Expected results	1. True

Test-ID	CERT_BKU_8
Purpose	Verify that the `KeyUsage` bits are set in conformance with RFC5246.
Version	1.20
References	[RFC5246] clause 7.4.6
Profile	SPOC-C
Preconditions	1. The certificate has passed the test case CERT_BKU_1 successfully. 2. The certificate has passed the test case CERT_PKI_4 successfully. 3. The `AlgorithmIdentifier` in the `subjectPublicKeyInfo` field contains the `rsaEncryption` OID.
Test scenario	Verify the following properties:

	1. The `digitalSignature` bit MUST be set in the certificate.
Expected results	1. True

3.13.4 **PrivateKeyUsagePeriod Extension**

Test-ID	CERT_PKU_1
Purpose	Verify that the `PrivateKeyUsagePeriod` extension is present.
Version	0.40
References	[Doc9303-12] Table 6 [TR VDS-NC] clause 3.6 [RFC5280] clause 4.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully.
Test scenario	Verify the following properties: 1. The `extensions` MUST contain exactly 1 instance of the `PrivateKeyUsagePeriod` extension.
Expected results	1. True

For the profiles MLS, DLS, TL-S, COMM, SPOC-C and SPOC-S the test cases CERT_PKU_2 to CERT_PKU_ 4 are conditional. A MLS, DLS, TL-S, COMM, SPOC Client or SPOC Server certificate must pass these test cases successfully if a `PrivateKeyUsagePeriod` extension is present.

Test-ID	CERT_PKU_2
Purpose	Verify that at most 1 instance of the `PrivateKeyUsagePeriod` extension is present.
Version	0.40
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6 [RFC5280] clause 4.2
Profile	MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully. 2. The optional `PrivateKeyUsagePeriod` extension is present.
Test scenario	Verify the following properties: 1. The `extensions` MUST contain exactly 1 instance of the `PrivateKeyUsagePeriod` extension.
Expected results	1. True

Test-ID	CERT_PKU_3
Purpose	Verify that the `PrivateKeyUsagePeriod` extension's criticality is in conformance with Doc9303-12.
Version	0.40
References	[Doc9303-12] Table 5 and Table 6 and clause 7 [TR VDS-NC] clause 3.6
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_PKU_1 or CERT_PKU_2 successfully.
Test scenario	Verify the following properties: 1. The `critical` field MUST be absent.
Expected results	1. True

Test-ID	CERT_PKU_4
Purpose	Verify that the `PrivateKeyUsagePeriod` extension is in conformance with Doc9303-12.
Version	0.30
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_PKU_1 or CERT_PKU_2 successfully.
Test scenario	Verify the following properties: 1. The `PrivateKeyUsagePeriod` extension MUST contain `notBefore` or `notAfter` or both. 2. `notBefore` / `notAfter` MUST be encoded as `generalizedTime`.
Expected results	1. True 2. True

3.13.5 **CertificatePolicies Extension**

For the profiles CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM, SPOC-C and SPOC-S the test cases in this clause are conditional. A CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM, SPOC Client or SPOC Server certificate must pass these test cases successfully if a `CertificatePolicies` extension is present.

Test-ID	CERT_CEP_1
Purpose	Verify that at most 1 instance of the `CertificatePolicies` extension is present.
Version	0.40
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6 [RFC5280] clause 4.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully. 2. The optional `CertificatePolicies` extension is present.
Test scenario	Verify the following properties: 1. The `extensions` MUST contain exactly 1 instance of the `CertificatePolicies` extension.
Expected results	1. True

Test-ID	CERT_CEP_2
Purpose	Verify that the `CertificatePolicies` extension's criticality is in conformance with Doc9303-12.
Version	0.40
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_CEP_1 successfully.
Test scenario	Verify the following properties: 1. The `critical` field MUST be absent.
Expected results	1. True

Test-ID	CERT_CEP_3

Purpose	Verify that the `CertificatePolicies` extension contains the required fields.
Version	0.40
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_CEP_1 successfully.
Test scenario	Verify the following properties: 1. The `CertificatePolicies` extension MUST contain the `PolicyInformation` sequence. 2. The `PolicyInformation` sequence MUST contain the `policyIdentifier`.
Expected results	1. True 2. True

3.13.6 **SubjectAltName Extension**

Test-ID	CERT_SAN_1
Purpose	Verify that the `SubjectAltName` extension is present.
Version	0.40
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6 [RFC5280] clause 4.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully.
Test scenario	Verify the following properties: 1. The `extensions` MUST contain exactly 1 instance of the `SubjectAltName` extension.
Expected results	1. True

Test-ID	CERT_SAN_2
Purpose	Verify that the `SubjectAltName` extension's criticality is in conformance with Doc9303-12.
Version	0.20
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_SAN_1 successfully.
Test scenario	Verify the following properties: 1. The `critical` field MUST be absent.
Expected results	1. True

Test-ID	CERT_SAN_3
Purpose	Verify that the `SubjectAltName` extension is in conformance with Doc9303-12.
Version	0.20
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_SAN_1 successfully.

Test scenario	Verify the following properties: 1. The `subjectAltName` value MUST include a `directoryName`. 2. This `directoryName` MUST contain a `localityName` that contains the ICAO country code as specified in [Doc9303-3] for the MRTD's MRZ of the issuing state or organization. 3. If this `directoryName` contains a `stateOrProvinceName`, the `stateOrProvinceName` SHALL indicate the ICAO assigned three-letter code for the issuing State or organization as specified in [Doc9303-3]. 4. This `directoryName` MUST NOT contain other attributes than the `localityName` and `stateOrProvinceName`.
Expected results	1. True 2. True 3. True or the `directoryName` contains no `stateOrProvinceName` 4. True

Test-ID	CERT_SAN_4
Purpose	Verify that the `SubjectAltName` extension contains a `dNSName` value.
Version	1.20
References	[Doc9303-12] clause 7.2.1 [RFC5280] clause 4.2.1.6
Profile	SPOC-S
Preconditions	1. The certificate has passed the test case CERT_SAN_1 successfully.
Test scenario	Verify the following properties: 1. The `subjectAltName` value MUST include a `dNSName`. 2. This `dNSName` MUST be encoded as `IA5String`.
Expected results	1. True 2. True

Test-ID	CERT_SAN_5
Purpose	Verify that one of the `dNSName` values matches the given host part of the SPOC URL.
Version	1.10
References	[Doc9303-12] clause 7.2.1
Profile	SPOC-S
Preconditions	1. The certificate has passed the test case CERT_SAN_4 successfully.
Test scenario	Verify the following properties: 1. One of the `dNSName` values MUST match the given host part of the SPOC URL.
Expected results	1. True

3.13.7 **IssuerAltName Extension**

Test-ID	CERT_IAN_1
Purpose	Verify that the `IssuerAltName` extension is present.
Version	0.40
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6 [RFC5280] clause 4.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully.

Test scenario	Verify the following properties: 1. The `extensions` MUST contain exactly 1 instance of the `IssuerAltName` extension.
Expected results	1. True

Test-ID	CERT_IAN_2
Purpose	Verify that the `IssuerAltName` extension's criticality is in conformance with Doc9303-12.
Version	0.20
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_IAN_1 successfully.
Test scenario	Verify the following properties: 1. The `critical` field MUST be absent.
Expected results	1. True

Test-ID	CERT_IAN_3
Purpose	Check that the `IssuerAltName` and `SubjectAltName` values of a Root CA certificate match.
Version	0.40
References	[Doc9303-12] clause 7.1.1.2 [TR VDS-NC] clause 3.6
Profile	CSCA-Root, CA-VDS-NC
Preconditions	1. The certificate has passed the test case CERT_IAN_1 successfully. 2. The certificate has passed the test case CERT_SAN_1 successfully.
Test scenario	Verify the following properties: 1. The `IssuerAltName` value and `SubjectAltName` value MUST exactly match.
Expected results	1. True

Test-ID	CERT_IAN_4
Purpose	Verify that the `IssuerAltName` extension is in conformance with Doc9303-12.
Version	0.40
References	[Doc9303-12] clause 7.1.1.2 [TR VDS-NC] clause 3.6
Profile	CSCA-Link, DS, MLS, DLS, TL-S, COMM
Preconditions	1. The certificate has passed the test case CERT_IAN_1 successfully. 2. The issuing CSCA Root certificate has passed test case CERT_SAN_1 successfully.
Test scenario	Verify the following properties: 1. The `IssuerAltName` value of the certificate and the issuing CSCA Root certificate's `SubjectAltName` value MUST exactly match.
Expected results	1. True

For the profiles SPOC-C and SPOC-S the test cases CERT_IAN_5 is conditional. A SPOC Client, a SPOC Server certificate must pass the test case CERT_IAN_5 successfully, if the certificate has been issued by a CSCA Root.

Test-ID	CERT_IAN_5
Purpose	Verify that the `IssuerAltName` extension is in conformance with Doc9303-12.

Version	1.20
References	[Doc9303-12] clause 7
Profile	SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_IAN_1 successfully. 2. The certificate has been issued by a CSCA Root, see Table 2. 3. The issuing CSCA Root certificate has passed test case CERT_SAN_1 successfully.
Test scenario	Verify the following properties: 1. The `IssuerAltName` value of the certificate and the issuing CSCA Root certificate's `SubjectAltName` value MUST exactly match.
Expected results	1. True

3.13.8 **BasicConstraints Extension**

Test-ID	CERT_BAC_1
Purpose	Verify that the `BasicConstraints` extension is present.
Version	0.40
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6 [RFC5280] clause 4.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC SPOC-CA
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully.
Test scenario	Verify the following properties: 1. The `extensions` MUST contain exactly 1 instance of the `BasicConstraints` extension.
Expected results	1. True

Test-ID	CERT_BAC_2
Purpose	Verify that the `BasicConstraints` extension's criticality is in conformance with Doc9303-12.
Version	0.20
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC SPOC-CA
Preconditions	1. The certificate has passed the test case CERT_BAC_1 successfully.
Test scenario	Verify the following properties: 1. The `critical` field MUST be set to TRUE.
Expected results	1. True

Test-ID	CERT_BAC_3
Purpose	Verify that the `BasicConstraints` value is in conformance with Doc9303-12.
Version	0.20
References	[Doc9303-12] Table 6 [TR VDS-NC] clause 3.6
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC
Preconditions	1. The certificate has passed the test case CERT_BAC_1 successfully.
Test scenario	Verify the following properties: 1. `cA` MUST be present. 2. cA value MUST be TRUE.

