DIGITALSIGN – CERTIFICADORA DIGITAL, SA.

CERTIFICATION PROFILE LIST

VERSION 1.7 – 30/10/2023
[LANGUAGE: ENGLISH]

VERSION HISTORY

Date	Edition nr	Content
18/01/2021	0.0	Initial draft
27/01/2021	1.0	Review and publication subsequent to the creation of the CAs
24/02/2021	1.1	Revision
08/04/2021	1.2	Revision
29/04/2021	1.3	Revision
15/09/2021	1.4	Revision
18/05/2022	1.5	Revision
20/09/2022	1.6	Revision
30/10/2023	1.7	Revision

RELATED DOCUMENTS

Document Details	Author(s)
Certification Practice Statement	DigitalSign

AUTHORIZATIONS

Created by	Approved by
Digitally Signed By: ÁLVARO OLIVEIRA DE MATOS Signing Time: 2023/10/30 10:29:24 WET +0000 Organization: DIGITALSIGN - CERTIFICADORA DIGITAL, SA Certificate Profile - Qualified Certificate - Member Entitlement - DIRETOR GERAL / GENERAL MANAGER Digital Qualified Certificate Electronically Signed Document. This electronic signature replaces the autograph signature in the EU.	Digitally Signed By: FERNANDO AVELINO LEITE DOS SANTOS MOREIRA Signing Time: 2023/10/30 14:41:45 WET +0000 Organization: DIGITALSIGN - CERTIFICADORA DIGITAL S.A. Certificate Profile - Qualified Certificate - Representative Entitlement - ASSINAR DOCUMENTOS E CONTRATOS Certificado Digital Qualificado Documento assinado eletronicamente. Esta assinatura eletrónica substitui a assinatura autógrafa na UE.

LEGAL NOTICE

Copyright © DigitalSign – Certificadora Digital, SA. All rights reserved.
DigitalSign is a registered trademark of DigitalSign - Certificadora Digital, SA. All other brands, trademarks and service marks are the property of their respective owners.

Any question or request for information regarding the content of this document should be directed to suporte@digitalsign.pt.

CONTENT

1. RSA Hierarchy 5
1.1. DIGITALSIGN QUALIFIED CA G1 5
1.1.1. OCSP [OID: 1.3.6.1.4.1.25596.4.2.1.1.1.1] 5
1.1.2. Individual [OID: 1.3.6.1.4.1.25596.4.2.1.1.1.2] 6
1.1.3. Professional [OID: 1.3.6.1.4.1.25596.4.2.1.1.1.3] 8
1.1.4. Member [OID: 1.3.6.1.4.1.25596.4.2.1.1.1.4] 10
1.1.5. Representative [OID: 1.3.6.1.4.1.25596.4.2.1.1.1.5] 12
1.1.6. Organization (eSeal) [OID: 1.3.6.1.4.1.25596.4.2.1.1.1.6] 14
1.2. DIGITALSIGN QUALIFIED TSA CA G1 16
1.2.1. OCSP [OID: 1.3.6.1.4.1.25596.4.2.1.2.1.1] 16
1.2.2. TimeStamp [OID: 1.3.6.1.4.1.25596.4.2.1.2.1.2] 17
1.3. DIGITALSIGN CA G1 18
1.3.1. OCSP [OID: 1.3.6.1.4.1.25596.4.2.1.3.1.1] 18
1.3.2. Basic [OID: 1.3.6.1.4.1.25596.4.2.1.3.1.2] 19
1.3.3. Individual [OID: 1.3.6.1.4.1.25596.4.2.1.3.1.3] 20
1.3.4. Member [OID: 1.3.6.1.4.1.25596.4.2.1.3.1.4] 22
1.3.5. Organization (eSeal) [OID: 1.3.6.1.4.1.25596.4.2.1.3.1.5] 24
1.4. DIGITALSIGN TSA CA G1 26
1.4.1. OCSP [OID: 1.3.6.1.4.1.25596.4.2.1.4.1.1] 26
1.4.2. TimeStamp [OID: 1.3.6.1.4.1.25596.4.2.1.4.1.2] 27
2. ECDSA Hierarchy 28
2.1. DIGITALSIGN QUALIFIED CA V1 28
2.1.1. OCSP [OID: 1.3.6.1.4.1.25596.4.2.2.1.1.1] 28
2.1.2. Individual [OID: 1.3.6.1.4.1.25596.4.2.2.1.1.2] 29
2.1.3. Professional [OID: 1.3.6.1.4.1.25596.4.2.2.1.1.3] 31
2.1.4. Member [OID: 1.3.6.1.4.1.25596.4.2.2.1.1.4] 33
2.1.5. Representative [OID: 1.3.6.1.4.1.25596.4.2.2.1.1.5] 35
2.1.6. Organization (eSeal) [OID: 1.3.6.1.4.1.25596.4.2.2.1.1.6] 37
2.2. DIGITALSIGN QUALIFIED TSA V1 39
2.2.1. OCSP [OID: 1.3.6.1.4.1.25596.4.2.2.2.1.1] 39
2.2.2. TimeStamp [OID: 1.3.6.1.4.1.25596.4.2.2.2.1.2] 40
2.3. DIGITALSIGN CA V1 41
2.3.1. OCSP [OID: 1.3.6.1.4.1.25596.4.2.2.3.1.1] 41
2.3.2. Basic [OID: 1.3.6.1.4.1.25596.4.2.2.3.1.2] 42
2.3.3. Individual [OID: 1.3.6.1.4.1.25596.4.2.2.3.1.3] 44
2.3.4. Member [OID: 1.3.6.1.4.1.25596.4.2.2.3.1.4] 46

2.3.5. Organization (eSeal) [OID: 1.3.6.1.4.1.25596.4.2.2.3.1.5] 48
2.4. DIGITALSIGN TSA CA V1 50
2.4.1. OCSP [OID: 1.3.6.1.4.1.25596.4.2.2.4.1.1] 50
2.4.2. TimeStamp [OID: 1.3.6.1.4.1.25596.4.2.2.4.1.2] 51

1. RSA HIERARCHY

1.1. DIGITALSIGN QUALIFIED CA G1

1.1.1. OCSP [OID: 1.3.6.1.4.1.25596.4.2.1.1.1.1]

Certificate used by OCSP Responder to sign and verify the OCSP service's responses regarding the status of the certificates issued by the CA.

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		1.2.840.113549.1.1.13 - sha512WithRSAEncryption	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<OCSP Application Name>	Required
	O	DigitalSign Certificadora Digital	Required
	OU (0 or more)	<Additional CA/RA information>	Optional
	C	PT	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Digital Signature	Required, Critical
Extended Key Usage		id-kp-OCSP (1.3.6.1.5.5.7.3.9)	Required
Subject Public Key Info		RSA (2048 bits or more)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required
Certificate Policies		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
		Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional
		Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.1.1.1.1	Required
		<Other Certificate Policies>	Optional
No check extension		1.3.6.1.5.5.7.48.1.5 (05 00)	Required
Authority Information Access		AIA: https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b	Optional

1.1.2. INDIVIDUAL [OID: 1.3.6.1.4.1.25596.4.2.1.1.1.2]

Certificate used for eIDAS compliant qualified signature by natural persons.

This certificate profile aims to identify a natural person (individual).

0.4.0.194112.1.2 [ETSI EN 319411-2 - QCP-n-qscd].

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		Allowed signature algorithm: - 1.2.840.113549.1.1.11 - sha256WithRSAEncryption - 1.2.840.113549.1.1.13 - sha512WithRSAEncryption	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<Name of the subscriber > Can include pseudonyms, nicknames, names with spelling other than defined by the registered name, and/or additional identification attributes Ex: CN = John Doe, G = John, SN = Doe CN = *Star* John, G = John, SN = Doe CN = John *Star* Doe / num: 123456, G = John, SN = Doe	Required
	OU	RemoteQSCDManagement	Rquired (ONLY in case of remote HSM certificate)
	G	<Given Name>	Required
	SN	<Surname>	Required
	SERIALNUMBER	<Subscriber ID (NIF / CC / PASS / other), according to ETSI EN 319 412-1>	Optional
	E	<Email address>	Required
	T	<Academic degree or another that the holder can use>	Optional
	OU	Limitation1 - <Any limitations for signature use (line 1)>	Optional
	OU	Limitation2 - <Any limitations for signature use (line 2)>	Optional
	OU	Limitation3 - <Any limitations for signature use (line 3)>	Optional
	OU	Obs1 - <Any additional information/comments (line 1)>	Optional
	OU	Obs2 - <Any additional information/comments (line 2)>	Optional
	OU	Obs3 - <Any additional information/comments (line 3)>	Optional
	OU (0 or more)	<Additional CA/RA information>	Optional
	OU	Certificate Profile - Qualified Certificate - Individual	Required
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Non Repudiation	Required, Critical
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2)	Optional
		Secure Email (1.3.6.1.5.5.7.3.4)	Required
Subject Alternative Name		RFC822 Name=<Email address>	Required
Subject Public Key Info		RSA (2048 bits or more)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required

Certificate Policies	Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt		Required
	Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>		Optional
	Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.1.1.1.2		Required
	Certificate Policy: Policy Identifier=0.4.0.194112.1.2		Required
	<Other Certificate Policies>		Optional
CRL Distribution Points	DistributionPoint: https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl		Required
	DistributionPoint: <Additional CRL Distribution Point(s)>		Optional
Freshest CRL	DistributionPoint: <Freshest CRL Distribution Point>		Optional
	DistributionPoint: <Additional Freshest CRL Distribution Point(s)>		Optional
QCStatements	id-qcs-pkixQCSyntax-v2 [1.3.6.1.5.5.7.11.2]	id-etsi-qcs-semanticsId-Natural [0.4.0.194121.1.1]	Required
	id-etsi-qcs-QcCompliance [0.4.0.1862.1.1]		Required
	id-etsi-qcs-QcSSCD [0.4.0.1862.1.4]		Required
	id-etsi-qcs-QcType [0.4.0.1862.1.6]	id-etsi-qct-esign [0.4.0.1862.1.6.1]	Required
	id-etsi-qcs-QcPDS [0.4.0.1862.1.5]	PdsLocation=<PDS URI> Language=en	Optional
		PdsLocation=<PDS URI> Language=<pt/other>	Optional
Authority Information Access	AIA: https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b		Optional
	AIA: <Application OCSP Responder URL>		Optional

1.1.3. PROFESSIONAL [OID: 1.3.6.1.4.1.25596.4.2.1.1.1.3]

Certificate used for eIDAS compliant qualified signature by natural persons.

