Sectigo S/MIME Certificate Profiles

Sectigo Limited
Version: 1.0.6
Effective: May 13, 2024
3rd Floor, Building 26 Exchange Quay, Trafford Road,
Salford, Greater Manchest, M5 3EQ, United Kingdom
Tel: +44 (0) 161 874 7070
www.sectigo.com
Sectigo Limited

Latest Revision: May 13, 2024

Table of Contents

INTRODUCTION

Sectigo only issues S/MIME certificates according to this document and the profiles defined. All S/MIME certificate profiles are detailed below.

Additionally, specific certificate policies and Sectigo liability arrangements that are not described in the S/MIME CP/CPS may be drawn up under contract for individual subscribers.

Different certificate profiles may be issued with different key usages.

MAILBOX Validated (MV)

The Mailbox validated S/MIME certificates refer to a certificate subject that is limited to (optionally) the email address or the serial number attributes of the subject. This means that Sectigo confirms that the mailbox holder has control over the requested mailbox address. At Sectigo we include only the email address as an optional field.

Multipurpose

OID: 1.3.6.1.4.1.6449.1.2.1.10.1 S/MIME Mailbox Validation Multipurpose

MVM

Field/Extension	Attribute	Content	Optional/Critical
Version		3 (0x2)	
Serial Number	containing at least 64 bits of output from a CSPRNG	XXX	
Signature Algorithm		Sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer	commonName	XXX	
	organizationName	XXX	
	countryName	XX	
Validity		1 or 2 years	
Subject	emailAddress (E)	MUST be identical to one of the SAN:rfc822Name values	Optional
Subject Public Key Info	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	RSA 2048 bits or P-256 minimum	
Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate		
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)		
Key Usage		See Key Usage table	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Client Authentication, email protection	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.10.1	
	cpsURI	https://sectigo.com/SMIMECPS	
	policyIdentifier	2.23.140.1.5.1.2	
CRL Distribution Points		XXXX	
Authority Information Access	CA Issuers	XXXX	
	OCSP	http://ocsp.sectigo.com	
Subject Alternative Name	Rfc822Name	Subscriber email	

Strict

OID: 1.3.6.1.4.1.6449.1.2.1.10.2 S/MIME Mailbox Validation Strict

MVS

Field/Extension	Attribute	Content	Optional/Critical
Version		3 (0x2)	
Serial Number	containing at least 64 bits of output from a CSPRNG	XXX	
Signature Algorithm		Sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer	commonName	XXX	
	organizationName	XXX	
	countryName	XX	
Validity		1 or 2 years	
Subject	emailAddress (E)	MUST be identical to one of the SAN:rfc822Name values	Optional
Subject Public Key Info	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	RSA 2048 bits or P-256 minimum	
Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate		
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)		
Key Usage		See Key Usage table	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		email protection	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.10.2	
	cpsURI	https://sectigo.com/SMIMECPS	
	policyIdentifier	2.23.140.1.5.1.3	
CRL Distribution Points		XXXX	
Authority Information Access	CA Issuers	XXXX	
	OCSP	http://ocsp.sectigo.com	
Subject Alternative Name	Rfc822Name	Subscriber email	

Legacy

OID: 1.3.6.1.4.1.6449.1.2.1.10.7 S/MIME Mailbox Validation Legacy

MVL

Field/Extension		Content	Optional/Critical
Version		3 (0x2)	
Serial Number	containing at least 64 bits of output from a CSPRNG	XXX	
Signature Algorithm		Sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer	commonName	XXX	
	organizationName	XXX	
	countryName	XX	
Validity		1, 2 or 3 years	
Subject	emailAddress (E)	MUST be identical to one of the SAN:rfc822Name values	Optional
Subject Public Key Info	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	RSA 2048 bits or P-256 minimum	
Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate		
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)		
Key Usage		See Key Usage table	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		email protection, client authentication	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.10.7	
	cpsURI	https://sectigo.com/SMIMECPS	
	policyIdentifier	2.23.140.1.5.1.1	
CRL Distribution Points		XXXX	
Authority Information Access	CA Issuers	XXXX	
	OCSP	http://ocsp.sectigo.com	
Subject Alternative Name	Rfc822Name	Subscriber email	

ORGANIZATION Validated (OV)

The Organization validated S/MIME certificates refer to a certificate subject that includes only attributes of the legal entity (organization) with no information regarding any natural person or individual. Sectigo only includes the organization name and its identifier.

