Table B.4 *(continued)*

Certificate component	Section in RFC 5280	Presence	Criticality	Description
Signature algorithm	4.1.1.2	M		Options: `1.2.840.10045.4.3.2` (ECDSA-with SHA256) `1.2.840.10045.4.3.3` (ECDSA-with SHA384) `1.2.840.10045.4.3.4` (ECDSA with SHA512)
Signature value	4.1.1.3	M		Value according to the signature algorithm. By creating this signature, the CA certifies the binding between the public key material and the subject of the certificate, i.e. the issuing authority.
Key Presence: M mandatory O optional Criticality: C critical NC not critical				

B.1.6 TLS server certificate – issuing authority

The TLS server certificate is used to protect the server retrieval methods using TLS. See Table B.5 for details.

Table B.5 — TLS server certificate: issuing authority

Certificate component	Section in RFC 5280	Presence	Criticality	Description
Version	4.1.2.1	M		Shall be `v3`.
Serial number	4.1.2.2	M		Non-sequential positive, non-zero integer, shall contain at least 63 bits of output from a CSPRNG, should contain at least 71 bits of output from a CSPRNG, maximum 20 octets.
Signature	4.1.2.3	M		Value shall match the OID in the signature algorithm (below).
Issuer	4.1.2.4	M		Same exact binary value as the subject of IACA certificate
Validity	4.1.2.5	M		
Not before		M		Date on which the certificate validity period begins.
Not after		M		Maximum of 822 days after “Not before” date
Key Presence: M mandatory O optional C conditional Criticality: C critical NC not critical				

Table B.5 *(continued)*

Certificate component	Section in RFC 5280	Presence	Criticality	Description
Subject	4.1.2.6	M		`countryName` is mandatory. The value shall be in upper case and contain the ISO 3166-1 alpha-2 code of the issuing country, exactly the same value as in the issuing country data element. The `countryName` shall be `PrintableString`. `stateOrProvinceName` is optional. If this element is present in the IACA root certificate, this element shall be present and hold the same value. The value shall exactly match the value of the data element "issuing_jurisdiction", if that element is present on the mDL. `organizationName` is optional. Its value is at the discretion of the IACA. `commonName` shall be present. Its value is at the discretion of the IACA. `localityName` is optional. Its value is at the discretion of the IACA. `serialNumber` is optional. If present, it shall be a `PrintableString`. Attributes that have a `DirectoryString` and for which the encoding is not listed above syntax shall be either `PrintableString` or `UTF8String`.
Subject public key info	4.1.2.7	M		
algorithm		M		`1.2.840.10045.2.1` (Elliptic curve)
parameters		M		Implicitly specify curve parameters through an OID associated with one of the following curves specified in FIPS 186-4: `1.2.840.10045.3.1.7` (Curve P-256) `1.3.132.0.34` (Curve P-384) `1.3.132.0.35` (Curve P-521) Or one of the following curves specified in RFC 5639: `1.3.36.3.3.2.8.1.1.7` (brainpoolP256r1) `1.3.36.3.3.2.8.1.1.9` (brainpoolP320r1) `1.3.36.3.3.2.8.1.1.11` (brainpoolP384r1) `1.3.36.3.3.2.8.1.1.13` (brainpoolP512r1)
subjectPublicKey		M		Public key shall be encoded in uncompressed form.
X.509v3 extensions	4.2	M		Further extensions may be present if they are marked non-critical.

Key

Presence:

M mandatory

O optional

C conditional

Criticality:

C critical

NC not critical

Table B.5 *(continued)*

Certificate component	Section in RFC 5280	Presence	Criticality	Description
Authority key identifier	4.2.1.1	M	NC	
keyIdentifier		M		Same value as the subject key identifier of the IACA root certificate
Subject key identifier	4.2.1.2	M	NC	SHA-1 hash of the subject public key `BIT STRING` value (excluding tag, length, and number of unused bits).
Key usage	4.2.1.3	M	C	
Digital signature				`1` (mandatory)
Non-repudiation				`0`
Key encipherment				`0`
Data encipherment				`0`
Key agreement				`0`
Key certificate signature				`0`
CRL signature				`0`
Encipher only				`0`
Decipher only				`0`
Subject alternative name	4.2.1.6	M	NC	
dNSName		M		Internet domain name of the server. Can have more than one dNSName.
Issuer alternative name	4.2.1.7	M	NC	The issuer alternative name extension shall provide contact information for the issuer of the certificate. For that purpose, the issuer alternative name shall include at least one of — `rfc822Name`, or — `uniformResourceIdentifier`. NOTE This contact information is intended to help establish trust in the certificate and the certified key by appropriate out of band mechanisms. Note that this information is only meant for contact information and does not in itself imply any level of trust in the certificate.
Extended key usage	4.2.1.12	M	C	
id-kp-serverAuth		M		TLS server authentication
id-kp-clientAuth		O		TLS client authentication. Optional, to handle particular cases where the issuing authority service may need to act also as TLS client of third-party systems.