This certificate profile aims to identify a natural person (individual), and their entitlement in the fulfilment of his/her profession. Usually this type of certificate is issued to members of professional associations, where the entitlement should be checked with his/her association.

0.4.0.194112.1.2 [ETSI EN 319411-2 - QCP-n-qscd].

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		Allowed signature algorithm: - 1.2.840.113549.1.1.11 - sha256WithRSAEncryption - 1.2.840.113549.1.1.13 - sha512WithRSAEncryption	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<Name of the subscriber > Can include pseudonyms, nicknames, names with spelling other than defined by the registered name, and/or additional identification attributes Ex: CN = John Doe, G = John, SN = Doe CN = *Star* John, G = John, SN = Doe CN = John *Star* Doe / num: 123456, G = John, SN = Doe	Required
	OU	RemoteQSCDManagement	Rquired (ONLY in case of remote HSM certificate)
	G	<Given Name>	Required
	SN	<Surname>	Required
	SERIALNUMBER	<Subscriber ID (NIF / CC / PASS / other), according to ETSI EN 319 412-1>	Optional
	E	<Email address>	Required
	T	<Academic degree or another that the holder can use>	Optional
	OU	Entitlement - <Professional qualification verified with the professional association or similar>	Required
	OU	Limitation1 - <Any limitations for signature use (line 1)>	Optional
	OU	Limitation2 - <Any limitations for signature use (line 2)>	Optional
	OU	Limitation3 - <Any limitations for signature use (line 3)>	Optional
	OU	Obs1 - <Any additional information/comments (line 1)>	Optional
	OU	Obs2 - <Any additional information/comments (line 2)>	Optional
	OU	Obs3 - <Any additional information/comments (line 3)>	Optional
	OU (0 or more)	<Additional CA/RA information>	Optional
	OU	Certificate Profile - Qualified Certificate - Professional	Required
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Non Repudiation	Required, Critical
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2)	Optional
		Secure Email (1.3.6.1.5.5.7.3.4)	Required
Subject Alternative Name		RFC822 Name=<Email address>	Required
Subject Public Key Info		RSA (2048 bits or more)	Required

Subject Key Identifier	Subject Public Key SHA-1		Required
Authority Key Identifier	Issuer Public Key SHA-1		Required
Certificate Policies	Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt		Required
	Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>		Optional
	Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.1.1.1.3		Required
	Certificate Policy: Policy Identifier=0.4.0.194112.1.2		Required
	<Other Certificate Policies>		Optional
CRL Distribution Points	DistributionPoint: https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl		Required
	DistributionPoint: <Additional CRL Distribution Point(s)>		Optional
Freshest CRL	DistributionPoint: <Freshest CRL Distribution Point>		Optional
	DistributionPoint: <Additional Freshest CRL Distribution Point(s)>		Optional
QCStatements	id-qcs-pkixQCSyntax-v2 [1.3.6.1.5.5.7.11.2]	id-etsi-qcs-semanticsId-Natural [0.4.0.194121.1.1]	Required
	id-etsi-qcs-QcCompliance [0.4.0.1862.1.1]		Required
	id-etsi-qcs-QcSSCD [0.4.0.1862.1.4]		Required
	id-etsi-qcs-QcType [0.4.0.1862.1.6]	id-etsi-qct-esign [0.4.0.1862.1.6.1]	Required
	id-etsi-qcs-QcPDS [0.4.0.1862.1.5]	PdsLocation=<PDS URI> Language=en	Optional
		PdsLocation=<PDS URI> Language=<pt/other>	Optional
Authority Information Access	AIA: https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b		Optional
	AIA: <Application OCSP Responder URL>		Optional

1.1.4. MEMBER [OID: 1.3.6.1.4.1.25596.4.2.1.1.1.4]

Certificate used for eIDAS compliant qualified signature by natural persons.

This certificate profile aims to identify a natural person (individual), and the position or function that takes/plays in a specified organization.

0.4.0.194112.1.2 [ETSI EN 319411-2 - QCP-n-qscd].

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		Allowed signature algorithm: - 1.2.840.113549.1.1.11 - sha256WithRSAEncryption - 1.2.840.113549.1.1.13 - sha512WithRSAEncryption	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<Name of the subscriber > Can include pseudonyms, nicknames, names with spelling other than defined by the registered name, and/or additional identification attributes Ex: CN = John Doe, G = John, SN = Doe CN = *Star* John, G = John, SN = Doe CN = John *Star* Doe / num: 123456, G = John, SN = Doe	Required
	OU	RemoteQSCDManagement	Rquired (ONLY in case of remote HSM certificate)
	G	<Given Name>	Required
	SN	<Surname>	Required
	SERIALNUMBER	<Subscriber ID (NIF / CC / PASS / other), according to ETSI EN 319 412-1>	Optional
	E	<Email address>	Required
	T	<Academic degree or another that the holder can use>	Optional
	OU	Entitlement - <Position/function that the subscriber holds in the organization (see "0" field)>	Required
	O	<Organization full name>	Required
	Organization Identifier (2.5.4.97)	<Organization ID, according to ETSI EN 319 412-1>	Required
	OU	Limitation1 - <Any limitations for signature use (line 1)>	Optional
	OU	Limitation2 - <Any limitations for signature use (line 2)>	Optional
	OU	Limitation3 - <Any limitations for signature use (line 3)>	Optional
	OU	Obs1 - <Any additional information/comments (line 1)>	Optional
	OU	Obs2 - <Any additional information/comments (line 2)>	Optional
	OU	Obs3 - <Any additional information/comments (line 3)>	Optional
	OU (0 or more)	<Additional CA/RA information>	Optional
	OU	Certificate Profile - Qualified Certificate - Member	Required
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Non Repudiation	Required, Critical
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2)	Optional
		Secure Email (1.3.6.1.5.5.7.3.4)	Required
Subject Alternative Name		RFC822 Name=<Email address>	Required

Subject Public Key Info	RSA (2048 bits or more)		Required
Subject Key Identifier	Subject Public Key SHA-1		Required
Authority Key Identifier	Issuer Public Key SHA-1		Required
Certificate Policies	Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt		Required
	Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>		Optional
	Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.1.1.1.4		Required
	Certificate Policy: Policy Identifier=0.4.0.194112.1.2		Required
	<Other Certificate Policies>		Optional
CRL Distribution Points	DistributionPoint: https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl		Required
	DistributionPoint: <Additional CRL Distribution Point(s)>		Optional
Freshest CRL	DistributionPoint: <Freshest CRL Distribution Point>		Optional
	DistributionPoint: <Additional Freshest CRL Distribution Point(s)>		Optional
QCStatements	id-qcs-pkixQCSyntax-v2 [1.3.6.1.5.5.7.11.2]	id-etsi-qcs-semanticsId-Natural [0.4.0.194121.1.1] id-etsi-qcs-SemanticsId-Legal [0.4.0.194121.1.2]	Required
	id-etsi-qcs-QcCompliance [0.4.0.1862.1.1]		Required
	id-etsi-qcs-QcSSCD [0.4.0.1862.1.4]		Required
	id-etsi-qcs-QcType [0.4.0.1862.1.6]	id-etsi-qct-esign [0.4.0.1862.1.6.1]	Required
	id-etsi-qcs-QcPDS [0.4.0.1862.1.5]	PdsLocation=<PDS URI> Language=en	Optional
		PdsLocation=<PDS URI> Language=<pt/other>	Optional
Authority Information Access	AIA: https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b		Optional
	AIA: <Application OCSP Responder URL>		Optional

1.1.5. REPRESENTATIVE [OID: 1.3.6.1.4.1.25596.4.2.1.1.1.5]

Certificate used for eIDAS compliant qualified signature by natural persons.

This certificate profile aims to identify a natural person (individual) as legal representative or attorney of a specified organization.

0.4.0.194112.1.2 [ETSI EN 319411-2 - QCP-n-qscd].

