Sectigo
Document Signing
Certificate profiles

Sectigo Limited
Version 2.0
Effective: February 7, 2024
Unit 7, Campus Road, Listerhills Science
Park, Bradford, BD7 1HR, United Kingdom
Tel: +44 (0) 161 874 7070
www.sectigo.com

Copyright Notice

Sectigo Limited
Attention: Legal Practices
Unit 7, Campus Road, Listerhills Science Park, Bradford, BD7 1HR, United Kingdom

Contents

INTRODUCTION

Sectigo only issues Document Signing certificates according to this document and the profiles defined. All Document Signing certificate profiles are detailed below.

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

Different certificate profiles may be issued with different key usages.

Note: eIDAS policies and profiles documents for (qualified) electronic signatures and seals are also applicable for Document Signing

Root CAs

Sectigo has generated and used some root CA certificates for the issuance of these certificate types. While one is a generic and old one, the new ones are specific for this type of certificates. Also, the Ensured root CA is included in this list.

USERTrust RSA CA

crt.sh | 1199354

Field/Extension		Content	Optional/Critical
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	01fd6d30fca3ca51a81bbc640e35032d	
Signature Algorithm		sha384WithRSAEncryption	
Issuer	commonName	USERTrust RSA Certification Authority	
	organizationName	The USERTRUST Network	
	locality	Jersey City	
	stateOrProvince	New Jersey	
	countryName	US	
Validity	Not before	Feb 1 00:00:00 2010 GMT	
	Not after	Jan 18 23:59:59 2038 GMT	
Subject	commonName	USERTrust RSA Certification Authority	
	organizationName	The USERTRUST Network	
	locality	Jersey City	
	stateOrProvince	New Jersey	
	countryName	US	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	rsaEncryption and 4096 bits	
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)		
Key Usage		Certificate Sign, CRL Sign	Critical
Basic Constraints		CA:TRUE	Critical

Sectigo Public Document Signing Root R46

crt.sh | 4292601243

Field/Extension		Content	Optional/Critical
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	fa7cbeea8b97a208d02ba6944904589f	
Signature Algorithm		sha384WithRSAEncryption	
Issuer	commonName	Sectigo Public Document Signing Root R46	
	organizationName	Sectigo Limited	
	countryName	GB	
Validity	Not before	Mar 22 00:00:00 2021 GMT	
	Not after	Mar 21 23:59:59 2046 GMT	

Subject	commonName (CN)	Sectigo Public Document Signing Root R46	
	organizationName	Sectigo Limited	
	countryName	GB	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	rsaEncryption and 4096 bits	
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)	b13879bab462914e8bc44b151fc5cfefc3a0a7f7	
Key Usage		Digital Signature, Certificate Sign, CRL Sign	Critical
Basic Constraints		CA:TRUE	Critical

Sectigo Public Document Signing Root E46

crt.sh | 4292602906

Field/Extension		**Content**	**Optional/Critical**
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	614a49e9aa87f4d59a3ee22eb2ad5b37	
Signature Algorithm		ecdsa-with-SHA384	
Issuer	commonName	Sectigo Public Document Signing Root E46	
	organizationName	Sectigo Limited	
	countryName	GB	
Validity	Not before	Mar 22 00:00:00 2021 GMT	
	Not after	Mar 21 23:59:59 2046 GMT	
Subject	commonName (CN)	Sectigo Public Document Signing Root E46	
	organizationName	Sectigo Limited	
	countryName	GB	
Subject Public Key Info	Public Key Algorithm and Public-Key	id-ecPublicKey and 384 bits	
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)	88d32391d4c932fb682cddfeaf87639e3f314768	
Key Usage		Digital Signature, Certificate Sign, CRL Sign	Critical
Basic Constraints		CA:TRUE	Critical