	3. `pathLenConstraint` MUST be present. 4. `pathLenConstraint` value MUST be 0.
Expected results	1. True 2. True 3. True 4. True

Test-ID	CERT_BAC_4
Purpose	Verify that the `BasicConstraints` value is in conformance with Doc9303-12.
Version	1.20
References	[Doc9303-12] clause 7.2.1 [RFC5280] clause 4.2.1.9
Profile	SPOC-CA
Preconditions	1. The certificate has passed the test case CERT_BAC_1 successfully.
Test scenario	Verify the following properties: 1. `cA` MUST be present. 2. cA value MUST be TRUE.
Expected results	1. True 2. True

3.13.9 **ExtKeyUsage Extension**

Test-ID	CERT_EKU_1
Purpose	Verify that the `ExtKeyUsage` extension is present.
Version	0.40
References	[Doc9303-12] Table 6, 7 and 8 and clause 7 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2 [RFC5280] clause 4.2
Profile	CA-VDS-NC, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully.
Test scenario	Verify the following properties: 1. The `extensions` MUST contain exactly 1 instance of the `ExtKeyUsage` extension.
Expected results	1. True

Test-ID	CERT_EKU_2
Purpose	Verify that the `ExtKeyUsage` extension's criticality is in conformance with the ICAO specifications.
Version	0.20
References	[Doc9303-12] Table 6, 7 and 8 and clause 7 [TR VDS-NC] clause 3.6 [TR DTC] clause 2.2.2
Profile	CA-VDS-NC, MLS, DLS, TL-S, COMM LDS2-B, LDS2-TS, LDS2-V PoR-S, PoT-S, PoV-S, DTA-S, BCS DTC-S SPOC-C, SPOC-S

Preconditions	1. The certificate has passed the test case CERT_EKU_1 successfully.
Test scenario	Verify the following properties: 1. The `critical` field MUST be set to TRUE.
Expected results	1. True

Note: The test cases CERT_EKU_3 and CERT_EKU_4 have been replaced by test case CERT_EKU_5 in version 1.20.

Test-ID	CERT_EKU_5
Purpose	Verify that the `ExtKeyUsage` value encodes the correct OID.
Version	1.20
References	See Table 3
Profile	See Table 3
Preconditions	1. The certificate has passed the test case CERT_EKU_1 successfully.
Test scenario	Verify the following properties: 1. For the `KeyPurposeId` the extension MUST encode the OID given in Table 3.
Expected results	1. True

Profiles	**Extended Key Usage OID**	**Reference**
MLS	2.23.136.1.1.3	[Doc9303-12] clause 7.1.1.3
DLS	2.23.136.1.1.8	[Doc9303-12] clause 7.1.1.3
LDS2-TS	2.23.136.1.1.9.8.1	[Doc9303-12] clause 7.1.2
LDS2-V	2.23.136.1.1.9.8.2	[Doc9303-12] clause 7.1.2
LDS2-B	2.23.136.1.1.9.8.3	[Doc9303-12] clause 7.1.2
BCS	2.23.136.1.1.11.1	[Doc9303-12] clause 7.1.3
PoR-S, PoT-S, PoV-S, DTA-S	2.23.136.1.1.14.2	[TR VDS-NC] clause 3.6
TL-S	2.23.136.1.1.15.2	[TR VDS-NC] clause 3.6
DTC-S	2.23.136.1.1.12.1	[TR DTC] clause 2.2.2
CA-VDS-NC	2.23.136.1.1.14.1	[TR VDS-NC] clause 3.6
SPOC-C	2.23.136.1.1.10.1	[Doc9303-12] clause 7.2.1
SPOC-S	2.23.136.1.1.10.2	[Doc9303-12] clause 7.2.1

Table 3 Extended Key Usage OIDs

3.13.10 **CRLDistributionPoints Extension**

Test-ID	CERT_CDP_1
Purpose	Verify that the `CRLDistributionPoints` extension is present.
Version	0.40
References	[Doc9303-12] Table 6 [TR VDS-NC] clause 3.6 [RFC5280] clause 4.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully.
Test scenario	Verify the following properties: 1. The `extensions` MUST contain exactly 1 instance of the `CRLDistributionPoints` extension.
Expected results	1. True

For the profiles COMM, SPOC-C and SPOC-S the test cases CERT_CDP_2 to CERT_CDP_ 5 are conditional. A COMM, SPOC Client or SPOC Server certificate must pass these test cases successfully if a `CRLDistributionPoints` extension is present.

Test-ID	CERT_CDP_2
Purpose	Verify that at most 1 instance of the `CRLDistributionPoints` extension is present.
Version	0.40
References	[Doc9303-12] Table 5 and Table 6 and clause 7 [RFC5280] clause 4.2
Profile	COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully. 2. The optional `CRLDistributionPoints` extension is present.
Test scenario	Verify the following properties: 1. The `extensions` MUST contain exactly 1 instance of the `CRLDistributionPoints` extension.
Expected results	1. True

Test-ID	CERT_CDP_3
Purpose	Verify that the `CRLDistributionPoints` extension's criticality is in conformance with Doc9303-12.
Version	0.40
References	[Doc9303-12] Table 5 and Table 6 and clause 7 [TR VDS-NC] clause 3.6
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_CDP_1 or CERT_CDP_2 successfully.
Test scenario	Verify the following properties: 1. The `critical` field MUST be absent.
Expected results	1. True

Test-ID	CERT_CDP_4
Purpose	Verify that the `CRLDistributionPoints` extension is in conformance with Doc9303-12.
Version	0.40
References	[Doc9303-12] Table 6 and clause 7.1.1.4 [TR VDS-NC] clause 3.6
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_CDP_1 or CERT_CDP_2 successfully.
Test scenario	Verify the following properties: 1. The `CRLDistributionPoints` sequence contains at least 1 `DistributionPoint` sequence. 2. In every `DistributionPoint` sequence the `distributionPoint` MUST be present. 3. In every `DistributionPoint` sequence `reasons` MUST be absent. 4. In every `DistributionPoint` sequence `cRLIssuer` MUST be absent.
Expected results	1. True 2. True 3. True 4. True

Test-ID	CERT_CDP_5
Purpose	Verify that the `distributionPoint` is encoded as http, https or ldap.
Version	0.40
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6 [RFC5280] clause 4.2.1.13
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_CDP_4 successfully.
Test scenario	Verify the following properties for every `DistributionPoint` in the `CRLDistributionPoints` sequence: 1. The `distributionPoint` is encoded as `fullName`, i.e. a sequence of `GeneralName`. 2. Every `GeneralName` is encoded either as `directoryName` or `uniformResourceIdentifier`. 3. The `uniformResourceIdentifier` MUST contain either a. an http URI according to [RFC2616] or b. an https URI according to [RFC2616] or c. an ldap URI according to [RFC4516] or d. a `directoryName`.
Expected results	1. True 2. True 3. True

3.13.11 Private Internet Extensions

For the profiles CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM, SPOC-C and SPOC-S the test cases CERT_PIE_1 and CERT_PIE_2 are conditional. A CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM, SPOC Client or SPOC Server certificate must pass these test case successfully if a Private Internet Extension is present.

Test-ID	CERT_PIE_1
Purpose	Verify that at most 1 instance of every type of Private Internet Extension is present.
Version	0.40
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6 [RFC5280] clause 4.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully. 2. The certificate contains an optional Private Internet Extension.
Test scenario	Verify the following properties for every type of extension that meets the preconditions: 1. The `extensions` MUST contain exactly 1 instance of this type of extension.
Expected results	1. True

Test-ID	CERT_PIE_2
Purpose	Verify that the Private Internet Extension's criticality is in conformance with Doc9303-12.
Version	0.40
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6

Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_PIE_1 successfully.
Test scenario	Verify the following properties for every type of extension that meets the preconditions: 1. The `critical` field MUST be absent.
Expected results	1. True

3.13.12 NameChange Extension

The test cases in this clause are conditional: A CSCA Link certificate must either pass the test cases CERT_NCH_1 and CERT_NCH_2 (if a `NameChange` extension is present in the CSCA Link certificate) or CERT_NCH_5 and CERT_NCH_6 (if no `NameChange` extension is present in the CSCA Link certificate).The new CSCA Root certificate must either pass test case CERT_NCH_3 (if a `NameChange` extension is present in the CSCA Link certificate) or CERT_NCH_4 (if no `NameChange` extension is present in the CSCA Link certificate).

Test-ID	CERT_NCH_1
Purpose	Verify that at most 1 instance of the `NameChange` extension is present.
Version	0.40
References	[Doc9303-12] Table 6 [RFC5280] clause 4.2
Profile	CSCA-Root, CSCA-Link
Preconditions	1. The certificate contains the optional `NameChange` extension.
Test scenario	Verify the following properties: 1. The `extensions` MUST contain exactly 1 instance of the `NameChange` extension.
Expected results	1. True

Test-ID	CERT_NCH_2
Purpose	Verify that the `NameChange` extension's criticality is in conformance with Doc9303-12.
Version	0.40
References	[Doc9303-12] Table 6
Profile	CSCA-Root, CSCA-Link
Preconditions	1. The certificate contains the optional `NameChange` extension.
Test scenario	Verify the following properties: 1. The `critical` field MUST be absent.
Expected results	1. True

Test-ID	CERT_NCH_3
Purpose	Verify that a name change has taken place if the `NameChange` extension is present in the CSCA Link certificate.
Version	1.00
References	[Doc9303-12] clause 7.1.1.5
Profile	CSCA-Root-New
Preconditions	1. The corresponding CSCA Link certificate has passed the test case CERT_NCH_1 successfully. 2. The new CSCA Root certificate has passed the test cases CERT_SUB_1, CERT_SAN_1 successfully. 3. The CSCA Link certificate has passed the test cases CERT_SUB_1, CERT_SAN_1 successfully. 4. The old CSCA Root certificate has passed the test case CERT_SUB_1

	successfully.
Test scenario	Verify the following properties: 1. The new CSCA Root certificate's `subject` value MUST exactly match the `subject` value of the corresponding CSCA Link certificate. 2. The new CSCA Root certificate's `subjectAltName` value MUST exactly match the `subjectAltName` value of the corresponding CSCA Link certificate. 3. The new CSCA Root certificate's `subject` value MUST NOT exactly match the `subject` field of the corresponding old CSCA Root certificate.
Expected results	1. True 2. True 3. True

Test-ID	CERT_NCH_4
Purpose	Verify that no name change has taken place, if the `NameChange` extension is absent in the CSCA Link certificate.
Version	1.00
References	[Doc9303-12] clause 7.1.1.5
Profile	CSCA-Root-New
Preconditions	1. The corresponding CSCA Link certificate does not contain the `NameChange` extension. 2. The new CSCA Root certificate has passed the test cases CERT_SUB_1, CERT_SAN_1 successfully. 3. The CSCA Link certificate has passed the test cases CERT_SUB_1, CERT_SAN_1 successfully. 4. The old CSCA Root certificate has passed the test case CERT_SUB_1 successfully.
Test scenario	Verify the following properties: 1. The new CSCA Root certificate's `subject` value MUST exactly match the `subject` value of the corresponding CSCA Link certificate. 2. The new CSCA Root certificate's `subjectAltName` value MUST exactly match the `subjectAltName` value of the corresponding CSCA Link certificate. 3. The new CSCA Root certificate's `subject` value MUST exactly match the `subject` value of the corresponding old CSCA Root certificate.
Expected results	1. True 2. True 3. True

Test-ID	CERT_NCH_5
Purpose	Verify that a name change has taken place if the `NameChange` extension is present in a CSCA Link certificate.
Version	1.00
References	[Doc9303-12] clause 7.1.1.5
Profile	CSCA-Link
Preconditions	1. The CSCA Link certificate has passed the test case CERT_NCH_1 successfully. 2. The CSCA Link certificate has passed the test cases CERT_ISS_1, CERT_SUB_1 successfully.
Test scenario	Verify the following properties: 1. The `issuer` value does not exactly match the `subject` value.