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		Allowed signature algorithm: - 1.2.840.113549.1.1.11 - sha256WithRSAEncryption - 1.2.840.113549.1.1.13 - sha512WithRSAEncryption	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<Name of the subscriber > Can include pseudonyms, nicknames, names with spelling other than defined by the registered name, and/or additional identification attributes Ex: CN = John Doe, G = John, SN = Doe CN = *Star* John, G = John, SN = Doe CN = John *Star* Doe / num: 123456, G = John, SN = Doe	Required
	OU	RemoteQSCDManagement	Rquired (ONLY in case of remote HSM certificate)
	G	<Given Name>	Required
	SN	<Surname>	Required
	SERIALNUMBER	<Subscriber ID (NIF / CC / PASS / other), according to ETSI EN 319 412-1>	Required
	E	<Email address>	Required
	T	<Powers of representation/qualification that the subscriber holds in the organization (see "0" field)>	Required
	O	<Organization full name>	Required
	Organization Identifier (2.5.4.97)	<Organization ID, according to ETSI EN 319 412-1>	Required
	OU	eidas-np-rep-lp-pt	Required
	OU	eidas-rep-limit-1: <Any limitations for signature use (line 1)>	Optional
	OU	eidas-rep-limit-2: <Any limitations for signature use (line 2)>	Optional
	OU	eidas-rep-limit-3: <Any limitations for signature use (line 3)>	Optional
	OU	Obs1 - <Any additional information/comments (line 1)>	Optional
	OU	Obs2 - <Any additional information/comments (line 2)>	Optional
	OU	Obs3 - <Any additional information/comments (line 3)>	Optional
	OU (0 or more)	<Additional CA/RA information>	Optional
	OU	Certificate Profile - Qualified Certificate - Representative	Required
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Non Repudiation	Required, Critical
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2)	Optional
		Secure Email (1.3.6.1.5.5.7.3.4)	Required
Subject Alternative Name		RFC822 Name=<Email address>	Required

Subject Public Key Info	RSA (2048 bits or more)		Required
Subject Key Identifier	Subject Public Key SHA-1		Required
Authority Key Identifier	Issuer Public Key SHA-1		Required
Certificate Policies	Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt		Required
	Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>		Optional
	Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.1.1.1.5		Required
	Certificate Policy: Policy Identifier=0.4.0.194112.1.2		Required
	<Other Certificate Policies>		Optional
CRL Distribution Points	DistributionPoint: https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl		Required
	DistributionPoint: <Additional CRL Distribution Point(s)>		Optional
Freshest CRL	DistributionPoint: <Freshest CRL Distribution Point>		Optional
	DistributionPoint: <Additional Freshest CRL Distribution Point(s)>		Optional
QCStatements	id-qcs-pkixQCSyntax-v2 [1.3.6.1.5.5.7.11.2]	id-etsi-qcs-semanticsId-Natural [0.4.0.194121.1.1] id-etsi-qcs-SemanticsId-Legal [0.4.0.194121.1.2]	Required
	id-etsi-qcs-QcCompliance [0.4.0.1862.1.1]		Required
	id-etsi-qcs-QcSSCD [0.4.0.1862.1.4]		Required
	id-etsi-qcs-QcType [0.4.0.1862.1.6]	id-etsi-qct-esign [0.4.0.1862.1.6.1]	Required
	id-etsi-qcs-QcPDS [0.4.0.1862.1.5]	PdsLocation=<PDS URI> Language=en	Optional
		PdsLocation=<PDS URI> Language=<pt/other>	Optional
Authority Information Access	AIA: https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b		Optional
	AIA: <Application OCSP Responder URL>		Optional

1.1.6. ORGANIZATION (ESEAL) [OID: 1.3.6.1.4.1.25596.4.2.1.1.1.6]

Certificate used for eIDAS compliant qualified seal by legal persons.

0.4.0.194112.1.3 [ETSI EN 319411-2 - QCP-l-qscd].

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		Allowed signature algorithm: - 1.2.840.113549.1.1.11 - sha256WithRSAEncryption - 1.2.840.113549.1.1.13 - sha512WithRSAEncryption	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<Organization name or authorized trademark>	Required
	OU	RemoteQSCDManagement	Rquired (ONLY in case of remote HSM certificate)
	E	<Email address>	Required
	O	<Organization full name>	Required
	Organization Identifier (2.5.4.97)	<Organization ID, according to ETSI EN 319 412-1>	Required
	OU	Limitation1 - <Any limitations for signature use (line 1)>	Optional
	OU	Limitation2 - <Any limitations for signature use (line 2)>	Optional
	OU	Limitation3 - <Any limitations for signature use (line 3)>	Optional
	OU	Obs1 - <Any additional information/comments (line 1)>	Optional
	OU	Obs2 - <Any additional information/comments (line 2)>	Optional
	OU	Obs3 - <Any additional information/comments (line 3)>	Optional
	OU (0 or more)	<Additional CA/RA information>	Optional
	OU	Certificate Profile - Qualified Certificate - Organization	Required
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Non Repudiation	Required, Critical
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2)	Optional
		Secure Email (1.3.6.1.5.5.7.3.4)	Required
Subject Alternative Name		RFC822 Name=<Email address>	Required
Subject Public Key Info		RSA (2048 bits or more)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required
Certificate Policies		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
		Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional

	Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.1.1.1.6		Required
	Certificate Policy: Policy Identifier=0.4.0.194112.1.3		Required
	<Other Certificate Policies>		Optional
CRL Distribution Points	DistributionPoint: https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl		Required
	DistributionPoint: <Additional CRL Distribution Point(s)>		Optional
Freshest CRL	DistributionPoint: <Freshest CRL Distribution Point>		Optional
	DistributionPoint: <Additional Freshest CRL Distribution Point(s)>		Optional
QCStatements	id-qcs-pkixQCSyntax-v2 [1.3.6.1.5.5.7.11.2]	id-etsi-qcs-SemanticsId-Legal [0.4.0.194121.1.2]	Required
	id-etsi-qcs-QcCompliance [0.4.0.1862.1.1]		Required
	id-etsi-qcs-QcSSCD [0.4.0.1862.1.4]		Required
	id-etsi-qcs-QcType [0.4.0.1862.1.6]	id-etsi-qct-eseal [0.4.0.1862.1.6.2]	Required
	id-etsi-qcs-QcPDS [0.4.0.1862.1.5]	PdsLocation=<PDS URI> Language=en	Optional
		PdsLocation=<PDS URI> Language=<pt/other>	Optional
Authority Information Access	AIA: https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b		Optional
	AIA: <Application OCSP Responder URL>		Optional

1.2. DIGITALSIGN QUALIFIED TSA CA G1

1.2.1. OCSP [OID: 1.3.6.1.4.1.25596.4.2.1.2.1.1]

Certificate used by OCSP Responder to sign and verify the OCSP service's responses regarding the status of the certificates issued by the CA.

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		1.2.840.113549.1.1.13 - sha512WithRSAEncryption	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<OCSP Application Name>	Required
	O	DigitalSign Certificadora Digital	Required
	OU (0 or more)	<Additional CA/RA information>	Optional
	C	PT	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Digital Signature	Required, Critical
Extended Key Usage		id-kp-OCSP (1.3.6.1.5.5.7.3.9)	Required
Subject Public Key Info		RSA (2048 bits or more)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required
Certificate Policies		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
		Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional
		Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.1.2.1.1	Required
		<Other Certificate Policies>	Optional
No check extension		1.3.6.1.5.5.7.48.1.5 (05 00)	Required
Authority Information Access		AIA: https://qtsa-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDTSACAG1.p7b	Optional

1.2.2. TIMESTAMP [OID: 1.3.6.1.4.1.25596.4.2.1.2.1.2]

Certificate used for by TimeStamping Authorities (TSA) to provide eIDAS compliant qualified timestamping services.

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		Allowed signature algorithm: - 1.2.840.113549.1.1.11 - sha256WithRSAEncryption - 1.2.840.113549.1.1.13 - sha512WithRSAEncryption	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<TSA Application Name>	Required
	O	<Organization full name>	Required
	Organization Identifier (2.5.4.97)	<Organization ID, according to ETSI EN 319 412-1>	Required
	OU (0 or more)	<Additional CA/RA information>	Optional
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Digital Signature	Required, Critical
		Non Repudiation	Required, Critical
Extended Key Usage		Time Stamping (1.3.6.1.5.5.7.3.8)	Required, Critical
Subject Public Key Info		RSA (2048 bits or more)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required
Certificate Policies		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
		Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional
		Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.1.2.1.2	Required
		<Other Certificate Policies>	Optional
CRL Distribution Points		DistributionPoint: https://qtsa-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDTSACAG1.crl	Required
		DistributionPoint: <Additional CRL Distribution Point(s)>	Optional
Freshest CRL		DistributionPoint: <Freshest CRL Distribution Point>	Optional
		DistributionPoint: <Additional Freshest CRL Distribution Point(s)>	Optional
Authority Information Access		AIA: https://qtsa-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDTSACAG1.p7b	Optional
		AIA: <Application OCSP Responder URL>	Optional

1.3. DIGITALSIGN CA G1

1.3.1. OCSP [OID: 1.3.6.1.4.1.25596.4.2.1.3.1.1]

Certificate used by OCSP Responder to sign and verify the OCSP service's responses regarding the status of the certificates issued by the CA.

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		1.2.840.113549.1.1.13 - sha512WithRSAEncryption	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<OCSP Application Name>	Required
	O	DigitalSign Certificadora Digital	Required
	OU (0 or more)	<Additional CA/RA information>	Optional
	C	PT	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Digital Signature	Required, Critical
Extended Key Usage		id-kp-OCSP (1.3.6.1.5.5.7.3.9)	Required
Subject Public Key Info		RSA (2048 bits or more)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required
Certificate Policies		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
		Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional
		Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.1.3.1.1	Required
		<Other Certificate Policies>	Optional
No check extension		1.3.6.1.5.5.7.48.1.5 (05 00)	Required
Authority Information Access		AIA: https://advca-g1.digitalsign.pt/DIGITALSIGNCAG1.p7b	Optional

1.3.2. BASIC [OID: 1.3.6.1.4.1.25596.4.2.1.3.1.2]

Certificate used for electronic signature/encryption by natural persons or electronic seal/encryption by legal persons.

This certificate profile aims to identify a natural or a legal person.