SECTIGO

Ensured Root CA

crt.sh | 56152602

Field/Extension		Content	Optional/Critical
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	4d610debb88300b06913a755a41b4b44	
Signature Algorithm		sha384WithRSAEncryption	
Issuer	commonName	Ensured Root CA	
	organizationName	Ensured B.V.	
	localityName	Heerhugowaard	
	stateOrProvince	Noord-Holland	
	countryName	NL	
Validity	Not before	Jul 23 00:00:00 2015 GMT	
	Not after	Jul 18 23:59:59 2038 GMT	
Subject	commonName	Ensured Root CA	
	organizationName	Ensured B.V.	
	localityName	Heerhugowaard	
	stateOrProvince	Noord-Holland	
	countryName	NL	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	rsaEncryption and 4096 bits	
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)	88d498eafa6650f89385df604b97fe2fa930dd50	
Key Usage		Digital Signature, Certificate Sign, CRL Sign	Critical
Basic Constraints		CA:TRUE	Critical

Issuing CAs

These issuing CAs are of specific purpose for this type of certificates. One is just under the generic root and the others are of the specific ones. This is similar to the Ensured issuing CA.

Sectigo RSA Document Signing CA

crt.sh | 1415494347

Field/Extension		Content	Optional/Critical
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	5afd7bdc000670c6e00e318ff5514482	
Signature Algorithm		sha384WithRSAEncryption	
Issuer	commonName	USERTrust RSA Certification Authority	
	organizationName	The USERTRUST Network	
	locality	Jersey City	
	stateOrProvince	New Jersey	
	countryName	US	
Validity	Not before	Apr 24 00:00:00 2019 GMT	
	Not after	Dec 31 23:59:59 2030 GMT	
Subject	commonName	Sectigo RSA Document Signing CA	
	organizationName	Sectigo Limited	
	locality	Salford	
	stateOrProvince	Greater Manchester	
	countryName	GB	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	rsaEncryption and 2048 bits	
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)	cc6bcf26bdfa4c2d4feb0c5f28eee3d98703ee0a	
Key Usage		Digital Signature, Certificate Sign, CRL Sign	Critical
Basic Constraints		CA:TRUE	Critical
Extended Key Usage		TLS Web Client Authentication, Code signing, e-mail protection, timestamping, document signing, adobe authentic document trust	
Certificate Policies	policyIdentifier	X509v3 Any Policy	
CRL Distribution Points		http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl	
Authority Information Access	CA Issuers	http://crt.usertrust.com/USERTrustRSAAddTrustCA.crt	
	OCSP	http://ocsp.usertrust.com	

Sectigo Public Document Signing CA R36

crt.sh | 4292606070

Field/Extension		Content	Optional/Critical
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	32ba1453956485ed2e7a6b46224537e1	
Signature Algorithm		sha384WithRSAEncryption	
Issuer	commonName	Sectigo Public Document Signing Root R46	
	organizationName	Sectigo Limited	
	countryName	GB	
Validity	Not before	Mar 22 00:00:00 2021 GMT	
	Not after	Mar 21 23:59:59 2036 GMT	
Subject	commonName (CN)	Sectigo Public Document Signing CA R36	
	OrganizationName (O)	Sectigo Limited	
	countryName (C)	GB	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	rsaEncryption and 3072 bits	
Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate	b13879bab462914e8bc44b151fc5Cfefc3a0a7f7	
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)	9480c4e1627fdab5d1961a4aed18d230d0f5564d	
Key Usage		Digital Signature, Certificate Sign, CRL Sign	Critical
Basic Constraints		CA:TRUE	Critical
Extended Key Usage		document signing, adobe authentic document trust	
Certificate Policies	policyIdentifier	X509v3 Any Policy	
CRL Distribution Points		http://crl.sectigo.com/SectigoPublicDocumentSigningRootR46.crl	
Authority Information Access	CA Issuers	http://crt.sectigo.com/SectigoPublicDocumentSigningRootR46.p7c	
	OCSP	http://ocsp.sectigo.com	

Sectigo Public Document Signing CA R36

crt.sh | 4292606071

Field/Extension		Content	Optional/Critical
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	639a960df757c07533727d64598e269f	