Key
Presence:
M mandatory
O optional
C conditional
Criticality:
C critical
NC not critical

Table B.5 *(continued)*

Certificate component	Section in RFC 5280	Presence	Criticality	Description
CRLDistributionPoints	4.2.1.13	M	NC	The 'reasons' and 'cRL Issuer' fields shall not be used.
distributionPoint		M		URI for CRL distribution point
Private internet extensions				
Authority information access	4.2.2.1	C	NC	Conditional, shall be present if the IACA has an OCSP service.
Access description **OCSP**		C		Conditional, shall be present if the CA issuing this certificate has an OCSP service.
accessMethod		M		`1.3.6.1.5.5.7.48.1` (OCSP)
accessLocation		M		URI for corresponding OCSP service
Signature algorithm	4.1.1.2	M		Options: `1.2.840.10045.4.3.2` (ECDSA-with SHA256) `1.2.840.10045.4.3.3` (ECDSA-with SHA384) `1.2.840.10045.4.3.4` (ECDSA with SHA512)
Signature value	4.1.1.3	M		Value according to the signature algorithm. By creating this signature, the CA certifies the binding between the public key material and the subject of the certificate, i.e. the IACA online service.

Key
Presence:
M mandatory
O optional
C conditional
Criticality:
C critical
NC not critical

B.1.7 mdoc reader authentication

The mDL reader should use the certificate profile according to Table B.6 for mdoc reader authentication (see 9.1.4).

Table B.6 — mdoc reader authentication

Certificate component	Section in RFC 5280	Presence	Criticality	Description
Version	4.1.2.1	M		Shall be `v3`.
Serial number	4.1.2.2	M		Non-sequential positive, non-zero integer, shall contain at least 63 bits of output from a CSPRNG, should contain at least 71 bits of output from a CSPRNG, maximum 20 octets.
Signature	4.1.2.3	M		Value shall match the OID in the signature algorithm (below).
Issuer	4.1.2.4	M		The same binary value as the Subject of a CA certificate used for mdoc reader authentication. NOTE 1 This CA certificate, and the manner in which it is trusted by an mDL, is outside the scope of this document.
Validity	4.1.2.5	M		
Not before		M		Date on which the certificate validity period begins.
Not after		M		Maximum of 1 187 days after "Not before" date
Subject	4.1.2.6	M		`commonName` shall be present. Other elements may be present in the Subject field.
Subject public key info	4.1.2.7	M		

algorithm		M		If any of the curves specified below for the `parameters` field is used, the following OID must be used, as specified in RFC 5480 and RFC 5639:
				`1.2.840.10045.2.1` (id-ecPublicKey)
				For curves Ed25519 or Ed448, one of the following OIDs must be used, as specified in RFC 8410:
				`1.3.101.112(Curve Ed25519)`
				`1.3.101.113(Curve Ed448)`

Key
Presence:
M mandatory
O optional
C conditional
Criticality:
C critical
NC not critical

Table B.6 *(continued)*

Certificate component	Section in RFC 5280	Presence	Criticality	Description
parameters		C		This field must only be present when the `algorithm` field contains the OID `1.2.840.10045.2.1`. Implicitly specify curve parameters through an OID associated with one of the following curves specified in FIPS 186-4: `1.2.840.10045.3.1.7` (Curve P-256) `1.3.132.0.34` (Curve P-384) `1.3.132.0.35` (Curve P-521) Or one of the following curves specified in RFC 5639: `1.3.36.3.3.2.8.1.1.7` (brainpoolP256r1) `1.3.36.3.3.2.8.1.1.9` (brainpoolP320r1) `1.3.36.3.3.2.8.1.1.11` (brainpoolP384r1) `1.3.36.3.3.2.8.1.1.13` (brainpoolP512r1)
subjectPublicKey		M		For all curves except Ed25519 or Ed448, the public key shall be encoded in uncompressed form.
X.509v3 extensions	4.2	M		Further extensions may be present if they are marked non-critical.
Authority key identifier	4.2.1.1	M	NC	
keyIdentifier		M		Same value as the subject key identifier of the Issuer CA certificate
Subject key identifier	4.2.1.2	M	NC	SHA-1 hash of the subjectPublicKey `BIT STRING` value (excluding tag, length, and number of unused bits).
Key usage	4.2.1.3	M	C	
Digital signature				`1` (mandatory)
Non-repudiation				`0`
Key encipherment				`0`
Data encipherment				`0`
Key agreement				`0`
Key certificate signature				`0`
CRL signature				`0`
Encipher only				`0`
Decipher only				`0`