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		Allowed signature algorithm: - 1.2.840.113549.1.1.11 - sha256WithRSAEncryption - 1.2.840.113549.1.1.13 - sha512WithRSAEncryption	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<Name of the subscriber > Can include pseudonyms, nicknames, names with spelling other than defined by the registered name, and/or additional identification attributes	Required
	OU	RemoteQSCDManagement	Rquired (ONLY in case of remote HSM certificate)
	E	<Email address>	Required
	OU	Authentication - Email Authenticated	Required
	OU (0 or more)	<Additional CA/RA information>	Optional
	OU	Certificate Profile - Basic	Required
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Non Repudiation, Digital Signature, Key Encipherment	Required, Critical
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2)	Optional
		Secure Email (1.3.6.1.5.5.7.3.4)	Required
Subject Alternative Name		RFC822 Name=<Email address>	Required
Subject Public Key Info		RSA (2048 bits or more)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required
Certificate Policies		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
		Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional
		Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.1.3.1.2	Required
		<Other Certificate Policies>	Optional
CRL Distribution Points		DistributionPoint: https://advca-g1.digitalsign.pt/DIGITALSIGNCAG1.crl	Required
		DistributionPoint: <Additional CRL Distribution Point(s)>	Optional
Freshest CRL		DistributionPoint: <Freshest CRL Distribution Point>	Optional
		DistributionPoint: <Additional Freshest CRL Distribution Point(s)>	Optional
Authority Information Access		AIA: https://advca-g1.digitalsign.pt/DIGITALSIGNCAG1.p7b	Optional
		AIA: <Application OCSP Responder URL>	Optional

1.3.3. INDIVIDUAL [OID: 1.3.6.1.4.1.25596.4.2.1.3.1.3]

Certificate used for electronic signature/encryption by natural persons.

This certificate profile aims to identify a natural person (individual).

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		Allowed signature algorithm: - 1.2.840.113549.1.1.11 - sha256WithRSAEncryption - 1.2.840.113549.1.1.13 - sha512WithRSAEncryption	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<Name of the subscriber > Can include pseudonyms, nicknames, names with spelling other than defined by the registered name, and/or additional identification attributes	Required
	OU	RemoteQSCDManagement	Rquired (ONLY in case of remote HSM certificate)
	SERIALNUMBER	<Subscriber ID (NIF / CC / PASS / other), according to ETSI EN 319 412-1>	Optional
	E	<Email address>	Required
	T	<Academic degree or another that the holder can use>	Optional
	OU	Limitation1 - <Any limitations for signature use (line 1)>	Optional
	OU	Limitation2 - <Any limitations for signature use (line 2)>	Optional
	OU	Limitation3 - <Any limitations for signature use (line 3)>	Optional
	OU	Obs1 - <Any additional information/comments (line 1)>	Optional
	OU	Obs2 - <Any additional information/comments (line 2)>	Optional
	OU	Obs3 - <Any additional information/comments (line 3)>	Optional
	OU	Authentication - Identity Authenticated	Required
	OU (0 or more)	<Additional CA/RA information>	Optional
	OU	Certificate Profile - Individual	Required
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Non Repudiation, Digital Signature, Key Encipherment	Required, Critical
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2)	Optional
		Secure Email (1.3.6.1.5.5.7.3.4)	Required
Subject Alternative Name		RFC822 Name=<Email address>	Required
Subject Public Key Info		RSA (2048 bits or more)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required
Certificate Policies		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
		Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional

	Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.1.3.1.3	Required
	<Other Certificate Policies>	Optional
CRL Distribution Points	DistributionPoint: https://advca-g1.digitalsign.pt/DIGITALSIGNCAG1.crl	Required
	DistributionPoint: <Additional CRL Distribution Point(s)>	Optional
Freshest CRL	DistributionPoint: <Freshest CRL Distribution Point>	Optional
	DistributionPoint: <Additional Freshest CRL Distribution Point(s)>	Optional
Authority Information Access	AIA: https://advca-g1.digitalsign.pt/DIGITALSIGNCAG1.p7b	Optional
	AIA: <Application OCSP Responder URL>	Optional

1.3.4. MEMBER [OID: 1.3.6.1.4.1.25596.4.2.1.3.1.4]

Certificate used for electronic signature/encryption by natural persons.

This certificate profile aims to identify a natural person (individual), and the position or function that takes/plays in a specified organization.

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		Allowed signature algorithm: - 1.2.840.113549.1.1.11 - sha256WithRSAEncryption - 1.2.840.113549.1.1.13 - sha512WithRSAEncryption	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<Name of the subscriber > Can include pseudonyms, nicknames, names with spelling other than defined by the registered name, and/or additional identification attributes	Required
	OU	RemoteQSCDManagement	Rquired (ONLY in case of remote HSM certificate)
	SERIALNUMBER	<Subscriber ID (NIF / CC / PASS / other), according to ETSI EN 319 412-1>	Optional
	E	<Email address>	Required
	T	<Position/function that the subscriber holds in the organization (see "0" field)>	Optional
	O	<Organization full name>	Required
	Organization Identifier (2.5.4.97)	<Organization ID, according to ETSI EN 319 412-1>	Required
	OU	Limitation1 - <Any limitations for signature use (line 1)>	Optional
	OU	Limitation2 - <Any limitations for signature use (line 2)>	Optional
	OU	Limitation3 - <Any limitations for signature use (line 3)>	Optional
	OU	Obs1 - <Any additional information/comments (line 1)>	Optional
	OU	Obs2 - <Any additional information/comments (line 2)>	Optional
	OU	Obs3 - <Any additional information/comments (line 3)>	Optional
	OU	Authentication - Identity Authenticated	Required
	OU (0 or more)	<Additional CA/RA information>	Optional
	OU	Certificate Profile - Member	Required
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Non Repudiation, Digital Signature, Key Encipherment	Required, Critical
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2)	Optional
		Secure Email (1.3.6.1.5.5.7.3.4)	Required
Subject Alternative Name		RFC822 Name=<Email address>	Required
Subject Public Key Info		RSA (2048 bits or more)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required

Certificate Policies	Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
	Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional
	Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.1.3.1.4	Required
	<Other Certificate Policies>	Optional
CRL Distribution Points	DistributionPoint: https://advca-g1.digitalsign.pt/DIGITALSIGNCAG1.crl	Required
	DistributionPoint: <Additional CRL Distribution Point(s)>	Optional
Freshest CRL	DistributionPoint: <Freshest CRL Distribution Point>	Optional
	DistributionPoint: <Additional Freshest CRL Distribution Point(s)>	Optional
Authority Information Access	AIA: https://advca-g1.digitalsign.pt/DIGITALSIGNCAG1.p7b	Optional
	AIA: <Application OCSP Responder URL>	Optional

1.3.5. ORGANIZATION (ESEAL) [OID: 1.3.6.1.4.1.25596.4.2.1.3.1.5]

Certificate used for electronic seal by legal persons.

This certificate profile aims to identify a legal person (organization).

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		Allowed signature algorithm: - 1.2.840.113549.1.1.11 - sha256WithRSAEncryption - 1.2.840.113549.1.1.13 - sha512WithRSAEncryption	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<Organization name or authorized trademark>	Required
	OU	RemoteQSCDManagement	Rquired (ONLY in case of remote HSM certificate)
	E	<Email address>	Required
	O	<Organization full name >	Required
	Organization Identifier (2.5.4.97)	<Organization ID, according to ETSI EN 319 412-1>	Required
	OU	Limitation1 - <Any limitations for signature use (line 1)>	Optional
	OU	Limitation2 - <Any limitations for signature use (line 2)>	Optional
	OU	Limitation3 - <Any limitations for signature use (line 3)>	Optional
	OU	Obs1 - <Any additional information/comments (line 1)>	Optional
	OU	Obs2 - <Any additional information/comments (line 2)>	Optional
	OU	Obs3 - <Any additional information/comments (line 3)>	Optional
	OU	Authentication - Identity Authenticated	Required
	OU (0 or more)	<Additional CA/RA information>	Optional
	OU	Certificate Profile - Organization	Required
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Non Repudiation, Digital Signature, Key Encipherment	Required, Critical
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2)	Optional
		Secure Email (1.3.6.1.5.5.7.3.4)	Required
Subject Alternative Name		RFC822 Name=<Email address>	Required
Subject Public Key Info		RSA (2048 bits or more)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required
Certificate Policies		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
		Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional

	Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.1.3.1.5	Required
	<Other Certificate Policies>	Optional
CRL Distribution Points	DistributionPoint: https://advca-g1.digitalsign.pt/DIGITALSIGNCAG1.crl	Required
	DistributionPoint: <Additional CRL Distribution Point(s)>	Optional
Freshest CRL	DistributionPoint: <Freshest CRL Distribution Point>	Optional
	DistributionPoint: <Additional Freshest CRL Distribution Point(s)>	Optional
Authority Information Access	AIA: https://advca-g1.digitalsign.pt/DIGITALSIGNCAG1.p7b	Optional
	AIA: <Application OCSP Responder URL>	Optional

1.4. DIGITALSIGN TSA CA G1

1.4.1. OCSP [OID: 1.3.6.1.4.1.25596.4.2.1.4.1.1]

Certificate used by OCSP Responder to sign and verify the OCSP service's responses regarding the status of the certificates issued by the CA.