Expected results	1. True

Test-ID	CERT_NCH_6
Purpose	Verify that no name change has taken place, if the `NameChange` extension is absent in a CSCA Link certificate.
Version	1.00
References	[Doc9303-12] clause 7.1.1.5
Profile	CSCA-Link
Preconditions	1. The CSCA Link certificate contains no `NameChange` extension. 2. The CSCA Link certificate has passed the test cases CERT_ISS_1, CERT_SUB_1 successfully.
Test scenario	Verify the following properties: 1. The `issuer` value MUST exactly match the `subject` value.
Expected results	1. True

3.13.13 DocumentType Extension

Test-ID	CERT_DTL_1
Purpose	Verify that the `DocumentType` extension is present.
Version	0.40
References	[Doc9303-12] Table 6 [TR VDS-NC] clause 3.6.4 [RFC5280] clause 4.2
Profile	DS PoR-S, PoT-S, PoV-S, DTA-S
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully.
Test scenario	Verify the following properties: 1. The `extensions` MUST contain exactly 1 instance of the `DocumentType` extension.
Expected results	1. True

Test-ID	CERT_DTL_2
Purpose	Verify that the `DocumentType` extension's criticality is in conformance with Doc9303-12.
Version	0.20
References	[Doc9303-12] Table 6 and 8 and clause 7.1.1.6 [TR VDS-NC] clause 3.6.4
Profile	DS PoR-S, PoT-S, PoV-S, DTA-S
Preconditions	1. The certificate has passed the test case CERT_DTL_1 or CERT_DTL_4 successfully.
Test scenario	Verify the following properties: 1. The `critical` field MUST be absent.
Expected results	1. True

Note: The test case CERT_DTL_2 does not apply to the BCS profile as [Doc9303-12] Table 8 does not specify the criticality.

Test-ID	CERT_DTL_3
Purpose	Verify that the `DocumentType` extension is in conformance with Doc9303-12.
Version	0.20
References	[Doc9303-12] Table 6 and 8 and clause 7.1.1.6 [TR VDS-NC] clause 3.6.4
Profile	DS

	PoR-S, PoT-S, PoV-S, DTA-S, BCS
Preconditions	1. The certificate has passed the test case CERT_DTL_1 or CERT_DTL_4 successfully.
Test scenario	Verify the following properties: 1. The `version` MUST be set to 0.
Expected results	1. True

Test-ID	CERT_DTL_4
Purpose	Verify that at most 1 instance of the `DocumentType` extension is present.
Version	1.10
References	[Doc9303-12] Table 8 [RFC5280] clause 4.2
Profile	BCS
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully. 2. The optional `DocumentType` extension is present.
Test scenario	Verify the following properties: 1. The `extensions` MUST contain exactly 1 instance of the `DocumentType` extension.
Expected results	1. True

Test-ID	CERT_DTL_5
Purpose	Verify that the `DocumentType` extension contains the correct document type value.
Version	1.10
References	[TR VDS-NC] clause 4.3.1
Profile	PoR-S
Preconditions	1. The certificate has passed the test case CERT_DTL_1 successfully.
Test scenario	Verify the following properties: 1. The `docTypeList` MUST contain a `DocumentType` with the value NR.
Expected results	1. True

Test-ID	CERT_DTL_6
Purpose	Verify that the `DocumentType` extension contains the correct document type value.
Version	1.10
References	[TR VDS-NC] clause 4.1.1
Profile	PoT-S
Preconditions	1. The certificate has passed the test case CERT_DTL_1 successfully.
Test scenario	Verify the following properties: 1. The `docTypeList` MUST contain a `DocumentType` with the value NT.
Expected results	1. True

Test-ID	CERT_DTL_7
Purpose	Verify that the `DocumentType` extension contains the correct document type value.
Version	1.10
References	[TR VDS-NC] clause 4.2.1
Profile	PoV-S
Preconditions	1. The certificate has passed the test case CERT_DTL_1 successfully.
Test scenario	Verify the following properties: 1. The `docTypeList` MUST contain a `DocumentType` with the value NV.
Expected results	1. True

Test-ID	CERT_DTL_8
Purpose	Verify that the `DocumentType` extension contains the correct document type value.
Version	1.10
References	[TR DTA] clause 3.2
Profile	DTA-S
Preconditions	1. The certificate has passed the test case CERT_DTL_1 successfully.
Test scenario	Verify the following properties: 1. The `docTypeList` MUST contain a `DocumentType` with the value ND.
Expected results	1. True

3.13.14 Other Private Extensions

For the profiles CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM, SPOC-C and SPOC-S the test cases CERT_OPE_1 and CERT_OPE_2 are conditional. A CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM, SPOC Client or SPOC Server certificate must pass these test cases successfully if an "other private extension" is present.

Test-ID	CERT_OPE_1
Purpose	Verify that at most 1 instance of every type of other private extension is present.
Version	0.40
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6 [RFC5280] clause 4.2
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_EXT_1 successfully. 2. The certificate contains an 'other private extension' (see Doc9303-12 Table 6).
Test scenario	Verify the following properties for every type of extension that meets the preconditions: 1. The `extensions` MUST contain exactly 1 instance of this type of extension.
Expected results	1. True

Test-ID	CERT_OPE_2
Purpose	Verify that other private extension's criticality is in conformance with Doc9303-12.
Version	0.40
References	[Doc9303-12] Table 6 and clause 7 [TR VDS-NC] clause 3.6
Profile	CSCA-Root, CSCA-Link, CA-VDS-NC, DS, MLS, DLS, TL-S, COMM SPOC-C, SPOC-S
Preconditions	1. The certificate has passed the test case CERT_OPE_1 successfully.
Test scenario	Verify the following properties for every type of extension that meets the preconditions: 1. The `critical` field MUST be absent.
Expected results	1. True

4 Certificate Revocation List Tests

This clause covers all CRL tests. All tests are mandatory, i.e. a CRL must pass these test cases successfully, unless marked as optional or conditional.

4.1 CertificateList

Test-ID	CRL_CERT_1
Purpose	Verify that the CRL has an ASN.1 structure and is DER encoded.
Version	0.40
References	[Doc9303-12] clause 7
Profile	CRL
Preconditions	-
Test scenario	Verify the following properties: 1. The CRL MUST be DER encoded. 2. The CRL MUST have an ASN.1 structure. (Note: This test case does not require that the CRL follows the specified ASN.1 schema.)
Expected results	1. True 2. True

Test-ID	CRL_CERT_2
Purpose	Verify that the structure of the CRL is in conformance with Doc9303-12.
Version	0.40
References	[Doc9303-12] Table 9
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_CERT_1 successfully.
Test scenario	Verify the following properties 1. The `CertificateList` sequence MUST contain the `tbsCertList` field. 2. The `CertificateList` sequence MUST contain the `signatureAlgorithm` field. 3. The `CertificateList` sequence MUST contain the `signatureValue` field.
Expected results	1. True 2. True 3. True

4.2 signatureAlgorithm

Test-ID	CRL_ALG_1
Purpose	Verify that the `signatureAlgorithm` value is in conformance with Doc9303-12.
Version	0.40
References	[Doc9303-12] clause 4.1.6 [RFC4055] clauses 3, 3.1, and 5 [RFC5758] clause 3.1
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_CERT_2 successfully.
Test scenario	See clause 7.1.
Expected results	See clause 7.1.

The test case CRL_ALG_2 is conditional. A CRL must pass the test case successfully if precondition 3 is fullfiled.

Test-ID	CRL_ALG_2

Purpose	In case of RSASSA-PSS verify that the `signatureAlgorithm` parameters match the parameters of the corresponding public key.
Version	0.30
References	[RFC4055] clause 3.3
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_ALG_1 successfully. 2. The issuing CSCA Root certificate has passed the test case CERT_RSA_2 successfully. 3. The parameters are present in the issuing CSCA Root certificate's `subjectPublicKeyInfo`.
Test scenario	Verify the following properties: 1. The `hashAlgorithm` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST match the `hashAlgorithm` in the issuing CSCA Root certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`. 2. The `maskGenAlgorithm` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST match the `maskGenAlgorithm` in the issuing CSCA Root certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`. 3. The `saltLength` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST be greater or equal than the `saltLength` value in the issuing CSCA Root certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`. 4. The `trailerField` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST match the `trailerField` in the issuing CSCA Root certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`, i.e. MUST be absent.
Expected results	1. True 2. True 3. True 4. True

4.3 signatureValue

Test-ID	CRL_SIGV_1
Purpose	Verify the cryptographic signature of the CRL.
Version	0.40
References	[Doc9303-12] Table 9
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_CERT_2 successfully. 2. The issuing CSCA Root certificate has passed the test case CERT_SIGV_1 successfully.
Test scenario	1. Verify the signature over the CRL using the signature from the CRL's `signatureValue` field the algorithm from the CRL's `signatureAlgorithm` field and the public key from the issuing CSCA Root certificate's `subjectPublicKeyInfo` field the corresponding public key parameters. The signature MUST be valid.
Expected results	1. True