Key

Presence:

M mandatory

O optional

C conditional

Criticality:

C critical

NC not critical

Table B.6 *(continued)*

Certificate component	Section in RFC 5280	Presence	Criticality	Description
Issuer alternative name	4.2.1.7	C	NC	Conditional, this extension shall be present if the certificate is issued by an IACA. The issuer alternative name extension shall provide contact information for the issuer of the certificate. For that purpose, the issuer alternative name shall include at least one of — `rfc822Name`, or — `uniformResourceIdentifier`. NOTE 2 This contact information is intended to help establish trust in the certificate and the certified key by appropriate out of band mechanisms. Note that this information is only meant for contact information and does not in itself imply any level of trust in the certificate.
Extended key usage	4.2.1.12	M	C	
		M		`1.0.18013.5.1.6` (mdlReaderAuth)
CRLDistribution-Points	4.2.1.13	M	NC	The 'reasons' and 'cRL Issuer' fields shall not be used.
distributionPoint		M		URI for CRL distribution point
Private internet extensions				
Authority information access	4.2.2.1	C	NC	Conditional, shall be present if the CA issuing this certificate has an OCSP service or would like to indicate other Access Description elements.
Access description **OCSP**		C		Conditional, shall be present if the CA issuing this certificate has an OCSP service.
accessMethod		M		`1.3.6.1.5.5.7.48.1` (OCSP)
accessLocation		M		URI for corresponding OCSP service
Signature algorithm	4.1.1.2	M		Options: `1.2.840.10045.4.3.2` (ECDSA-with SHA256) `1.2.840.10045.4.3.3` (ECDSA-with SHA384) `1.2.840.10045.4.3.4` (ECDSA with SHA512)
Signature value	4.1.1.3	M		Value according to the signature algorithm. By creating this signature, the CA certifies the binding between the public key material and the subject of the certificate, i.e. the mDL reader.

Key
Presence:
M mandatory
O optional
C conditional
Criticality:
C critical
NC not critical

B.1.8 TLS client authentication certificate

The mdoc reader should use the certificate profile according to Table B.7 for TLS client authentication (see 9.2.1).

Table B.7 — TLS client authentication certificate

Certificate component	Section in RFC 5280	Presence	Criticality	Description
Version	4.1.2.1	M		Shall be `v3`.
Serial number	4.1.2.2	M		Non-sequential positive, non-zero integer, shall contain at least 63 bits of output from a CSPRNG, should contain at least 71 bits of output from a CSPRNG, maximum 20 octets.
Signature	4.1.2.3	M		Value shall match the OID in the signature algorithm (below).
Issuer	4.1.2.4	M		The same binary value as the Subject of a CA certificate used for TLS client authentication. NOTE 1 This CA certificate, and the manner in which it is trusted by an mDL, is outside the scope of this document.
Validity	4.1.2.5	M		
Not before		M		Date on which the certificate validity period begins.
Not after		M		Maximum of 1 187 days after "Not before" date
Subject	4.1.2.6	M		`commonName` shall be present. Other elements may be present in the Subject field.
Subject public key info	4.1.2.7	M		
algorithm		M		`1.2.840.10045.2.1` (Elliptic curve)
parameters		M		Implicitly specify curve parameters through an OID associated with one of the following curves specified in FIPS 186-4: `1.2.840.10045.3.1.7` (Curve P-256) `1.3.132.0.34` (Curve P-384) `1.3.132.0.35` (Curve P-521) Or one of the following curves specified in RFC 5639: `1.3.36.3.3.2.8.1.1.7` (brainpoolP256r1) `1.3.36.3.3.2.8.1.1.9` (brainpoolP320r1) `1.3.36.3.3.2.8.1.1.11` (brainpoolP384r1) `1.3.36.3.3.2.8.1.1.13` (brainpoolP512r1)
subjectPublicKey		M		Public key shall be encoded in uncompressed form.
X.509v3 extensions	4.2	M		Further extensions may be present if they are marked non-critical.