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		1.2.840.113549.1.1.13 - sha512WithRSAEncryption	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<OCSP Application Name>	Required
	O	DigitalSign Certificadora Digital	Required
	OU (0 or more)	<Additional CA/RA information>	Optional
	C	PT	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Digital Signature	Required, Critical
Extended Key Usage		id-kp-OCSP (1.3.6.1.5.5.7.3.9)	Required
Subject Public Key Info		RSA (2048 bits or more)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required
Certificate Policies		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
		Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional
		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.2.1.4.1.1	Required
		<Other Certificate Policies>	Optional
No check extension		1.3.6.1.5.5.7.48.1.5 (05 00)	Required
Authority Information Access		AIA: https://advtsa-g1.digitalsign.pt/DIGITALSIGNTSACAG1.p7b	Optional

1.4.2. TIMESTAMP [OID: 1.3.6.1.4.1.25596.4.2.1.4.1.2]

Certificate used for by TimeStamping Authorities (TSA) to provide timestamping services.

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		Allowed signature algorithm: - 1.2.840.113549.1.1.11 - sha256WithRSAEncryption - 1.2.840.113549.1.1.13 - sha512WithRSAEncryption	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<TSA Application Name>	Required
	O	<Organization full name>	Required
	Organization Identifier (2.5.4.97)	<Organization ID, according to ETSI EN 319 412-1>	Required
	OU (0 or more)	<Additional CA/RA information>	Optional
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Digital Signature	Required, Critical
		Non Repudiation	Required, Critical
Extended Key Usage		Time Stamping (1.3.6.1.5.5.7.3.8)	Required, Critical
Subject Public Key Info		RSA (2048 bits or more)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required
Certificate Policies		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
		Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional
		Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.1.4.1.2	Required
		<Other Certificate Policies>	Optional
CRL Distribution Points		DistributionPoint: https://advtsa-g1.digitalsign.pt/DIGITALSIGNTSACAG1.crl	Required
		DistributionPoint: <Additional CRL Distribution Point(s)>	Optional
Freshest CRL		DistributionPoint: <Freshest CRL Distribution Point>	Optional
		DistributionPoint: <Additional Freshest CRL Distribution Point(s)>	Optional
Authority Information Access		AIA: https://advtsa-g1.digitalsign.pt/DIGITALSIGNTSACAG1.p7b	Optional
		AIA: <Application OCSP Responder URL>	Optional

2. ECDSA HIERARCHY

2.1. DIGITALSIGN QUALIFIED CA V1

2.1.1. OCSP [OID: 1.3.6.1.4.1.25596.4.2.2.1.1.1]

Certificate used by OCSP Responder to sign and verify the OCSP service's responses regarding the status of the certificates issued by the CA.

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		1.2.840.10045.4.3.3 - sha384ECDSA	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<OCSP Application Name>	Required
	O	DigitalSign Certificadora Digital	Required
	OU (0 or more)	<Additional CA/RA information>	Optional
	C	PT	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Digital Signature	Required, Critical
Extended Key Usage		id-kp-OCSP (1.3.6.1.5.5.7.3.9)	Required
Subject Public Key Info		1.2.840.10045.2.1 + 1.3.132.0.34 (ECC 384 bits)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required
Certificate Policies		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
		Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional
		Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.2.1.1.1	Required
		<Other Certificate Policies>	Optional
No check extension		1.3.6.1.5.5.7.48.1.5 (05 00)	Required
Authority Information Access		AIA: https://qca-v1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAV1.p7b	Optional

2.1.2. INDIVIDUAL [OID: 1.3.6.1.4.1.25596.4.2.2.1.1.2]

Certificate used for eIDAS compliant qualified signature by natural persons.

This certificate profile aims to identify a natural person (individual).

0.4.0.194112.1.2 [ETSI EN 319411-2 - QCP-n-qscd].

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		Allowed signature algorithm: - 1.2.840.10045.4.3.2 - sha256ECDSA - 1.2.840.10045.4.3.3 - sha384ECDSA	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<Name of the subscriber > Can include pseudonyms, nicknames, names with spelling other than defined by the registered name, and/or additional identification attributes Ex: CN = John Doe, G = John, SN = Doe CN = *Star* John, G = John, SN = Doe CN = John *Star* Doe / num: 123456, G = John, SN = Doe	Required
	OU	RemoteQSCDManagement	Rquired (ONLY in case of remote HSM certificate)
	G	<Given Name>	Required
	SN	<Surname>	Required
	SERIALNUMBER	<Subscriber ID (NIF / CC / PASS / other), according to ETSI EN 319 412-1>	Optional
	E	<Email address>	Required
	T	<Academic degree or another that the holder can use>	Optional
	OU	Limitation1 - <Any limitations for signature use (line 1)>	Optional
	OU	Limitation2 - <Any limitations for signature use (line 2)>	Optional
	OU	Limitation3 - <Any limitations for signature use (line 3)>	Optional
	OU	Obs1 - <Any additional information/comments (line 1)>	Optional
	OU	Obs2 - <Any additional information/comments (line 2)>	Optional
	OU	Obs3 - <Any additional information/comments (line 3)>	Optional
	OU (0 or more)	<Additional CA/RA information>	Optional
	OU	Certificate Profile - Qualified Certificate - Individual	Required
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Non Repudiation	Required, Critical
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2)	Required
		Secure Email (1.3.6.1.5.5.7.3.4)	Required
Subject Alternative Name		RFC822 Name=<Email address>	Required
Subject Public Key Info		1.2.840.10045.2.1 + 1.2.840.10045.3.1.7 (ECC 256 bits)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required

Certificate Policies	Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt		Required
	Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>		Optional
	Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.2.1.1.2		Required
	Certificate Policy: Policy Identifier=0.4.0.194112.1.2		Required
	<Other Certificate Policies>		Optional
CRL Distribution Points	DistributionPoint: https://qca-v1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAV1.crl		Required
	DistributionPoint: <Additional CRL Distribution Point(s)>		Optional
Freshest CRL	DistributionPoint: <Freshest CRL Distribution Point>		Optional
	DistributionPoint: <Additional Freshest CRL Distribution Point(s)>		Optional
QCStatements	id-qcs-pkixQCSyntax-v2 [1.3.6.1.5.5.7.11.2]	id-etsi-qcs-semanticsId-Natural [0.4.0.194121.1.1]	Required
	id-etsi-qcs-QcCompliance [0.4.0.1862.1.1]		Required
	id-etsi-qcs-QcSSCD [0.4.0.1862.1.4]		Required
	id-etsi-qcs-QcType [0.4.0.1862.1.6]	id-etsi-qct-esign [0.4.0.1862.1.6.1]	Required
	id-etsi-qcs-QcPDS [0.4.0.1862.1.5]	PdsLocation=<PDS URI> Language=en	Optional
		PdsLocation=<PDS URI> Language=<pt/other>	Optional
Authority Information Access	AIA: https://qca-v1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAV1.p7b		Optional
	AIA: <Application OCSP Responder URL>		Optional

2.1.3. PROFESSIONAL [OID: 1.3.6.1.4.1.25596.4.2.2.1.1.3]

Certificate used for eIDAS compliant qualified signature by natural persons.

This certificate profile aims to identify a natural person (individual), and their entitlement in the fulfilment of his/her profession. Usually this type of certificate is issued to members of professional associations, where the entitlement should be checked with his/her association.

0.4.0.194112.1.2 [ETSI EN 319411-2 - QCP-n-qscd].

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		Allowed signature algorithm: - 1.2.840.10045.4.3.2 - sha256ECDSA - 1.2.840.10045.4.3.3 - sha384ECDSA	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<Name of the subscriber > Can include pseudonyms, nicknames, names with spelling other than defined by the registered name, and/or additional identification attributes Ex: CN = John Doe, G = John, SN = Doe CN = *Star* John, G = John, SN = Doe CN = John *Star* Doe / num: 123456, G = John, SN = Doe	Required
	OU	RemoteQSCDManagement	Rquired (ONLY in case of remote HSM certificate)
	G	<Given Name>	Required
	SN	<Surname>	Required
	SERIALNUMBER	<Subscriber ID (NIF / CC / PASS / other), according to ETSI EN 319 412-1>	Optional
	E	<Email address>	Required
	T	<Academic degree or another that the holder can use>	Optional
	OU	Entitlement - <Professional qualification verified with the professional association or similar>	Required
	OU	Limitation1 - <Any limitations for signature use (line 1)>	Optional
	OU	Limitation2 - <Any limitations for signature use (line 2)>	Optional
	OU	Limitation3 - <Any limitations for signature use (line 3)>	Optional
	OU	Obs1 - <Any additional information/comments (line 1)>	Optional
	OU	Obs2 - <Any additional information/comments (line 2)>	Optional
	OU	Obs3 - <Any additional information/comments (line 3)>	Optional
	OU (0 or more)	<Additional CA/RA information>	Optional
	OU	Certificate Profile - Qualified Certificate - Professional	Required
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Non Repudiation	Required, Critical
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2)	Required
		Secure Email (1.3.6.1.5.5.7.3.4)	Required
Subject Alternative Name		RFC822 Name=<Email address>	Required
Subject Public Key Info		1.2.840.10045.2.1 + 1.2.840.10045.3.1.7 (ECC 256 bits)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required

Authority Key Identifier	Issuer Public Key SHA-1		Required
Certificate Policies	Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt		Required
	Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>		Optional
	Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.2.1.1.3		Required
	Certificate Policy: Policy Identifier=0.4.0.194112.1.2		Required
	<Other Certificate Policies>		Optional
CRL Distribution Points	DistributionPoint: https://qca-v1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAV1.crl		Required
	DistributionPoint: <Additional CRL Distribution Point(s)>		Optional
Freshest CRL	DistributionPoint: <Freshest CRL Distribution Point>		Optional
	DistributionPoint: <Additional Freshest CRL Distribution Point(s)>		Optional
QCStatements	id-qcs-pkixQCSyntax-v2 [1.3.6.1.5.5.7.11.2]	id-etsi-qcs-semanticsId-Natural [0.4.0.194121.1.1]	Required
	id-etsi-qcs-QcCompliance [0.4.0.1862.1.1]		Required
	id-etsi-qcs-QcSSCD [0.4.0.1862.1.4]		Required
	id-etsi-qcs-QcType [0.4.0.1862.1.6]	id-etsi-qct-esign [0.4.0.1862.1.6.1]	Required
	id-etsi-qcs-QcPDS [0.4.0.1862.1.5]	PdsLocation=<PDS URI> Language=en	Optional
		PdsLocation=<PDS URI> Language=<pt/other>	Optional
Authority Information Access	AIA: https://qca-v1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAV1.p7b		Optional
	AIA: <Application OCSP Responder URL>		Optional

2.1.4. MEMBER [OID: 1.3.6.1.4.1.25596.4.2.2.1.1.4]

Certificate used for eIDAS compliant qualified signature by natural persons.