4.4 version

Test-ID	CRL_VER_1
Purpose	Verify that the `version` field is present in `tbsCertList`.
Version	0.40
References	[Doc9303-12] Table 9
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_CERT_2 successfully.
Test scenario	Verify the following properties: 1. The `tbsCertList` sequence MUST contain the `version` field.
Expected results	1. True

Test-ID	CRL_VER_2
Purpose	Verify that the `version` value is in conformance with Doc9303-12.
Version	0.20
References	[Doc9303-12] Table 9
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_VER_1 successfully.
Test scenario	Verify the following properties: 1. The `version` value MUST be `v2`.
Expected results	1. True

4.5 signature

Test-ID	CRL_SIG_1
Purpose	Verify that the `signature` field is present in `tbsCertList`.
Version	0.40
References	[Doc9303-12] Table 9
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_CERT_2 successfully.
Test scenario	Verify the following properties: 1. The `tbsCertList` sequence MUST contain the `signature` field.
Expected results	1. True

Test-ID	CRL_SIG_2
Purpose	Verify that the `signature` field is in accordance with the `signatureAlgorithm` field in the sequence `CertificateList`.
Version	0.20
References	[Doc9303-12] Table 9
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_SIG_1 successfully.
Test scenario	Verify the following properties: 1. The `signature` field MUST contain the same algorithm identifier as the `signatureAlgorithm` field in the sequence `CertificateList`.
Expected results	1. True

4.6 issuer

Test-ID	CRL_ISS_1
Purpose	Verify that the `issuer` field is present in `tbsCertList`.
Version	0.40
References	[Doc9303-12] Table 9
Profile	CRL

Preconditions	1. The CRL has passed the test case CRL_CERT_2 successfully.
Test scenario	Verify the following properties: 1. The `tbsCertList` sequence MUST contain the `issuer` field.
Expected results	1. True

Test-ID	CRL_ISS_2
Purpose	Verify that the `issuer` field is in conformance with Doc9303-12.
Version	0.20
References	[Doc9303-12] Table 9
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_ISS_1 successfully.
Test scenario	Verify the following properties: 1. The `countryName` MUST be present. 2. The `countryName` MUST be upper case. 3. The `countryName` MUST be a `PrintableString`. 4. The `serialNumber`, if present, MUST be `PrintableString`. 5. Other attributes that have `DirectoryString` syntax, if present, MUST be either `PrintableString` or `UTF8String`.
Expected results	1. True 2. True 3. True 4. True 5. True

Test-ID	CRL_ISS_3
Purpose	Verify that the CRL's `issuer` matches the `subject` of the issuing CSCA Root certificate.
Version	0.40
References	[RFC5280] clause 4.1.2.4 and clause 5.1.2.3
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_ISS_1 successfully. 2. The issuing CSCA Root certificate has passed the test case CERT_SUB_1 successfully.
Test scenario	Verify the following properties: 1. The CRL's `issuer` value MUST exactly match the `subject` value of the CRL's issuing CSCA Root certificate.
Expected results	1. True

4.7 thisUpdate

Test-ID	CRL_TUP_1
Purpose	Verify that the `thisUpdate` field is present in `tbsCertList`.
Version	0.40
References	[Doc9303-12] Table 9
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_CERT_2 successfully.
Test scenario	Verify the following properties: 1. The `tbsCertList` sequence MUST contain the `thisUpdate` field.
Expected results	1. True

Test-ID	CRL_TUP_2
Purpose	Verify that the `thisUpdate` field is in conformance with Doc9303-12.
Version	0.40

References	[Doc9303-12] Table 9
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_TUP_1 successfully.
Test scenario	Verify the following properties: See clause 7.2
Expected results	See clause 7.2

4.8 nextUpdate

Test-ID	CRL_NUP_1
Purpose	Verify that the `nextUpdate` field is present in `tbsCertList`.
Version	0.40
References	[Doc9303-12] Table 9
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_CERT_2 successfully.
Test scenario	Verify the following properties: 1. The `tbsCertList` sequence MUST contain the `nextUpdate` field.
Expected results	1. True

Test-ID	CRL_NUP_2
Purpose	Verify that the `nextUpdate` field is in conformance with Doc9303-12.
Version	0.40
References	[Doc9303-12] Table 9
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_NUP_1 successfully.
Test scenario	Verify the following properties: See clause 7.2
Expected results	See clause 7.2

4.9 RevokedCertificates

All test cases in this clause are conditional. A CRL must pass all test cases successfully, if the `revokedCertificates` field is present.

Test-ID	CRL_REC_1
Purpose	Verify that `revokedCertificates` contains the fields specified by Doc9303-12.
Version	0.40
References	[Doc9303-12] Table 9
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_CERT_2 successfully. 2. The `revokedCertificates` field is present.
Test scenario	Verify the following properties for every component of the `revokedCertificates` sequence: 1. The `userCertificate` MUST be present. 2. The `revocationDate` MUST be present. 3. The `crlEntryExtensions` MUST be absent.
Expected results	1. True 2. True 3. True

Note: The test specification does not verify that the `userCertificate` field contains a certificate serial number according to [Doc9303-12] Table 5 (positive integer, maximum 20 octets, represented in the smallest number of octets). The `userCertificate` field may contain a certificate serial number that does not match [Doc9303-12] Table 5 in order to revoke a certificate with a non-standard serial number.

Test-ID	CRL_REC_3
Purpose	Verify that the `revocationDate` field is in conformance with Doc9303-12.
Version	0.30
References	[Doc9303-12] Table 9 [RFC5280] clause 5.1.2.6
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_REC_1 successfully.
Test scenario	Verify the following properties for every `revocationDate` field in `revokedCertificates`: See clause 7.2
Expected results	See clause 7.2

4.10 crlExtensions

Test-ID	CRL_EXT_1
Purpose	Verify that the `crlExtensions` field is present in `tbsCertList`.
Version	0.40
References	[Doc9303-12] Table 9
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_CERT_2 successfully.
Test scenario	Verify the following properties: 1. The `tbsCertList` sequence MUST contain the `crlExtensions` field.
Expected results	1. True

Test-ID	CRL_EXT_2
Purpose	Verify that extensions which must not be used according to Doc9303-12 are absent in the `crlExtensions` field.
Version	0.40
References	[Doc9303-12] Table 10
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_EXT_1 successfully.
Test scenario	Verify the following properties: 1. The `crlExtensions` sequence MUST NOT contain extensions that are marked as ‘do not use (x)’ in Doc9303-12 Table 10.
Expected results	1. True

Note: Test case CRL_EXT_3 has been deleted in version 1.10.

The test case CRL_EXT_4 is conditional. A CRL must pass the test case successfully if precondition 2 is fullfiled.

Test-ID	CRL_EXT_4
Purpose	Verify that private extensions are non-critical.
Version	1.10
References	[Doc9303-12] table 10
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_EXT_1 successfully.

	2. The `crlExtensions` field contains a private extension.
Test scenario	Verify the following properties for every type of extension that meets the preconditions: 1. The extension's `critical` field MUST be absent.
Expected results	1. True

4.10.1 **AuthorityKeyIdentifier**

Test-ID	CRL_AKI_1
Purpose	Verify that the `AuthorityKeyIdentifier` extension is present.
Version	0.40
References	[Doc9303-12] Table 10
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_EXT_1 successfully.
Test scenario	Verify the following properties: 1. The `crlExtensions` MUST contain exactly 1 instance of the `AuthorityKeyIdentifier` extension.
Expected results	1. True

Test-ID	CRL_AKI_2
Purpose	Verify that the `AuthorityKeyIdentifier` extension's criticality is in conformance with Doc9303-12.
Version	0.20
References	[Doc9303-12] Table 9 and Table 10
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_AKI_1 successfully.
Test scenario	Verify the following properties: 1. The `critical` field MUST be absent.
Expected results	1. True

Test-ID	CRL_AKI_3
Purpose	Verify that the `AuthorityKeyIdentifier` extension contains a `keyIdentifier`.
Version	0.20
References	[Doc9303-12] Table 10
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_AKI_1 successfully.
Test scenario	Verify the following properties: 1. The `keyIdentifier` MUST be present in the `AuthorityKeyIdentifier` sequence.
Expected results	1. True

Test-ID	CRL_AKI_4
Purpose	Verify that the `AuthorityKeyIdentifier` value is identical to the `subjectKeyIdentifier` value of the issuing CSCA Root certificate.
Version	0.40
References	[Doc9303-12] Table 10
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_AKI_3 successfully. 2. The issuing CSCA Root certificate has passed the test case CERT_SKI_4 successfully.
Test scenario	Verify the following properties:

	1. The `keyIdentifier` value in the CRL's `AuthorityKeyIdentifier` extension MUST be identical to the `subjectKeyIdentifier` value of the issuing CSCA Root certificate's `SubjectKeyIdentifier` extension.
Expected results	1. True

4.10.2 **IssuerAltName**

All test cases in this clause are conditional. A CRL must pass all test cases successfully, if an `IssuerAltName` extension is present.

Test-ID	CRL_IAN_1
Purpose	Verify that at most 1 instance of the `IssuerAltName` extension is present.
Version	0.40
References	[Doc9303-12] Table 10
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_EXT_1 successfully. 2. The `crlExtensions` contains the optional `IssuerAltName` extension.
Test scenario	Verify the following properties: 1. The `crlExtensions` MUST contain exactly 1 instance of the `IssuerAltName` extension.
Expected results	1. True

Test-ID	CRL_IAN_2
Purpose	Verify that the `IssuerAltName` extension's criticality is in conformance with Doc9303-12.
Version	0.40
References	[Doc9303-12] Table 9 and Table 10
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_IAN_1 successfully.
Test scenario	Verify the following properties: 1. The `critical` field MUST be absent.
Expected results	1. True

4.10.3 **CRLNumber**

Test-ID	CRL_CRN_1
Purpose	Verify that the `CRLNumber` extension is present.
Version	0.40
References	[Doc9303-12] Table 10
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_EXT_1 successfully.
Test scenario	Verify the following properties: 1. The `crlExtensions` MUST contain exactly 1 instance of the `CRLNumber` extension.
Expected results	1. True

Test-ID	CRL_CRN_2
Purpose	Verify that the `CRLNumber` extension's criticality is in conformance with Doc9303-12.
Version	0.20
References	[Doc9303-12] Table 9 and Table 10
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_CRN_1 successfully.