Signature Algorithm		ecdsa-with-SHA384	
Issuer	commonName	Sectigo Public Document Signing Root E46	
	organizationName	Sectigo Limited	
	countryName	GB	
Validity	Not before	Mar 22 00:00:00 2021 GMT	
	Not after	Mar 21 23:59:59 2036 GMT	
Subject	commonName (CN)	Sectigo Public Document Signing CA E36	
	OrganizationName (O)	Sectigo Limited	
	countryName (C)	GB	
Subject Public Key Info	Public Key Algorithm and EcpkParameters	id-ecPublicKey and 256 bits	
Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate	88d32391d4c932fb682cddfeaf87639e3f314768	
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)	d18110972ba04870135e81e87bfc366af68a37c3	
Key Usage		Digital Signature, Certificate Sign, CRL Sign	Critical
Basic Constraints		CA:TRUE	Critical
Extended Key Usage		document signing, adobe authentic document trust	
Certificate Policies	policyIdentifier	X509v3 Any Policy	
CRL Distribution Points		http://crl.sectigo.com/SectigoPublicDocumentSigningRootE46.crl	
Authority Information Access	CA Issuers	http://crt.sectigo.com/SectigoPublicDocumentSigningRootE46.p7c	
	OCSP	http://ocsp.sectigo.com	

Ensured Document Signing CA

crt.sh | 4292606071

Field/Extension		**Content**	**Optional/Critical**
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	7dc4ca1eefccd9e5cefa552ba897887b	
Signature Algorithm		sha384WithRSAEncryption	
Issuer	commonName	Ensured Root CA	
	organizationName	Ensured B.V.	
	localityName	Heerhugowaard	
	stateOrProvince	Noord-Holland	
	countryName	NL	
Validity	Not before	Oct 25 00:00:00 2016 GMT	
	Not after	Oct 24 23:59:59 2031 GMT	

Subject	commonName (CN)	Ensured Document Signing CA	
	organizationName (O)	Ensured B.V.	
	localityName	Heerhugowaard	
	stateOrProvince	Noord-Holland	
	countryName (C)	NL	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	rsaEncryption and 4096 bits	
Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate	88d498eafa6650f89385df604b97fe2fa930dd50	
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)	ca091cc32a85258d5abf2e0f96807d4cfdcc1f52	
Key Usage		Digital Signature, Certificate Sign, CRL Sign	Critical
Basic Constraints		CA:TRUE	Critical
Extended Key Usage		document signing, adobe authentic document trust	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.44710.2.1	
CRL Distribution Points		http://crl.ensuredca.com/EnsuredRootCA_2.crl	
Authority Information Access	CA Issuers	http://crt.ensuredca.com/EnsuredRootCA_3.crt	
	OCSP	http://ocsp.ensuredca.com	

End entity

Sectigo and Ensured offer the same document signing certificates features but differ in the device used for the issuance. Basically there 3 options:

- Local device: issued in USB tokens
- Remote: issued in remote HSMs
- External trusted: issued in a remote third party HSM linked to a signing solution

Document Signing (local)

Field/Extension		**Content**	**Optional/Critical**
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG		
Signature Algorithm		Sha256WithRSAEncryption	
Issuer	commonName	Sectigo RSA Document Signing CA	
	organizationName	Sectigo Limited	
	locality	Salford	
	stateOrProvince	Greater Manchester	
	countryName	GB	
Validity	1, 2 or 3 years		
Subject	commonName		
	emailAddress		
	organizationName		
	street		optional
	locality		optional
	stateOrProvince		
	postalCode		optional
	countryName		
Subject Public Key Info	rsaEncryption and RSAPublicKey		
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		Digital Signature, Key Encipherment	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Document Signing, Client Authentication, Adobe Authentic Documents Trust	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.6.6	
	CPS URI	https://sectigo.com/dsCPS	
CRL Distribution Points		http://crl.sectigo.com/SectigoRSADocumentSigningCA.crl	

Authority Information Access	CA Issuers	http://crt.sectigo.com/SectigoRSADocumentSigningCA.crt	
	OCSP	http://ocsp.sectigo.com	
Subject Alternative Name	Rfc822Name	email: user@example.com	

Document Signing (remote)