This certificate profile aims to identify a natural person (individual), and the position or function that takes/plays in a specified organization.

0.4.0.194112.1.2 [ETSI EN 319411-2 - QCP-n-qscd].

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		Allowed signature algorithm: - 1.2.840.10045.4.3.2 - sha256ECDSA - 1.2.840.10045.4.3.3 - sha384ECDSA	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<Name of the subscriber > Can include pseudonyms, nicknames, names with spelling other than defined by the registered name, and/or additional identification attributes Ex: CN = John Doe, G = John, SN = Doe CN = *Star* John, G = John, SN = Doe CN = John *Star* Doe / num: 123456, G = John, SN = Doe	Required
	OU	RemoteQSCDManagement	Rquired (ONLY in case of remote HSM certificate)
	G	<Given Name>	Required
	SN	<Surname>	Required
	SERIALNUMBER	<Subscriber ID (NIF / CC / PASS / other), according to ETSI EN 319 412-1>	Optional
	E	<Email address>	Required
	T	<Academic degree or another that the holder can use>	Optional
	OU	Entitlement - <Position/function that the subscriber holds in the organization (see "0" field)>	Required
	O	<Organization full name>	Required
	Organization Identifier (2.5.4.97)	<Organization ID, according to ETSI EN 319 412-1>	Required
	OU	Limitation1 - <Any limitations for signature use (line 1)>	Optional
	OU	Limitation2 - <Any limitations for signature use (line 2)>	Optional
	OU	Limitation3 - <Any limitations for signature use (line 3)>	Optional
	OU	Obs1 - <Any additional information/comments (line 1)>	Optional
	OU	Obs2 - <Any additional information/comments (line 2)>	Optional
	OU	Obs3 - <Any additional information/comments (line 3)>	Optional
	OU (0 or more)	<Additional CA/RA information>	Optional
	OU	Certificate Profile - Qualified Certificate - Member	Required
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Non Repudiation	Required, Critical
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2)	Required
		Secure Email (1.3.6.1.5.5.7.3.4)	Required
Subject Alternative Name		RFC822 Name=<Email address>	Required

Subject Public Key Info	1.2.840.10045.2.1 + 1.2.840.10045.3.1.7 (ECC 256 bits)		Required
Subject Key Identifier	Subject Public Key SHA-1		Required
Authority Key Identifier	Issuer Public Key SHA-1		Required
Certificate Policies	Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt		Required
	Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>		Optional
	Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.2.1.1.4		Required
	Certificate Policy: Policy Identifier=0.4.0.194112.1.2		Required
	<Other Certificate Policies>		Optional
CRL Distribution Points	DistributionPoint: https://qca-v1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAV1.crl		Required
	DistributionPoint: <Additional CRL Distribution Point(s)>		Optional
Freshest CRL	DistributionPoint: <Freshest CRL Distribution Point>		Optional
	DistributionPoint: <Additional Freshest CRL Distribution Point(s)>		Optional
QCStatements	id-qcs-pkixQCSyntax-v2 [1.3.6.1.5.5.7.11.2]	id-etsi-qcs-semanticsId-Natural [0.4.0.194121.1.1] id-etsi-qcs-SemanticsId-Legal [0.4.0.194121.1.2]	Required
	id-etsi-qcs-QcCompliance [0.4.0.1862.1.1]		Required
	id-etsi-qcs-QcSSCD [0.4.0.1862.1.4]		Required
	id-etsi-qcs-QcType [0.4.0.1862.1.6]	id-etsi-qct-esign [0.4.0.1862.1.6.1]	Required
	id-etsi-qcs-QcPDS [0.4.0.1862.1.5]	PdsLocation=<PDS URI> Language=en	Optional
		PdsLocation=<PDS URI> Language=<pt/other>	Optional
Authority Information Access	AIA: https://qca-v1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAV1.p7b		Optional
	AIA: <Application OCSP Responder URL>		Optional

2.1.5. REPRESENTATIVE [OID: 1.3.6.1.4.1.25596.4.2.2.1.1.5]

Certificate used for eIDAS compliant qualified signature by natural persons.

This certificate profile aims to identify a natural person (individual) as legal representative or attorney of a specified organization.

0.4.0.194112.1.2 [ETSI EN 319411-2 - QCP-n-qscd].

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		Allowed signature algorithm: - 1.2.840.10045.4.3.2 - sha256ECDSA - 1.2.840.10045.4.3.3 - sha384ECDSA	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<Name of the subscriber > Can include pseudonyms, nicknames, names with spelling other than defined by the registered name, and/or additional identification attributes Ex: CN = John Doe, G = John, SN = Doe CN = *Star* John, G = John, SN = Doe CN = John *Star* Doe / num: 123456, G = John, SN = Doe	Required
	OU	RemoteQSCDManagement	Rquired (ONLY in case of remote HSM certificate)
	G	<Given Name>	Required
	SN	<Surname>	Required
	SERIALNUMBER	<Subscriber ID (NIF / CC / PASS / other), according to ETSI EN 319 412-1>	Required
	E	<Email address>	Required
	T	<Powers of representation/qualification that the subscriber holds in the organization (see "0" field)>	Required
	O	<Organization full name>	Required
	Organization Identifier (2.5.4.97)	<Organization ID, according to ETSI EN 319 412-1>	Required
	OU	eidas-np-rep-lp-pt	Required
	OU	eidas-rep-limit-1: <Any limitations for signature use (line 1)>	Optional
	OU	eidas-rep-limit-2: <Any limitations for signature use (line 2)>	Optional
	OU	eidas-rep-limit-3: <Any limitations for signature use (line 3)>	Optional
	OU	Obs1 - <Any additional information/comments (line 1)>	Optional
	OU	Obs2 - <Any additional information/comments (line 2)>	Optional
	OU	Obs3 - <Any additional information/comments (line 3)>	Optional
	OU (0 or more)	<Additional CA/RA information>	Optional
	OU	Certificate Profile - Qualified Certificate - Representative	Required
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Non Repudiation	Required, Critical
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2)	Required
		Secure Email (1.3.6.1.5.5.7.3.4)	Required
Subject Alternative Name		RFC822 Name=<Email address>	Required

Subject Public Key Info	1.2.840.10045.2.1 + 1.2.840.10045.3.1.7 (ECC 256 bits)		Required
Subject Key Identifier	Subject Public Key SHA-1		Required
Authority Key Identifier	Issuer Public Key SHA-1		Required
Certificate Policies	Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt		Required
	Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>		Optional
	Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.2.1.1.5		Required
	Certificate Policy: Policy Identifier=0.4.0.194112.1.2		Required
	<Other Certificate Policies>		Optional
CRL Distribution Points	DistributionPoint: https://qca-v1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAV1.crl		Required
	DistributionPoint: <Additional CRL Distribution Point(s)>		Optional
Freshest CRL	DistributionPoint: <Freshest CRL Distribution Point>		Optional
	DistributionPoint: <Additional Freshest CRL Distribution Point(s)>		Optional
QCStatements	id-qcs-pkixQCSyntax-v2 [1.3.6.1.5.5.7.11.2]	id-etsi-qcs-semanticsId-Natural [0.4.0.194121.1.1] id-etsi-qcs-SemanticsId-Legal [0.4.0.194121.1.2]	Required
	id-etsi-qcs-QcCompliance [0.4.0.1862.1.1]		Required
	id-etsi-qcs-QcSSCD [0.4.0.1862.1.4]		Required
	id-etsi-qcs-QcType [0.4.0.1862.1.6]	id-etsi-qct-esign [0.4.0.1862.1.6.1]	Required
	id-etsi-qcs-QcPDS [0.4.0.1862.1.5]	PdsLocation=<PDS URI> Language=en	Optional
		PdsLocation=<PDS URI> Language=<pt/other>	Optional
Authority Information Access	AIA: https://qca-v1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAV1.p7b		Optional
	AIA: <Application OCSP Responder URL>		Optional

2.1.6. ORGANIZATION (ESEAL) [OID: 1.3.6.1.4.1.25596.4.2.2.1.1.6]

Certificate used for eIDAS compliant qualified seal by legal persons.

0.4.0.194112.1.3 [ETSI EN 319411-2 - QCP-l-qscd].