Test scenario	Verify the following properties: 1. The `critical` field MUST be absent.
Expected results	1. True

Test-ID	CRL_CRN_3
Purpose	Verify that the `CRLNumber` extension is in conformance with Doc9303-12.
Version	0.40
References	[Doc9303-12] Table 10
Profile	CRL
Preconditions	1. The CRL has passed the test case CRL_CRN_1 successfully.
Test scenario	Verify the following properties: 1. MUST be non-negative integer. 2. MUST be maximum 20 octets. 3. MUST be represented in the smallest number of octets.
Expected results	1. True 2. True 3. True

Note: The Doc9303-12 Table 10 requirement “MUST use 2’s complement encoding” is implicitly tested.

5 Master List and Trust List Tests

This clause covers all Master List and Trust List tests. All tests are mandatory, i.e. a Master List, Trust List must pass these test cases successfully, unless marked as optional or conditional.

5.1 ContentInfo

Test-ID	ML_CIN_1
Purpose	Verify that the List has an ASN.1 structure and is DER encoded.
Version	1.10
References	[Doc9303-12] clause 9 [TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	-
Test scenario	Verify the following properties: 1. The List MUST be DER encoded. 2. The List MUST have an ASN.1 structure. (Note: This test case does not require that the List follows the specified ASN.1 schema.)
Expected results	1. True 2. True

Test-ID	ML_CIN_2
Purpose	Verify that the structure of the List is in conformance with the ICAO specifications.
Version	1.10
References	[Doc9303-12] Table 18 [TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_CIN_1 successfully.
Test scenario	Verify the following properties: 1. The `ContentInfo` sequence MUST contain the `contentType` field. 2. The `ContentInfo` sequence MUST contain the `signedData` field.
Expected results	1. True 2. True

5.2 contentType

Test-ID	ML_CTY_1
Purpose	Verify that the `contentType` denotes the signed data type.
Version	1.10
References	[Doc9303-12] clause 18 [TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_CIN_2 successfully.
Test scenario	Verify the following properties: 1. The `contentType` in the `ContentInfo` sequence MUST be `id-signedData` [RFC5652].
Expected results	1. True

5.3 version

Test-ID	ML_VER_1
Purpose	Verify that the `version` field is present in `signedData`.
Version	1.10

References	[Doc9303-12] Table 18 [TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_CIN_2 successfully.
Test scenario	Verify the following properties: 1. The `signedData` sequence MUST contain the `version` field.
Expected results	1. True

Test-ID	ML_VER_2
Purpose	Verify that the `version` value under `signedData` is in conformance with the ICAO specifications.
Version	1.10
References	[Doc9303-12] Table 18 [TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_VER_1 successfully.
Test scenario	Verify the following properties: 1. The `version` value MUST be `v3`.
Expected results	1. True

5.4 digestAlgorithms

Test-ID	ML_DALG_1
Purpose	Verify that the `digestAlgorithms` field is present in `signedData`.
Version	1.10
References	[Doc9303-12] Table 18 [TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_CIN_2 successfully.
Test scenario	Verify the following properties: 1. The `signedData` sequence MUST contain the `digestAlgorithms` field.
Expected results	1. True

Note: Test case ML_DALG_2 has been deleted in version 1.10.

5.5 encapContentInfo

Test-ID	ML_ECI_1
Purpose	Verify that the `encapContentInfo` field is present in `signedData`.
Version	1.10
References	[Doc9303-12] Table 18 [TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_CIN_2 successfully.
Test scenario	Verify the following properties: 1. The `signedData` sequence MUST contain the `encapContentInfo` field.
Expected results	1. True

5.5.1 eContentType

Test-ID	ML_ECT_1
Purpose	Verify that the `eContentType` field is present in `encapContentInfo`.
Version	1.10
References	[Doc9303-12] Table 18 [TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_ECI_1 successfully.
Test scenario	Verify the following properties: 1. The `encapContentInfo` sequence MUST contain the `eContentType` field.
Expected results	1. True

Test-ID	ML_ECT_2
Purpose	Verify that the `eContentType` field is in conformance with Doc9303-12.
Version	0.20
References	[Doc9303-12] Table 18
Profile	ML
Preconditions	1. The Master List has passed the test case ML_ECT_1 successfully.
Test scenario	Verify the following properties: 1. The `eContentType` MUST be `id-icao-cscaMasterList`.
Expected results	1. True

Test-ID	ML_ECT_3
Purpose	Verify that the `eContentType` field is in conformance with the ICAO specifications.
Version	1.10
References	[TR VDS-NC] clause 3.6.7
Profile	TL
Preconditions	1. The Trust List has passed the test case ML_ECT_1 successfully.
Test scenario	Verify the following properties: 1. The `eContentType` MUST be `id-icao-trustList`.
Expected results	1. True

5.5.2 eContent

Test-ID	ML_ECO_1
Purpose	Verify that the `eContent` field is present in `encapContentInfo`.
Version	1.10
References	[Doc9303-12] Table 18 [TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_ECI_1 successfully.
Test scenario	Verify the following properties: 1. The `encapContentInfo` sequence MUST contain the `eContent` field.
Expected results	1. True

Test-ID	ML_ECO_2
Purpose	Verify that the `eContent` field, i.e.the encoded contents of a `cscaMasterList`, is in conformance with Doc9303-12.
Version	1.00

References	[Doc9303-12] Table 18 and clause 9.2
Profile	ML
Preconditions	1. The Master List has passed the test case ML_ECO_1 successfully. 2. The Master List has passed the test case ML_SCE_2 successfully.
Test scenario	Verify the following properties: 1. The `version` value MUST be `v0`. 2. The `certList` MUST contain the CSCA Root certificate that belongs to the Master List Signer certificate, i.e. the `certList` MUST contain a certificate with a `subjectKeyIdentifier` that matches the Master List Signer certificate's `authorityKeyIdentier`. 3. All objects in the `certList` MUST successfully pass the test case CERT_CERT_2.
Expected results	1. True 2. True 3. True

Test-ID	ML_ECO_3
Purpose	Verify that the `eContent` field, i.e.the encoded contents of a `TrustList`, is in conformance with the ICAO specifications.
Version	1.10
References	[TR VDS-NC] clause 3.6.7
Profile	TL
Preconditions	1. The Trust List has passed the test case ML_ECO_1 successfully. 2. The Trust List has passed the test case ML_SCE_3 successfully.
Test scenario	Verify the following properties: 1. The `version` value MUST be `v0`. 2. The `certList` MUST contain the CSCA Root certificate that belongs to the Trust List Signer certificate, i.e. the `certList` MUST contain a certificate with a `subjectKeyIdentifier` that matches the Trust List Signer certificate's `authorityKeyIdentier`. 3. All objects in the `certList` MUST successfully pass the test case CERT_CERT_2.
Expected results	1. True 2. True 3. True

5.6 certificates

Test-ID	ML_SCE_1
Purpose	Verify that the `certificates` field is present in `signedData`.
Version	1.10
References	[Doc9303-12] Table 18 [TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_CIN_2 successfully.
Test scenario	Verify the following properties: 1. The `signedData` sequence MUST contain the `certificates` field.
Expected results	1. True

Test-ID	ML_SCE_2
Purpose	Verify that the `certificates` field contains the Master List Signer certificate.

Version	1.20
References	[Doc9303-12] Table 18
Profile	ML
Preconditions	1. The Master List has passed the test case ML_SCE_1 successfully. 2. The Master List has passed the test case ML_SID_1 successfully.
Test scenario	Verify the following properties: 1. Exactly one certificate in the `certificates` field MUST match the `sid` in the `signerInfo`. 2. This certificate MUST pass the test case CERT_EKU_5 for the MLS profile successfully.
Expected results	1. True 2. True

Test-ID	ML_SCE_3
Purpose	Verify that the `certificates` field contains the Trust List Signer certificate.
Version	1.20
References	[TR VDS-NC] clause 3.6.7
Profile	TL
Preconditions	1. The Trust List has passed the test case ML_SCE_1 successfully. 2. The Trust List has passed the test case ML_SID_1 successfully.
Test scenario	Verify the following properties: 1. Exactly one certificate in the `certificates` field MUST match the `sid` in the `signerInfo`. 2. This certificate MUST pass the test case CERT_EKU_5 for the TLS profile successfully.
Expected results	1. True 2. True

5.7 crls

Test-ID	ML_CRL_1
Purpose	Verify that the `crls` field is absent in `signedData`.
Version	1.10
References	[Doc9303-12] Table 18 [TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_CIN_2 successfully.
Test scenario	Verify the following properties: 1. The `signedData` sequence MUST NOT contain the `crls` field.
Expected results	1. True

5.8 signerInfos

Test-ID	ML_SIN_1
Purpose	Verify that the `signerInfos` field is present in `signedData`.
Version	1.10
References	[Doc9303-12] Table 18 [TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_CIN_2 successfully.
Test scenario	Verify the following properties:

	1. The `signedData` sequence MUST contain the `signerInfos` field.
Expected results	1. True

Note: Test case ML_SIN_2 has been deleted in version 1.10.

Test-ID	ML_SIN_3
Purpose	Verify that the `signerInfos` contains at least 1 `signerInfo`.
Version	1.10
References	[Doc9303-12] Table 18 [TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_SIN_1 successfully.
Test scenario	Verify the following properties: 1. The `signerInfos` MUST contain at least 1 `signerInfo` field.
Expected results	1. True

The test cases in clauses 5.8.1 to 5.8.6 must be executed for every `signerInfo` element. At least one `signerInfo` element must pass all the applicable test cases in clauses 5.8.1 to 5.8.6.

5.8.1 **version**

Test-ID	ML_SIV_1
Purpose	Verify that the `version` field is present in `signerInfo`.
Version	1.10
References	[Doc9303-12] Table 18 [TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_SIN_3 successfully.
Test scenario	Verify the following properties for the `signerInfo` element: 1. The `signerInfo` sequence MUST contain the `version` field.
Expected results	1. True

Test-ID	ML_SIV_2
Purpose	Verify that the `version` value under `signerInfo` is in conformance with RFC5652.
Version	1.10
References	[RFC5652] clause 5.3
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_SIV_1 successfully. 2. The List has passed the test case ML_SID_1 successfully.
Test scenario	Verify the following properties for the `signerInfo` element: 1. If `SignerIdentifier` is `issuerAndSerialNumber`, then the version MUST be 1. If the `SignerIdentifier` is `subjectKeyIdentifier`, then the version MUST be 3.
Expected results	1. True

5.8.2 **sid**

Test-ID	ML_SID_1
Purpose	Verify that the `sid` field is present in `signerInfo`.
Version	1.10
References	[Doc9303-12] Table 18

	[TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_SIN_3 successfully.
Test scenario	Verify the following properties for the `signerInfo` element: 1. The `signerInfo` sequence MUST contain the `sid` field.
Expected results	1. True

The test cases ML_SCE_2 and ML_SCE_3, see clause 5.6, cover the requirements on the `sid` field.