Multipurpose

OID: 1.3.6.1.4.1.6449.1.2.1.10.3 S/MIME Organization Validation Multipurpose

OVM

Field/Extension		Content	Optional/Critical
Version		3 (0x2)	
Serial Number	containing at least 64 bits of output from a CSPRNG	XXX	
Signature Algorithm		Sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer	commonName	XXX	
	organizationName	XXX	
	countryName	XX	
Validity		1 or 2 years	
Subject	commonName (CN)	XXXX (organizationName)	Optional
	organizationIdentifier	3 characters+Country ID+ -IdentifierExample: VATUK-04058690 or VATES-A29394909 as per ETSI EN 319 412-1.	
	Email (E)	xxx@xxx	Optional
	OrganizationName (O)	XXXX	
	Locality	XXXX	Optional
	StateorProvince	XXXX	Optional
	countryName (C)	XXXX	
Subject Public Key Info	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	RSA 2048 bits or P-256 minimum	
Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate		
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)		
Key Usage		See Key Usage table	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Client Authentication, emailProtection	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.10.3	
	cpsURI	https://sectigo.com/SMIMECPS	

Field/Extension		Content	Optional/Critical
	policyIdentifier	2.23.140.1.5.2.2	
CRL Distribution Points		XXXX	
Authority Information Access	CA Issuers	XXXX	
	OCSP	http://ocsp.sectigo.com	
Subject Alternative Name	Rfc822Name	Subscriber email	

SPONSORED Validated (SV)

The Sponsor validated S/MIME certificates refer to a certificate subject that combines natural person (individual) attributes with legal person (organization) attributes. At Sectigo we include the organization name, and its identifier, and the individual name while others are optional fields.

Multipurpose

OID: 1.3.6.1.4.1.6449.1.2.1.10.4 S/MIME Sponsored Validation Multipurpose

SVM

Field/Extension		Content	Optional/Critical
Version		3 (0x2)	
Serial Number	containing at least 64 bits of output from a CSPRNG	XXX	
Signature Algorithm		Sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer	commonName	XXX	
	organizationName	XXX	
	countryName	XX	
Validity		1 or 2 years	
Subject	commonName (CN)	(personal name)	Optional
	Title	XXXX	Optional
	Name (G)	XXXX	
	Surname (SN)	XXXX	
	organizationIdentifier	3 characters+Country ID+ -IdentifierExample: VATUK-04058690 or VATES-A29394909 as per ETSI EN 319 412-1.	
	Email (E)	xxx@xxx	Optional
	OrganizationName (O)	XXXX	
	Locality	XXXX	Optional
	StateorProvince	XXXX	Optional
	countryName (C)	XXXX	
Subject Public Key Info	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	RSA 2048 bits or P-256 minimum	
Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate		
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)		
Key Usage		See Key Usage table	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Email protection, Client Authentication	

Field/Extension		Content	Optional/Critical
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.10.4	
	cpsURI	https://sectigo.com/SMIMECPS	
	policyIdentifier	2.23.140.1.5.3.2	
CRL Distribution Points		XXXX	
Authority Information Access	CA Issuers	XXXX	
	OCSP	http://ocsp.sectigo.com	
Subject Alternative Name	Rfc822Name	Subscriber email	

INDIVIDUAL Validated (IV)

The Individual validated S/MIME certificates refer to a certificate subject that includes only attributes of the natural person (individual) with no information regarding any legal person. Sectigo only includes the name and surname of the individual.

Multipurpose

OID: 1.3.6.1.4.1.6449.1.2.1.10.5 S/MIME Individual Validation Multipurpose

IVM

Field/Extension		Content	Optional/Critical
Version		3 (0x2)	
Serial Number	containing at least 64 bits of output from a CSPRNG	XXX	
Signature Algorithm		Sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer	commonName	XXX	
	organizationName	XXX	
	countryName	XX	
Validity		1 or 2 years	
Subject	commonName (CN)	XXXX (Personal name)	Optional
	Title	XXXX	Optional
	Name (G)	XXXX	
	Surname (SN)	XXXX	
	Email (E)	xxx@xxx	Optional
	Locality	XXXX	Optional
	StateorProvince	XXXX	Optional
	countryName (C)	XXXX	
Subject Public Key Info	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	RSA 2048 bits or P-256 minimum	
Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate		
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)		
Key Usage		See Key Usage table	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Client Authentication, email protection	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.10.5	
	cpsURI	https://sectigo.com/SMIMECPS	
	policyIdentifier	2.23.140.1.5.4.2	
CRL Distribution Points		XXXX	