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		Allowed signature algorithm: - 1.2.840.10045.4.3.2 - sha256ECDSA - 1.2.840.10045.4.3.3 - sha384ECDSA	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<Organization name or authorized trademark>	Required
	OU	RemoteQSCDManagement	Rquired (ONLY in case of remote HSM certificate)
	E	<Email address>	Required
	O	<Organization full name>	Required
	Organization Identifier (2.5.4.97)	<Organization ID, according to ETSI EN 319 412-1>	Required
	OU	Limitation1 - <Any limitations for signature use (line 1)>	Optional
	OU	Limitation2 - <Any limitations for signature use (line 2)>	Optional
	OU	Limitation3 - <Any limitations for signature use (line 3)>	Optional
	OU	Obs1 - <Any additional information/comments (line 1)>	Optional
	OU	Obs2 - <Any additional information/comments (line 2)>	Optional
	OU	Obs3 - <Any additional information/comments (line 3)>	Optional
	OU (0 or more)	<Additional CA/RA information>	Optional
	OU	Certificate Profile - Qualified Certificate - Organization	Required
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Non Repudiation	Required, Critical
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2)	Required
		Secure Email (1.3.6.1.5.5.7.3.4)	Required
Subject Alternative Name		RFC822 Name=<Email address>	Required
Subject Public Key Info		1.2.840.10045.2.1 + 1.2.840.10045.3.1.7 (ECC 256 bits)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required
Certificate Policies		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
		Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional
		Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.2.1.1.6	Required

	Certificate Policy: Policy Identifier=0.4.0.194112.1.3		Required
	<Other Certificate Policies>		Optional
CRL Distribution Points	DistributionPoint: https://qca-v1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAV1.crl		Required
	DistributionPoint: <Additional CRL Distribution Point(s)>		Optional
Freshest CRL	DistributionPoint: <Freshest CRL Distribution Point>		Optional
	DistributionPoint: <Additional Freshest CRL Distribution Point(s)>		Optional
QCStatements	id-qcs-pkixQCSyntax-v2 [1.3.6.1.5.5.7.11.2]	id-etsi-qcs-SemanticsId-Legal [0.4.0.194121.1.2]	Required
	id-etsi-qcs-QcCompliance [0.4.0.1862.1.1]		Required
	id-etsi-qcs-QcSSCD [0.4.0.1862.1.4]		Required
	id-etsi-qcs-QcType [0.4.0.1862.1.6]	id-etsi-qct-eseal [0.4.0.1862.1.6.2]	Required
	id-etsi-qcs-QcPDS [0.4.0.1862.1.5]	PdsLocation=<PDS URI> Language=en	Optional
		PdsLocation=<PDS URI> Language=<pt/other>	Optional
Authority Information Access	AIA: https://qca-v1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAV1.p7b		Optional
	AIA: <Application OCSP Responder URL>		Optional

2.2. DIGITALSIGN QUALIFIED TSA V1

2.2.1. OCSP [OID: 1.3.6.1.4.1.25596.4.2.2.2.1.1]

Certificate used by OCSP Responder to sign and verify the OCSP service's responses regarding the status of the certificates issued by the CA.

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		1.2.840.10045.4.3.3 - sha384ECDSA	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<OCSP Application Name>	Required
	O	DigitalSign Certificadora Digital	Required
	OU (0 or more)	<Additional CA/RA information>	Optional
	C	PT	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Digital Signature	Required, Critical
Extended Key Usage		id-kp-OCSP (1.3.6.1.5.5.7.3.9)	Required
Subject Public Key Info		1.2.840.10045.2.1 + 1.3.132.0.34 (ECC 384 bits)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required
Certificate Policies		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
		Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional
		Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.2.2.1.1	Required
		<Other Certificate Policies>	Optional
No check extension		1.3.6.1.5.5.7.48.1.5 (05 00)	Required
Authority Information Access		AIA: https://qtsa-v1.digitalsign.pt/DIGITALSIGNQUALIFIEDTSACAV1.p7b	Optional

2.2.2. TIMESTAMP [OID: 1.3.6.1.4.1.25596.4.2.2.2.1.2]

Certificate used for by TimeStamping Authorities (TSA) to provide eIDAS compliant qualified timestamping services.

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		1.2.840.10045.4.3.3 - sha384ECDSA	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<TSA Application Name>	Required
	O	<Organization full name>	Required
	Organization Identifier (2.5.4.97)	<Organization ID, according to ETSI EN 319 412-1>	Required
	OU (0 or more)	<Additional CA/RA information>	Optional
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Digital Signature	Required, Critical
		Non Repudiation	Required, Critical
Extended Key Usage		Time Stamping (1.3.6.1.5.5.7.3.8)	Required, Critical
Subject Public Key Info		1.2.840.10045.2.1 + 1.3.132.0.34 (ECC 384 bits)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required
Certificate Policies		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
		Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional
		Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.2.2.1.2	Required
		<Other Certificate Policies>	Optional
CRL Distribution Points		DistributionPoint: https://qtsa-v1.digitalsign.pt/DIGITALSIGNTQUALIFIEDTSACAV1.crl	Required
		DistributionPoint: <Additional CRL Distribution Point(s)>	Optional
Freshest CRL		DistributionPoint: <Freshest CRL Distribution Point>	Optional
		DistributionPoint: <Additional Freshest CRL Distribution Point(s)>	Optional
Authority Information Access		AIA: https://qtsa-v1.digitalsign.pt/DIGITALSIGNQUALIFIEDTSACAV1.p7b	Optional
		AIA: <Application OCSP Responder URL>	Optional

2.3. DIGITALSIGN CA V1

2.3.1. OCSP [OID: 1.3.6.1.4.1.25596.4.2.2.3.1.1]

Certificate used by OCSP Responder to sign and verify the OCSP service's responses regarding the status of the certificates issued by the CA.

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		1.2.840.10045.4.3.3 - sha384ECDSA	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<OCSP Application Name>	Required
	O	DigitalSign Certificadora Digital	Required
	OU (0 or more)	<Additional CA/RA information>	Optional
	C	PT	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Digital Signature	Required, Critical
Extended Key Usage		id-kp-OCSP (1.3.6.1.5.5.7.3.9)	Required
Subject Public Key Info		1.2.840.10045.2.1 + 1.3.132.0.34 (ECC 384 bits)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required
Certificate Policies		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
		Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional
		Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.2.3.1.1	Required
		<Other Certificate Policies>	Optional
No check extension		1.3.6.1.5.5.7.48.1.5 (05 00)	Required
Authority Information Access		AIA: https://advca-v1.digitalsign.pt/DIGITALSIGNCAV1.p7b	Optional

2.3.2. BASIC [OID: 1.3.6.1.4.1.25596.4.2.2.3.1.2]

Certificate used for electronic signature/encryption by natural persons or electronic seal/encryption by legal persons.

This certificate profile aims to identify a natural or a legal person.

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		Allowed signature algorithm: - 1.2.840.10045.4.3.2 - sha256ECDSA - 1.2.840.10045.4.3.3 - sha384ECDSA	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<Name of the subscriber > Can include pseudonyms, nicknames, names with spelling other than defined by the registered name, and/or additional identification attributes	Required
	OU	RemoteQSCDManagement	Rquired (ONLY in case of remote HSM certificate)
	E	<Email address>	Required
	OU	Authentication - Email Authenticated	Required
	OU (0 or more)	<Additional CA/RA information>	Optional
	OU	Certificate Profile - Basic	Required
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Non Repudiation, Digital Signature, Key Encipherment	Required, Critical
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2)	Required
		Secure Email (1.3.6.1.5.5.7.3.4)	Required
Subject Alternative Name		RFC822 Name=<Email address>	Required
Subject Public Key Info		1.2.840.10045.2.1 + 1.2.840.10045.3.1.7 (ECC 256 bits)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required
Certificate Policies		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
		Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional
		Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.2.3.1.2	Required
		<Other Certificate Policies>	Optional
CRL Distribution Points		DistributionPoint: https://advca-v1.digitalsign.pt/DIGITALSIGNCAV1.crl	Required
		DistributionPoint: <Additional CRL Distribution Point(s)>	Optional
Freshest CRL		DistributionPoint: <Freshest CRL Distribution Point>	Optional
		DistributionPoint: <Additional Freshest CRL Distribution Point(s)>	Optional
Authority Information Access		AIA: https://advca-v1.digitalsign.pt/DIGITALSIGNCAV1.p7b	Optional

	AIA: <Application OCSP Responder URL>	Optional

2.3.3. INDIVIDUAL [OID: 1.3.6.1.4.1.25596.4.2.2.3.1.3]

Certificate used for electronic signature/encryption by natural persons.

This certificate profile aims to identify a natural person (individual).

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		Allowed signature algorithm: - 1.2.840.10045.4.3.2 - sha256ECDSA - 1.2.840.10045.4.3.3 - sha384ECDSA	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<Name of the subscriber > Can include pseudonyms, nicknames, names with spelling other than defined by the registered name, and/or additional identification attributes	Required
	OU	RemoteQSCDManagement	Rquired (ONLY in case of remote HSM certificate)
	SERIALNUMBER	<Subscriber ID (NIF / CC / PASS / other), according to ETSI EN 319 412-1>	Optional
	E	<Email address>	Required
	T	<Academic degree or another that the holder can use>	Optional
	OU	Limitation1 - <Any limitations for signature use (line 1)>	Optional
	OU	Limitation2 - <Any limitations for signature use (line 2)>	Optional
	OU	Limitation3 - <Any limitations for signature use (line 3)>	Optional
	OU	Obs1 - <Any additional information/comments (line 1)>	Optional
	OU	Obs2 - <Any additional information/comments (line 2)>	Optional
	OU	Obs3 - <Any additional information/comments (line 3)>	Optional
	OU	Authentication - Identity Authenticated	Required
	OU (0 or more)	<Additional CA/RA information>	Optional
	OU	Certificate Profile - Individual	Required
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Non Repudiation, Digital Signature, Key Encipherment	Required, Critical
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2)	Required
		Secure Email (1.3.6.1.5.5.7.3.4)	Required
Subject Alternative Name		RFC822 Name=<Email address>	Required
Subject Public Key Info		1.2.840.10045.2.1 + 1.2.840.10045.3.1.7 (ECC 256 bits)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required
Certificate Policies		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
		Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional

	Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.2.3.1.3	Required
	<Other Certificate Policies>	Optional
CRL Distribution Points	DistributionPoint: https://advca-v1.digitalsign.pt/DIGITALSIGNCAV1.crl	Required
	DistributionPoint: <Additional CRL Distribution Point(s)>	Optional
Freshest CRL	DistributionPoint: <Freshest CRL Distribution Point>	Optional
	DistributionPoint: <Additional Freshest CRL Distribution Point(s)>	Optional
Authority Information Access	AIA: https://advca-v1.digitalsign.pt/DIGITALSIGNCAV1.p7b	Optional
	AIA: <Application OCSP Responder URL>	Optional

2.3.4. MEMBER [OID: 1.3.6.1.4.1.25596.4.2.2.3.1.4]

Certificate used for electronic signature/encryption by natural persons.