5.8.3 digestAlgorithm

Test-ID	ML_SDA_1
Purpose	Verify that the `digestAlgorithm` field is present in `signerInfo`.
Version	1.10
References	[Doc9303-12] Table 18 [TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_SIN_3 successfully.
Test scenario	Verify the following properties for the `signerInfo` element: 1. The `signerInfo` sequence MUST contain the `digestAlgorithm` field.
Expected results	1. True

Test-ID	ML_SDA_2
Purpose	Verify that the `digestAlgorithm` field contains a hashing algorithm specified in Doc9303-12.
Version	1.10
References	[Doc9303-12] Table 18 and clause 4.1.6 [TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_SDA_1 successfully.
Test scenario	Verify the following properties for the `signerInfo` element: 1. The `digestAlgorithm` field MUST contain an algorithm identifier specified in Table 11. 2. The parameters MUST be absent.
Expected results	1. True 2. True

5.8.4 signedAttrs

Test-ID	ML_SAT_1
Purpose	Verify that the `signedAttrs` field is present in `signerInfo`.
Version	1.10
References	[Doc9303-12] Table 18 [TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_SIN_3 successfully.
Test scenario	Verify the following properties for the `signerInfo` element: 1. The `signerInfo` sequence MUST contain the `signedAttrs` field.
Expected results	1. True

Test-ID	ML_SAT_2

Purpose	Verify that the `signedAttrs` field includes the signing time.
Version	1.10
References	[Doc9303-12] Table 18 [TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_SAT_1 successfully.
Test scenario	Verify the following properties for the `signerInfo` element: 1. The `signedAttrs` MUST include the `signingTime` Attribute.
Expected results	1. True

Test-ID	ML_SAT_3
Purpose	Verify that the `signingTime` attribute is in conformance with [RFC5652].
Version	1.10
References	[RFC5652] clause 11.3
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_SAT_2 successfully.
Test scenario	Verify the following properties: See clause 7.2
Expected results	See clause 7.2

Test-ID	ML_SAT_4
Purpose	Verify that the `signingTime` lies within the validity period of the Master List Signer certificate.
Version	0.50
References	[Doc9303-12] [RFC5652] Note: The referenced documents do not explicitly specify the corresponding requirement, but implicitly.
Profile	ML
Preconditions	1. The ML has passed the test case ML_SAT_2 successfully. 2. The Master List Signer's certificate has passed the test case CERT_VAL_1 successfully.
Test scenario	Verify the following properties: 1. The `signingTime` date MUST be equal to or after the Master List Signer certificate's `validity notBefore` date. 2. The `signingTime` date MUST be equal to or before the Master List Signer certificate's `validity notAfter` date.
Expected results	1. True 2. True

Test-ID	ML_SAT_5
Purpose	Verify that the `signedAttrs` field contains the `MessageDigest` attribute.
Version	1.10
References	[RFC5652] clause 5.3 and clause 11.2
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_SAT_1 successfully.
Test scenario	Verify the following properties for the `signerInfo` element: 1. The `signedAttrs` MUST contain exactly one instance of the `MessageDigest` attribute according to [RFC5652] clause 11.2. 2. The `MessageDigest` attribute MUST have a single attribute value.
Expected results	1. True

	2. True

Note: The test cases ML_SIG_2 and ML_SIG_3 verify that the MessageDigest attribute value is correct.

Test-ID	ML_SAT_6
Purpose	Verify that the `signedAttrs` field contains the `ContentType` attribute.
Version	1.10
References	[RFC5652] clause 5.3 and clause 11.1
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_SAT_1 successfully.
Test scenario	Verify the following properties: 1. The `signedAttrs` MUST contain exactly one instance of the `ContentType` attribute according to [RFC5652] clause 11.1. 2. The `ContentType` attribute MUST have a single attribute value.
Expected results	1. True 2. True

Test-ID	ML_SAT_7
Purpose	Verify that the `ContentType` attribute value is correct.
Version	0.30
References	[RFC5652] clause 11.1
Profile	ML
Preconditions	1. The Master List has passed the test case ML_SAT_6 successfully.
Test scenario	Verify the following properties: 1. The `ContentType` attribute value MUST be `id-icao-cscaMasterList`.
Expected results	1. True

Test-ID	ML_SAT_8
Purpose	Verify that the `signingTime` lies within the validity period of the Trust List Signer certificate.
Version	1.10
References	[TR VDS-NC] clause 3.6.7 [RFC5652] Note: The referenced documents do not explicitly specify the corresponding requirement, but implicitly.
Profile	TL
Preconditions	1. The TL has passed the test case ML_SAT_2 successfully. 2. The Trust List Signer's certificate has passed the test case CERT_VAL_1 successfully.
Test scenario	Verify the following properties: 1. The `signingTime` date MUST be equal to or after the Trust List Signer certificate's `validity notBefore` date. 2. The `signingTime` date MUST be equal to or before the Trust List Signer certificate's `validity notAfter` date.
Expected results	1. True 2. True

Test-ID	ML_SAT_9
Purpose	Verify that the `ContentType` attribute value is correct.
Version	1.10

References	[RFC5652] clause 11.1
Profile	TL
Preconditions	1. The Trust List has passed the test case ML_SAT_6 successfully.
Test scenario	Verify the following properties: 1. The `ContentType` attribute value MUST be `id-icao-trustList`.
Expected results	1. True

5.8.5 signatureAlgorithm

Test-ID	ML_ALG_1
Purpose	Verify that the `signatureAlgorithm` field is present in `signerInfo`.
Version	1.10
References	[Doc9303-12] Table 18 [TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_SIN_3 successfully.
Test scenario	Verify the following properties for the `signerInfo` element: 1. The `signerInfo` sequence MUST contain the `signatureAlgorithm` field.
Expected results	1. True

Test-ID	ML_ALG_2
Purpose	Verify that the `signatureAlgorithm` value is in conformance with Doc9303-12.
Version	1.10
References	[Doc9303-12] clause 4.1.6 [RFC4055] clauses 3, 3.1, and 5 [RFC4056] [RFC5754]
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_ALG_1 successfully.
Test scenario	See clause 7.1.
Expected results	See clause 7.1.

The test case ML_DALG_3 is conditional. A Master List must pass the test case successfully if precondition 3 is fullfiled.

Test-ID	ML_ALG_3
Purpose	In case of RSASSA-PSS verify that the `signatureAlgorithm` parameters match the parameters of the corresponding public key.
Version	0.40
References	[RFC4055] clause 3.3
Profile	ML
Preconditions	1. The Master List has passed the test case ML_ALG_2 successfully. 2. The Master List has passed the test case ML_SCE_2 successfully. 3. The Master List Signer certificate stored in the Master List's `certificates` field uses the OID `id-RSASSA-PSS` in `subjectPublicKeyInfo` and the parameters of type `RSASSA-PSS-params` are present.
Test scenario	Verify the following properties: 1. The Master List Signer certificate MUST pass the test case CERT_RSA_2 successfully.

	2. The `hashAlgorithm` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST match the `hashAlgorithm` in the Master List Signer certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`. 3. The `maskGenAlgorithm` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST match the `maskGenAlgorithm` in the Master List Signer certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`. 4. The `saltLength` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST be greater or equal than the `saltLength` value in the Master List Signer certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`. 5. The `trailerField` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST match the `trailerField` in the Master List Signer certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`, i.e. MUST be absent.
Expected results	1. True 2. True 3. True 4. True 5. True

The test case ML_DALG_4 is conditional. A Trust List must pass the test case successfully if precondition 3 is fullfiled.

Test-ID	ML_ALG_4
Purpose	In case of RSASSA-PSS verify that the `signatureAlgorithm` parameters match the parameters of the corresponding public key.
Version	1.10
References	[RFC4055] clause 3.3
Profile	TL
Preconditions	1. The Trust List has passed the test case ML_ALG_2 successfully. 2. The Trust List has passed the test case ML_SCE_3 successfully. 3. The Trust List Signer certificate stored in the Trust List's `certificates` field uses the OID `id-RSASSA-PSS` in `subjectPublicKeyInfo` and the parameters of type `RSASSA-PSS-params` are present.
Test scenario	Verify the following properties: 1. The Trust List Signer certificate MUST pass the test case CERT_RSA_2 successfully. 2. The `hashAlgorithm` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST match the `hashAlgorithm` in the Trust List Signer certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`. 3. The `maskGenAlgorithm` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST match the `maskGenAlgorithm` in the Trust List Signer certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`. 4. The `saltLength` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST be greater or equal than the `saltLength` value in the Trust List Signer certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`. 5. The `trailerField` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST match the `trailerField` in the Trust List Signer certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`, i.e. MUST be absent.

Expected results	1. True 2. True 3. True 4. True 5. True

5.8.6 signature

Test-ID	ML_SIG_1
Purpose	Verify that the `signature` field is present in `signerInfo`.
Version	1.10
References	[Doc9303-12] Table 18 [TR VDS-NC] clause 3.6.7
Profile	ML, TL
Preconditions	1. The List has passed the test case ML_SIN_3 successfully.
Test scenario	Verify the following properties for the `signerInfo` element: 1. The `signerInfo` sequence MUST contain the `signature` field.
Expected results	1. True

Test-ID	ML_SIG_2
Purpose	Verify the cryptographic signature of the Master List.
Version	0.40
References	[Doc9303-12] Table 18 and clause 5.3
Profile	ML
Preconditions	1. The Master List has passed the test case ML_SIG_1 successfully. 2. The Master List has passed the test case ML_SCE_2 successfully. 3. The `eContent` field contains the issuing CSCA Root certificate.
Test scenario	Verify the following properties: 1. The Master List Signer certificate stored in the `certificates` field MUST pass the test case CERT_SIGV_2 successfully. 2. Calculate the content message digest as described in [RFC5652] clause 5.4 using the algorithm indicated in the `digestAlgorithm`. This message digest value MUST be the same as the value of the `messageDigest` attribute included in the `signedAttributes` of the `SignedData signerInfo`. 3. Verify the signature using the signature value from the `signerInfo signature` field the algorithm from the `signerInfo signatureAlgorithm` field and the public key from the Master List Signer's certificate stored in the `signedData certificates` field; this certificate matches the `sid` in the `signerInfo` the corresponding public key parameters. The signature MUST be valid.
Expected results	1. True 2. True 3. True

Test-ID	ML_SIG_3
Purpose	Verify the cryptographic signature of the Trust List.
Version	1.10
References	[TR VDS-NC] clause 3.6.7

Profile	TL
Preconditions	1. The Trust List has passed the test case ML_SIG_1 successfully. 2. The Trust List has passed the test case ML_SCE_3 successfully.
Test scenario	Verify the following properties: 1. The Trust List Signer certificate stored in the `certificates` field MUST pass the test case CERT_SIGV_2 successfully. 2. Calculate the content message digest as described in [RFC5652] clause 5.4 using the algorithm indicated in the `digestAlgorithm`. This message digest value MUST be the same as the value of the `messageDigest` attribute included in the `signedAttributes` of the `SignedData signerInfo`. 3. Verify the signature using the signature value from the `signerInfo signature` field the algorithm from the `signerInfo signatureAlgorithm` field and the public key from the Trust List Signer's certificate stored in the `signedData certificates` field; this certificate matches the `sid` in the `signerInfo` the corresponding public key parameters. The signature MUST be valid.
Expected results	1. True 2. True 3. True

6 Deviation List Tests

This clause covers all Deviation List tests. All tests are mandatory, i.e. a Deviation List must pass these test cases successfully, unless marked as optional or conditional.