Key

Presence:

M mandatory

O optional

C conditional

Criticality:

C critical

NC not critical

Table B.7 *(continued)*

Certificate component	Section in RFC 5280	Presence	Criticality	Description
Authority key identifier	4.2.1.1	M	NC	
keyIdentifier		M		Same value as the subject key identifier of the Issuer CA certificate
Subject key identifier	4.2.1.2	M	NC	SHA-1 hash of the subjectPublicKey `BIT STRING` value (excluding tag, length, and number of unused bits).
Key usage	4.2.1.3	M	C	
Digital signature				`1` (mandatory)
Non-repudiation				`0`
Key encipherment				`0`
Data encipherment				`0`
Key agreement				`0`
Key certificate signature				`0`
CRL signature				`0`
Encipher only				`0`
Decipher only				`0`
Issuer alternative name	4.2.1.7	C	NC	Conditional, this extension shall be present if the certificate is issued by an IACA. The issuer alternative name extension shall provide contact information for the issuer of the certificate. For that purpose, the issuer alternative name shall include at least one of — `rfc822Name`, or — `uniformResourceIdentifier`. NOTE 2 This contact information is intended to help establish trust in the certificate and the certified key by appropriate out of band mechanisms. Note that this information is only meant for contact information and does not in itself imply any level of trust in the certificate.
Extended key usage	4.2.1.12	M	C	
		M		`1.0.18013.5.1.9` (mdlTLSClientAuth)
id-kp-clientAuth		M		Allows the usage of TLS based client authentication.
CRLDistributionPoints	4.2.1.13	M	NC	The 'reasons' and 'cRL Issuer' fields shall not be used.
distributionPoint		M		URI for CRL distribution point

Key
Presence:
M mandatory
O optional
C conditional
Criticality:
C critical
NC not critical

Table B.7 *(continued)*

Certificate component	Section in RFC 5280	Presence	Criticality	Description
Private internet extensions				
Authority information access	4.2.2.1	C	NC	Conditional, shall be present if the CA issuing this certificate has an OCSP service or would like to indicate other Access Description elements.
Access description **OCSP**		C		Conditional, shall be present if the CA issuing this certificate has an OCSP service.
accessMethod		M		`1.3.6.1.5.5.7.48.1` (OCSP)
accessLocation		M		URI for corresponding OCSP service
Signature algorithm	4.1.1.2	M		Options: `1.2.840.10045.4.3.2` (ECDSA-with SHA256) `1.2.840.10045.4.3.3` (ECDSA-with SHA384) `1.2.840.10045.4.3.4` (ECDSA with SHA512)
Signature value	4.1.1.3	M		Value according to the signature algorithm. By creating this signature, the CA certifies the binding between the public key material and the subject of the certificate, i.e. the mDL reader.
Key Presence: M mandatory O optional C conditional Criticality: C critical NC not critical				

B.1.9 OCSP signer certificate

The OCSP signer certificate is used to sign OCSP messages. See Table B.8 for details.

Table B.8 — OCSP signer certificate

Certificate component	Section in RFC 5280	Presence	Criticality	Description
Version	4.1.2.1	M		Shall be `v3`.
Serial number	4.1.2.2	M		Non-sequential positive, non-zero integer, shall contain at least 63 bits of output from a CSPRNG, should contain at least 71 bits of output from a CSPRNG, maximum 20 octets.
Signature	4.1.2.3	M		Value shall match the OID in the signature algorithm (below).
Issuer	4.1.2.4	M		Same exact binary value as the subject of IACA certificate
Validity	4.1.2.5	M		
Not before		M		Date on which the certificate validity period begins.
Not after		M		If the OCSP signer certificate supports the CRLDistribution-Points extension: Maximum of 457 days after "Not before" date. If the OCSP signer certificate supports the Revocation Checking of an Authorized Responder extension: Maximum of 90 days after "Not before" date.
Subject	4.1.2.6	M		`countryName` is mandatory. The value shall be in upper case and contain the ISO 3166-1 alpha-2 code of the issuing country, exactly the same value as in the issuing country data element. The `countryName` shall be `PrintableString`. `stateOrProvinceName` is optional. If this element is present in the IACA root certificate, this element shall be present and hold the same value. The value shall exactly match the value of the data element "issuing_jurisdiction", if that element is present on the mDL. `organizationName` is optional. Its value is at the discretion of the IACA. `commonName` shall be present. Its value is at the discretion of the IACA. `localityName` is optional. Its value is at the discretion of the IACA. `serialNumber` is optional. If present, it shall be a `PrintableString`. Attributes that have a `DirectoryString` and for which the encoding is not listed above syntax shall be either `PrintableString` or `UTF8String`.
Subject public key info	4.1.2.7	M		
algorithm		M		`1.2.840.10045.2.1` (Elliptic curve)

Key

Presence:

M mandatory

O optional

C conditional

Criticality:

C critical

NC not critical