This certificate profile aims to identify a natural person (individual), and the position or function that takes/plays in a specified organization.

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		Allowed signature algorithm: - 1.2.840.10045.4.3.2 - sha256ECDSA - 1.2.840.10045.4.3.3 - sha384ECDSA	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<Name of the subscriber > Can include pseudonyms, nicknames, names with spelling other than defined by the registered name, and/or additional identification attributes	Required
	OU	RemoteQSCDManagement	Rquired (ONLY in case of remote HSM certificate)
	SERIALNUMBER	<Subscriber ID (NIF / CC / PASS / other), according to ETSI EN 319 412-1>	Optional
	E	<Email address>	Required
	T	<Position/function that the subscriber holds in the organization (see "0" field)>	Optional
	O	<Organization full name>	Required
	Organization Identifier (2.5.4.97)	<Organization ID, according to ETSI EN 319 412-1>	Required
	OU	Limitation1 - <Any limitations for signature use (line 1)>	Optional
	OU	Limitation2 - <Any limitations for signature use (line 2)>	Optional
	OU	Limitation3 - <Any limitations for signature use (line 3)>	Optional
	OU	Obs1 - <Any additional information/comments (line 1)>	Optional
	OU	Obs2 - <Any additional information/comments (line 2)>	Optional
	OU	Obs3 - <Any additional information/comments (line 3)>	Optional
	OU	Authentication - Identity Authenticated	Required
	OU (0 or more)	<Additional CA/RA information>	Optional
	OU	Certificate Profile - Member	Required
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Non Repudiation, Digital Signature, Key Encipherment	Required, Critical
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2)	Required
		Secure Email (1.3.6.1.5.5.7.3.4)	Required
Subject Alternative Name		RFC822 Name=<Email address>	Required
Subject Public Key Info		1.2.840.10045.2.1 + 1.2.840.10045.3.1.7 (ECC 256 bits)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required

Certificate Policies	Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
	Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional
	Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.2.3.1.4	Required
	<Other Certificate Policies>	Optional
CRL Distribution Points	DistributionPoint: https://advca-v1.digitalsign.pt/DIGITALSIGNCAV1.crl	Required
	DistributionPoint: <Additional CRL Distribution Point(s)>	Optional
Freshest CRL	DistributionPoint: <Freshest CRL Distribution Point>	Optional
	DistributionPoint: <Additional Freshest CRL Distribution Point(s)>	Optional
Authority Information Access	AIA: https://advca-v1.digitalsign.pt/DIGITALSIGNCAV1.p7b	Optional
	AIA: <Application OCSP Responder URL>	Optional

2.3.5. ORGANIZATION (ESEAL) [OID: 1.3.6.1.4.1.25596.4.2.2.3.1.5]

Certificate used for electronic seal by legal persons.

This certificate profile aims to identify a legal person (organization).

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		Allowed signature algorithm: - 1.2.840.10045.4.3.2 - sha256ECDSA - 1.2.840.10045.4.3.3 - sha384ECDSA	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<Organization name or authorized trademark>	Required
	OU	RemoteQSCDManagement	Rquired (ONLY in case of remote HSM certificate)
	E	<Email address>	Required
	O	<Organization full name>	Required
	Organization Identifier (2.5.4.97)	<Organization ID, according to ETSI EN 319 412-1>	Required
	OU	Limitation1 - <Any limitations for signature use (line 1)>	Optional
	OU	Limitation2 - <Any limitations for signature use (line 2)>	Optional
	OU	Limitation3 - <Any limitations for signature use (line 3)>	Optional
	OU	Obs1 - <Any additional information/comments (line 1)>	Optional
	OU	Obs2 - <Any additional information/comments (line 2)>	Optional
	OU	Obs3 - <Any additional information/comments (line 3)>	Optional
	OU	Authentication - Identity Authenticated	Required
	OU (0 or more)	<Additional CA/RA information>	Optional
	OU	Certificate Profile - Organization	Required
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Non Repudiation, Digital Signature, Key Encipherment	Required, Critical
Extended Key Usage		Client Authentication (1.3.6.1.5.5.7.3.2)	Required
		Secure Email (1.3.6.1.5.5.7.3.4)	Required
Subject Alternative Name		RFC822 Name=<Email address>	Required
Subject Public Key Info		1.2.840.10045.2.1 + 1.2.840.10045.3.1.7 (ECC 256 bits)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required
Certificate Policies		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
		Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional

	Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.2.3.1.5	Required
	<Other Certificate Policies>	Optional
CRL Distribution Points	DistributionPoint: https://advca-v1.digitalsign.pt/DIGITALSIGNCAV1.crl	Required
	DistributionPoint: <Additional CRL Distribution Point(s)>	Optional
Freshest CRL	DistributionPoint: <Freshest CRL Distribution Point>	Optional
	DistributionPoint: <Additional Freshest CRL Distribution Point(s)>	Optional
Authority Information Access	AIA: https://advca-v1.digitalsign.pt/DIGITALSIGNCAV1.p7b	Optional
	AIA: <Application OCSP Responder URL>	Optional

2.4. DIGITALSIGN TSA CA V1

2.4.1. OCSP [OID: 1.3.6.1.4.1.25596.4.2.2.4.1.1]

Certificate used by OCSP Responder to sign and verify the OCSP service's responses regarding the status of the certificates issued by the CA.

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		1.2.840.10045.4.3.3 - sha384ECDSA	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<OCSP Application Name>	Required
	O	DigitalSign Certificadora Digital	Required
	OU (0 or more)	<Additional CA/RA information>	Optional
	C	PT	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Digital Signature	Required, Critical
Extended Key Usage		id-kp-OCSP (1.3.6.1.5.5.7.3.9)	Required
Subject Public Key Info		1.2.840.10045.2.1 + 1.3.132.0.34 (ECC 384 bits)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required
Certificate Policies		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
		Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional
		Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.2.4.1.1	Required
		<Other Certificate Policies>	Optional
No check extension		1.3.6.1.5.5.7.48.1.5 (05 00)	Required
Authority Information Access		AIA: https://advtsa-v1.digitalsign.pt/DIGITALSIGNTSACAV1.p7b	Optional

2.4.2. TIMESTAMP [OID: 1.3.6.1.4.1.25596.4.2.2.4.1.2]

Certificate used for by TimeStamping Authorities (TSA) to provide timestamping services.

Certificate Component		Value / Description	Type
Version		V3	Required
Serial Number (certificate)		<Unique serial number of the certificate>	Required
signatureAlgorithm		1.2.840.10045.4.3.3 - sha384ECDSA	Required
Issuer		<Issuer CA DN>	Required
not Before		<Initial validity>	Required
not After		<Final validity>	Required
Subject	CN	<TSA Application Name>	Required
	O	<Organization full name>	Required
	Organization Identifier (2.5.4.97)	<Organization ID, according to ETSI EN 319 412-1>	Required
	OU (0 or more)	<Additional CA/RA information>	Optional
	C	<Country of the subscriber>	Required
Basic Constraints		CA=False	Required, Critical
Key Usage		Digital Signature	Required, Critical
		Non Repudiation	Required, Critical
Extended Key Usage		Time Stamping (1.3.6.1.5.5.7.3.8)	Required, Critical
Subject Public Key Info		1.2.840.10045.2.1 + 1.3.132.0.34 (ECC 384 bits)	Required
Subject Key Identifier		Subject Public Key SHA-1	Required
Authority Key Identifier		Issuer Public Key SHA-1	Required
Certificate Policies		Certificate Policy: Policy Identifier = 1.3.6.1.4.1.25596.4.1.1 Policy Qualifier Info: Policy qualifier id = CPS Qualifier = https://pki.digitalsign.pt	Required
		Policy Qualifier Id=User Notice Qualifier: Notice Text=<Notice>	Optional
		Certificate Policy: Policy Identifier=1.3.6.1.4.1.25596.4.2.2.4.1.2	Required
		<Other Certificate Policies>	Optional
CRL Distribution Points		DistributionPoint: https://advtsa-v1.digitalsign.pt/DIGITALSIGNTSACAV1.crl	Required
		DistributionPoint: <Additional CRL Distribution Point(s)>	Optional
Freshest CRL		DistributionPoint: <Freshest CRL Distribution Point>	Optional
		DistributionPoint: <Additional Freshest CRL Distribution Point(s)>	Optional
Authority Information Access		AIA: https://advtsa-v1.digitalsign.pt/DIGITALSIGNTSACAV1.p7b	Optional
		AIA: <Application OCSP Responder URL>	Optional