Field/Extension		**Content**	**Optional/Critical**
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG		
Signature Algorithm		Sha256WithRSAEncryption	
Issuer	commonName	Sectigo RSA Document Signing CA	
	organizationName	Sectigo Limited	
	locality	Salford	
	stateOrProvince	Greater Manchester	
	countryName	GB	
Validity	1,2 or 3 years		
Subject	commonName		
	emailAddress		
	organizationName		
	street		optional
	locality		optional
	stateOrProvince		
	postalCode		optional
	countryName		
Subject Public Key Info	rsaEncryption and RSAPublicKey		
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		Digital Signature, Key Encipherment	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Document Signing, Client Authentication, Adobe Authentic Documents Trust	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.6.7	
	CPS URI	https://sectigo.com/dsCPS	
CRL Distribution Points		http://crl.sectigo.com/SectigoRSADocumentSigningCA.crl	

Authority Information Access	CA Issuers	http://crt.sectigo.com/SectigoRSADocumentSigningCA.crt	
	OCSP	http://ocsp.sectigo.com	
Subject Alternative Name	Rfc822Name	email: user@example.com	

Document Signing (external trusted partner)

Field/Extension		**Content**	**Optional/Critical**
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG		
Signature Algorithm		Sha256WithRSAEncryption	
Issuer	commonName	Sectigo RSA Document Signing CA	
	organizationName	Sectigo Limited	
	locality	Salford	
	stateOrProvince	Greater Manchester	
	countryName	GB	
Validity	1,2 or 3 years		
Subject	commonName		
	emailAddress		
	organizationName		
	street		Optional
	locality		Optional
	stateOrProvince		
	postalCode		optional
	countryName		
Subject Public Key Info	rsaEncryption and RSAPublicKey		
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		Digital Signature, Key Encipherment	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Document Signing, Client Authentication, Adobe Authentic Documents Trust	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.6.8	
	CPS URI	https://sectigo.com/dsCPS	
CRL Distribution Points		http://crl.sectigo.com/SectigoRSADocumentSigningCA.crl	

Authority Information Access	CA Issuers	http://crt.sectigo.com/SectigoRSADocumentSigningCA.crt	
	OCSP	http://ocsp.sectigo.com	
Subject Alternative Name	Rfc822Name	email: user@example.com	

Document Signing (Ensured)

Field/Extension		**Content**	**Optional/Critical**
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG		
Signature Algorithm		Sha256WithRSAEncryption	
Issuer	commonName	Ensured Document Signing CA	
	organizationName	Ensured B.V.	
	locality	Heerhugowaard	
	stateOrProvince	Noord-Holland	
	countryName		
Validity	1, 2 or 3 years		
Subject	commonName		
	emailAddress		
	organizationName		
	stateOrProvince		
	countryName		
Subject Public Key Info	rsaEncryption and RSAPublicKey		
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		Digital Signature, Non-Repudiation	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Document Signing, Adobe Authentic Documents Trust	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.44710.2.1	
	CPS URI	https://www.ensured.com/repository	
CRL Distribution Points		http://crl.ensuredca.com/EnsuredDocumentSigningCA_2.crl	

Authority Information Access	CA Issuers	http://crt.ensuredca.com/EnsuredDocumentSigningCA_2.crt	
	OCSP	http://ocsp.ensuredca.com	
Subject Alternative Name	Rfc822Name	email: user@example.com	

Sectigo OIDs

1.3.6.1.4.1.6449.1.2.1.6.6	Sectigo Document Signing (local)
1.3.6.1.4.1.6449.1.2.1.6.7	Sectigo Document Signing (remote)
1.3.6.1.4.1.6449.1.2.1.6.8	Sectigo Document Signing (trusted partner)
1.3.6.1.4.1.44710.2.1	Ensured Document Signing (local)

EKU OIDs

1.3.6.1.4.1.311.10.3.12	Microsoft Document Signing
1.2.840.113583.1.1.5	Adobe Authentic Document Trust
1.3.6.1.5.5.7.3.36	RFC 9336

Annex A: Changelog

Version	Change description	Date
1.0	First version	4/10/22
2.0	Added RFC 9336 EKU OID for the document signing. Modify the cpsURI to point to a new one specific, dsCPS.	7/2/24