6.1 ContentInfo

Test-ID	DL_CIN_1
Purpose	Verify that the Deviation List has an ASN.1 structure and is DER encoded.
Version	0.40
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	-
Test scenario	Verify the following properties: 1. The Deviation List MUST be DER encoded. 2. The Deviation List MUST have an ASN.1 structure. (Note: This test case does not require that the Deviation List follows the specified ASN.1 schema.)
Expected results	1. True 2. True

Test-ID	DL_CIN_2
Purpose	Verify that the structure of the Deviation List is in conformance with Doc9303-12.
Version	0.40
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_CIN_1 successfully.
Test scenario	Verify the following properties: 1. The `ContentInfo` sequence MUST contain the `contentType` field. 2. The `ContentInfo` sequence MUST contain the `signedData` field.
Expected results	1. True 2. True

6.2 contentType

Test-ID	DL_CTY_1
Purpose	Verify that the `contentType` denotes the signed data type.
Version	0.40
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_CIN_2 successfully.
Test scenario	Verify the following properties: 1. The `contentType` in the `ContentInfo` sequence MUST be `id-signedData` [RFC3852].
Expected results	1. True

6.3 version

Test-ID	DL_VER_1
Purpose	Verify that the `version` field is present in `signedData`.
Version	0.40
References	[Doc9303-12] clause 10
Profile	DL

Preconditions	1. The Deviation List has passed the test case DL_CIN_2 successfully.
Test scenario	Verify the following properties: 1. The `signedData` sequence MUST contain the `version` field.
Expected results	1. True

Test-ID	DL_VER_2
Purpose	Verify that the `version` value under `signedData` is in conformance with Doc9303-12.
Version	0.20
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_VER_1 successfully.
Test scenario	Verify the following properties: 1. The `version` value MUST be `v3`.
Expected results	1. True

6.4 digestAlgorithms

Test-ID	DL_DALG_1
Purpose	Verify that the `digestAlgorithms` field is present in `signedData`.
Version	0.40
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_CIN_2 successfully.
Test scenario	Verify the following properties: 1. The `signedData` sequence MUST contain the `digestAlgorithms` field.
Expected results	1. True

Note: Test case DL_DALG_2 has been deleted in version 1.10.

6.5 encapContentInfo

Test-ID	DL_ECI_1
Purpose	Verify that the `encapContentInfo` field is present in `signedData`.
Version	0.40
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_CIN_2 successfully.
Test scenario	Verify the following properties: 1. The `signedData` sequence MUST contain the `encapContentInfo` field.
Expected results	1. True

6.5.1 eContentType

Test-ID	DL_ECT_1
Purpose	Verify that the `eContentType` field is present in `encapContentInfo`.
Version	0.40
References	[Doc9303-12] clause 10
Profile	DL

Preconditions	1. The Deviation List has passed the test case DL_ECI_1 successfully.
Test scenario	Verify the following properties: 1. The `encapContentInfo` sequence MUST contain the `eContentType` field.
Expected results	1. True

Test-ID	DL_ECT_2
Purpose	Verify that the `eContentType` field is in conformance with Doc9303-12.
Version	0.20
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_ECT_1 successfully.
Test scenario	Verify the following properties: 1. The `eContentType` MUST be `id-icao-DeviationList` (2.23.136.1.1.7).
Expected results	1. True

6.5.2 **eContent**

Test-ID	DL_ECO_1
Purpose	Verify that the `eContent` field is present in `encapContentInfo`.
Version	0.20
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_ECI_1 successfully.
Test scenario	Verify the following properties: 1. The `encapContentInfo` sequence MUST contain the `eContent` field.
Expected results	1. True

The content of the Deviation List's `eContent` field, i.e. the encoding of the deviations, is out of the scope of this version, see clause 1.1.

6.6 certificates

Test-ID	DL_SCE_1
Purpose	Verify that the `certificates` field is present in `signedData`.
Version	0.40
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_CIN_2 successfully.
Test scenario	Verify the following properties: 1. The `signedData` sequence MUST contain the `certificates` field.
Expected results	1. True

Test-ID	DL_SCE_2
Purpose	Verify that the `certificates` field contains the Deviation List Signer certificate.
Version	1.20
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_SCE_1 successfully.

	2. The Deviation List has passed the test case DL_SID_1 successfully.
Test scenario	Verify the following properties: 1. Exactly one certificate in the `certificates` field MUST match the `sid` in the `signerInfo`. 2. This certificate MUST pass the test case CERT_EKU_5 for the DLS profile successfully.
Expected results	1. True 2. True

6.7 crls

Test-ID	DL_CRL_1
Purpose	Verify that the `crls` field is absent in `signedData`.
Version	0.40
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_CIN_2 successfully.
Test scenario	Verify the following properties: 1. The `signedData` sequence MUST NOT contain the `crls` field.
Expected results	1. True

6.8 signerInfos

Test-ID	DL_SIN_1
Purpose	Verify that the `signerInfos` field is present in `signedData`.
Version	0.40
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_CIN_2 successfully.
Test scenario	Verify the following properties: 1. The `signedData` sequence MUST contain the `signerInfos` field.
Expected results	1. True

Note: Test case DL_SIN_2 has been deleted in version 1.10.

Test-ID	DL_SIN_3
Purpose	Verify that the `signerInfos` contains at least 1 `signerInfo`.
Version	1.10
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_SIN_1 successfully.
Test scenario	Verify the following properties: 1. The `signerInfos` MUST contain at least 1 `signerInfo` field.
Expected results	1. True

The test cases in clauses 6.8.1 to 6.8.7 must be executed for every `signerInfo` element. At least one `signerInfo` element must pass all the applicable test cases in clauses 6.8.1 to 6.8.7.

6.8.1 version

Test-ID	DL_SIV_1

Purpose	Verify that the `version` field is present in `signerInfo`.
Version	1.10
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_SIN_3 successfully.
Test scenario	Verify the following properties for the `signerInfo` element: 1. The `signerInfo` sequence MUST contain the `version` field.
Expected results	1. True

Test-ID	DL_SIV_2
Purpose	Verify that the `version` value under `signerInfo` is in conformance with RFC3852.
Version	0.40
References	[RFC3852] clause 5.3
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_SIV_1 successfully. 2. The Deviation List has passed the test case DL_SID_1 successfully.
Test scenario	Verify the following properties for the `signerInfo` element: 1. If `SignerIdentifier` is `issuerAndSerialNumber`, then the version MUST be 1. If the `SignerIdentifier` is `subjectKeyIdentifier`, then the version MUST be 3.
Expected results	1. True

6.8.2 sid

Test-ID	DL_SID_1
Purpose	Verify that the `sid` field is present in `signerInfo`.
Version	1.10
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_SIN_3 successfully.
Test scenario	Verify the following properties for the `signerInfo` element: 1. The `signerInfo` sequence MUST contain the `sid` field.
Expected results	1. True

The test case DL_SCE_2, see clause 6.6, covers the Doc9303-12 requirements on the `sid` field.

6.8.3 digestAlgorithm

Test-ID	DL_SDA_1
Purpose	Verify that the `digestAlgorithm` field is present in `signerInfo`.
Version	1.10
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_SIN_3 successfully.
Test scenario	Verify the following properties for the `signerInfo` element: 1. The `signerInfo` sequence MUST contain the `digestAlgorithm` field.
Expected results	1. True

Test-ID	DL_SDA_2
Purpose	Verify that the `digestAlgorithm` field contains a hashing algorithm

	specified in Doc9303-12.
Version	0.30
References	[Doc9303-12] clause 4.1.6
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_SDA_1 successfully.
Test scenario	Verify the following properties for the `signerInfo` element: 1. The `digestAlgorithm` field MUST contain an algorithm identifier specified in Table 11. 2. The parameters MUST be absent.
Expected results	1. True 2. True

6.8.4 **signedAttrs**

Test-ID	DL_SAT_1
Purpose	Verify that the `signedAttrs` field is present in `signerInfo`.
Version	1.10
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_SIN_3 successfully.
Test scenario	Verify the following properties for the `signerInfo` element: 1. The `signerInfo` sequence MUST contain the `signedAttrs` field.
Expected results	1. True

Test-ID	DL_SAT_2
Purpose	Verify that the `signedAttrs` field includes the signing time.
Version	0.30
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_SAT_1 successfully.
Test scenario	Verify the following properties for the `signerInfo` element: 1. The `signedAttrs` MUST include the `signingTime` Attribute.
Expected results	1. True

Test-ID	DL_SAT_3
Purpose	Verify that the `signingTime` attribute is in conformance with [RFC3852].
Version	0.40
References	[RFC3852] clause 11.3
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_SAT_2 successfully.
Test scenario	Verify the following properties: See clause 7.2
Expected results	See clause 7.2

Test-ID	DL_SAT_4
Purpose	Verify that the `signingTime` lies within the validity period of the Deviation List Signer certificate.
Version	0.50
References	[Doc9303-12] [RFC3852] Note: The referenced documents do not explicitly specify the corresponding requirement, but implicitly.