Field/Extension		Content	Optional/Critical
Authority Information Access	CA Issuers	XXXX	
	OCSP	http://ocsp.sectigo.com	
Subject Alternative Name	Rfc822Name	Subscriber email	

Strict

OID: 1.3.6.1.4.1.6449.1.2.1.10.6 S/MIME Individual Validation Strict

IVS

Field/Extension		Content	Optional/Critical
Version		3 (0x2)	
Serial Number	containing at least 64 bits of output from a CSPRNG	XXX	
Signature Algorithm		Sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer	commonName	XXX	
	organizationName	XXX	
	countryName	XX	
Validity		1 or 2 years	
Subject	commonName (CN)	XXXX (personal name)	Optional
	Title	XXXX	Optional
	Name (G)	XXXX	
	Surname (SN)	XXXX	
	Email (E)	xxx@xxx	Optional
	Locality	XXXX	Optional
	StateorProvince	XXXX	Optional
	countryName (C)	XXXX	
Subject Public Key Info	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	RSA 2048 bits or P-256 minimum	
Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate		
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)		
Key Usage		See Key Usage table	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		email protection	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.10.6	
	cpsURI	https://sectigo.com/SMIMECPS	

Field/Extension		Content	Optional/Critical
	policyIdentifier	2.23.140.1.5.4.3	
CRL Distribution Points		XXXX	
Authority Information Access	CA Issuers	XXXX	
	OCSP	http://ocsp.sectigo.com	
Subject Alternative Name	Rfc822Name	Subscriber email	

Notes

- Enterprise customers: All profiles but mainly SV
- Retail customers: All profiles except SV. KU Options for “Signing + Encryption” and “Signing Only”.
- Rest of customers: All profiles except SV

Key Usage table

Below: Key Usage table. This table specifies the allowed combinations depending on intended usage and key type.

Purpose	Key Type	Key Usage
Signing + Encryption	RSA	digitalSignature, keyEncipherment
Signing + Encryption	ECC	digitalSignature, keyAgreement
Signing Only	RSA	digitalSignature
Signing Only	ECC	digitalSignature
Encryption Only	RSA	keyEncipherment
Encryption Only	ECC	keyAgreement

Additionally: When an RSA key type is used on a Legacy or Multipurpose profile and keyEncipherment is set, the dataEncipherment KU may also be set but is not required. It may not be used on Strict profiles, or if keyEncipherment is absent.

Subject fields

- Locality (L) and StateorProvince (ST) are both optional but both can´t go in the profile, only one must go in the profile, so one or the other. stateOrProvince is preferred.

Sectigo OIDs

- 1.3.6.1.4.1.6449.1.2.1.10.1 S/MIME MVM
- 1.3.6.1.4.1.6449.1.2.1.10.2 S/MIME MVS
- 1.3.6.1.4.1.6449.1.2.1.10.3 S/MIME OVM
- 1.3.6.1.4.1.6449.1.2.1.10.4 S/MIME SVM
- 1.3.6.1.4.1.6449.1.2.1.10.5 S/MIME IVM
- 1.3.6.1.4.1.6449.1.2.1.10.6 S/MIME IVS
- 1.3.6.1.4.1.6449.1.2.1.10.7 S/MIME MVL

Additional Extensions

Sectigo S/MIME certificates MAY include one or more of the following extensions.

Extension Name	Extension OID	Definition
szOID_CERTIFICATE_TEMPLATE	1.3.6.1.4.1.311.21.7	Microsoft Open Specifications

Changelog

Version	Change Description
1.0	New doc
1.0.1	New MVL profile
1.0.2	Changes in the Common Name
1.0.3	Add Key Usage table
1.0.4	minor changes reflecting updates from the CABF SMIME BRs
1.0.5	Update of the CPS URI
1.0.6	Allow Extension for Certificate Template (1.3.6.1.4.1.311.21.7) (szOID_CERTIFICATE_TEMPLATE)