Profile	DL
Preconditions	1. The DL has passed the test case DL_SAT_2 successfully. 2. The Deviation List Signer's certificate has passed the test case CERT_VAL_1 successfully.
Test scenario	Verify the following properties: 1. The `signingTime` date MUST be equal to or after the Deviation List Signer certificate's `validity notBefore` date. 2. The `signingTime` date MUST be equal to or before the Deviation List Signer certificate's `validity notAfter` date.
Expected results	1. True 2. True

Test-ID	DL_SAT_5
Purpose	Verify that the `signedAttrs` field contains the `MessageDigest` attribute.
Version	0.30
References	[RFC3852] clause 5.3 and clause 11.2
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_SAT_1 successfully.
Test scenario	Verify the following properties for the `signerInfo` element: 1. The `signedAttrs` MUST contain exactly one instance of the `MessageDigest` attribute according to [RFC3852] clause 11.2. 2. The `MessageDigest` attribute MUST have a single attribute value.
Expected results	1. True 2. True

Note: The test case DL_SIG_2 verifies that the MessageDigest attribute value is correct.

Test-ID	DL_SAT_6
Purpose	Verify that the `signedAttrs` field contains the `ContentType` attribute.
Version	0.30
References	[RFC3852] clause 5.3 and clause 11.1
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_SAT_1 successfully.
Test scenario	Verify the following properties: 1. The `signedAttrs` MUST contain exactly 1 instance of the `ContentType` attribute according to [RFC3852] clause 11.1. 2. The `ContentType` attribute MUST have a single attribute value.
Expected results	1. True 2. True

Test-ID	DL_SAT_7
Purpose	Verify that the `ContentType` attribute value is correct.
Version	0.30
References	[RFC3852] clause 11.1
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_SAT_6 successfully.
Test scenario	Verify the following properties: 1. The `ContentType` attribute value MUST be `id-icao-DeviationList` (2.23.136.1.1.7).
Expected results	1. True

6.8.5 signatureAlgorithm

Test-ID	DL_ALG_1
Purpose	Verify that the `signatureAlgorithm` field is present in `signerInfo`.
Version	1.10
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_SIN_3 successfully.
Test scenario	Verify the following properties for the `signerInfo` element: 1. The `signerInfo` sequence MUST contain the `signatureAlgorithm` field.
Expected results	1. True

Test-ID	DL_ALG_2
Purpose	Verify that the `signatureAlgorithm` value is in conformance with Doc9303-12.
Version	0.20
References	[Doc9303-12] clause 4.1.6 [RFC4055] clauses 3, 3.1, and 5 [RFC4056] [RFC5754]
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_ALG_1 successfully.
Test scenario	See clause 7.1.
Expected results	See clause 7.1.

The test case DL_DALG_3 is conditional. A Deviation List must pass the test case successfully if precondition 3 is fullfiled.

Test-ID	DL_ALG_3
Purpose	In case of RSASSA-PSS verify that the `signatureAlgorithm` parameters match the parameters of the corresponding public key.
Version	0.40
References	[RFC4055] clause 3.3
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_ALG_2 successfully. 2. The Deviation List has passed the test case DL_SCE_2 successfully. 3. The Deviation List Signer certificate stored in the Deviation List's `certificates` field uses the OID `id-RSASSA-PSS` in `subjectPublicKeyInfo` and the parameters of type `RSASSA-PSS-params` are present.
Test scenario	Verify the following properties: 1. The Deviation List Signer certificate MUST pass the test case CERT_RSA_2 successfully. 2. The `hashAlgorithm` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST match the `hashAlgorithm` in the Deviation List Signer certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`. 3. The `maskGenAlgorithm` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST match the `maskGenAlgorithm` in the Deviation List Signer certificate's `subjectPublicKeyInfo` `RSASSA-PSS-params`. 4. The `saltLength` in the `signatureAlgorithm` `RSASSA-PSS-params` MUST be greater or equal than the `saltLength` value in the Deviation List Signer certificate's `subjectPublicKeyInfo` `RSASSA-`

	PSS-params. 5. The trailerField in the signatureAlgorithm RSASSA-PSS-params MUST match the trailerField in the Deviation List Signer certificate's subjectPublicKeyInfo RSASSA-PSS-params, i.e. MUST be absent.
Expected results	1. True 2. True 3. True 4. True 5. True

6.8.6 **signature**

Test-ID	DL_SIG_1
Purpose	Verify that the signature field is present in signerInfo.
Version	1.10
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_SIN_3 successfully.
Test scenario	Verify the following properties for the signerInfo element: 1. The signerInfo sequence MUST contain the signature field.
Expected results	1. True

Test-ID	DL_SIG_2
Purpose	Verify the cryptographic signature of the Deviation List.
Version	0.40
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_SIG_1 successfully. 2. The Deviation List has passed the test case DL_SCE_2 successfully.
Test scenario	Verify the following properties: 1. The Deviation List Signer certificate stored in the certificates field MUST pass the test case CERT_SIGV_2 successfully. 2. Calculate the content message digest as described in [RFC3852] clause 5.4 using the algorithm indicated in the digestAlgorithm. This message digest value MUST be the same as the value of the messageDigest attribute included in the signedAttributes of the SignedData signerInfo. 3. Verify the signature using the signature value from the signerInfo signature field the algorithm from the signerInfo signatureAlgorithm field and the public key from the Deviation List Signer's certificate stored in the signedData certificates field; this certificate matches the sid in the signerInfo the corresponding public key parameters. The signature MUST be valid.
Expected results	1. True 2. True 3. True

6.8.7 **unsignedAttrs**

Test-ID	DL_USA_1
Purpose	Verify that the `unsignedAttrs` field is absent in `signerInfo`.
Version	1.10
References	[Doc9303-12] clause 10
Profile	DL
Preconditions	1. The Deviation List has passed the test case DL_SIN_3 successfully.
Test scenario	Verify the following properties for each `signerInfo` element: 1. The `signerInfo` sequence MUST NOT contain the `unsignedAttrs` field.
Expected results	1. True

7 Generic Test Cases

This clause specifies generic test case templates for fields that are common to certificates, CRLs, Master Lists, and Deviation Lists. The test cases in clauses 3 to 6 refer to these templates and add the missing details such as Test-ID, Purpose, References, Profile, and Preconditions for the test case specification.

7.1 signatureAlgorithm

Test-ID	
Purpose	
Version	0.20
References	
Profile	
Preconditions	
Test scenario	Verify the following properties: 1. The `algorithm` in the `AlgorithmIdentifier` sequence MUST contain one of the OIDs listed in the following tables: Table 4 for RSASSA-PSS Table 5 for RSASSA-PKCS1_v15 Table 7 for ECDSA Table 10 for DSA 2. In case of ECDSA and DSA the `parameters` field MUST be absent. 3. In case of RSASSA-PSS the `parameters` field MUST be present and a. The parameters MUST follow the [RFC4055] clause 3.1 `RSASSA-PSS-params` ASN.1 syntax definition; b. The `hashAlgorithm` MUST use one of the OIDs listed in Table 11; c. The `maskGenAlgorithm` MUST use one of the Algorithm Identifiers listed in Table 6. 4. In case of RSASSA-PKCS1_v15 the `parameters` MUST be NULL.
Expected results	1. True 2. True 3. True a. True b. True c. True 4. True The test object MUST successfully pass test scenario step 1 and either 2, 3, or 4.

7.2 Time

Test-ID	
Purpose	
Version	0.40
References	
Profile	
Preconditions	
Test scenario	1. MUST terminate with Zulu (Z). 2. Seconds element MUST be present. 3. Dates through 2049 MUST be in `UTCTime`. 4. `UTCTime` MUST be represented as YYMMDDHHMMSSZ. 5. Dates in 2050 and beyond MUST be in `GeneralizedTime`.

	6. `GeneralizedTime` MUST NOT have fractional seconds. 7. `GeneralizedTime` MUST be represented as YYYYMMDDHHMMSSZ.
Expected results	1. True 2. True 3. True 4. True 5. True 6. True 7. True

8 Object Identifiers und Algorithm Identifiers

This clause lists OIDs and algorithm identifiers that are used in the test cases.

8.1 RSA

OID abbreviation	OID value	Reference
`id-RSASSA-PSS`	1.2.840.113549.1.1.10	[RFC4055]

Table 4 RSASSA-PSS OID

OID abbreviation	OID value	Reference
`sha224WithRSAEncryption`	1.2.840.113549.1.1.14	[RFC4055]
`sha256WithRSAEncryption`	1.2.840.113549.1.1.11	[RFC4055]
`sha384WithRSAEncryption`	1.2.840.113549.1.1.12	[RFC4055]
`sha512WithRSAEncryption`	1.2.840.113549.1.1.13	[RFC4055]

Table 5 RSASSA-PKCS1_v15 OIDs

Algorithm Identifier	Reference
`mgf1SHA224Identifier`	[RFC4055]
`mgf1SHA256Identifier`	[RFC4055]
`mgf1SHA384Identifier`	[RFC4055]
`mgf1SHA512Identifier`	[RFC4055]

Table 6 Mask Generation Function Algorithm Identifiers

8.2 ECDSA

OID abbreviation	OID value	Reference
`ecdsa-with-SHA224`	1.2.840.10045.4.3.1	[RFC5758]
`ecdsa-with-SHA256`	1.2.840.10045.4.3.2	[RFC5758]
`ecdsa-with-SHA384`	1.2.840.10045.4.3.3	[RFC5758]
`ecdsa-with-SHA512`	1.2.840.10045.4.3.4	[RFC5758]

Table 7 ECDSA OIDs

OID abbreviation	OID value	Reference
`prime-field`	1.2.840.10045.1.1	[RFC3279]
`characteristic-two-field`	1.2.840.10045.1.2	[RFC3279]

Table 8 `fieldType` OIDs

OID abbreviation	OID value	Parameters	Reference
`gnBasis`	1.2.840.10045.1.2.1.1	`NULL`	[RFC3279]
`tpBasis`	1.2.840.10045.1.2.1.2	`Trinomial`	[RFC3279]
`ppBasis`	1.2.840.10045.1.2.1.3	`Pentanomial`	[RFC3279]

Table 9 Characteristic 2 basis OIDs

8.3 DSA

OID abbreviation	OID value	Reference
`id-dsa-with-sha224`	2.16.840.1.101.3.4.3.1	[RFC5758]
`id-dsa-with-sha256`	2.16.840.1.101.3.4.3.2	[RFC5758]

Table 10 DSA OIDs

8.4 Hash algorithms

OID abbreviation	OID value	Reference
id-sha224	2.16.840.1.101.3.4.2.4	[RFC4055]
id-sha256	2.16.840.1.101.3.4.2.1	[RFC4055]
id-sha384	2.16.840.1.101.3.4.2.2	[RFC4055]
id-sha512	2.16.840.1.101.3.4.2.3	[RFC4055]

Table 11 Hash OIDs