Certificate Profiles List

List

MULTICERT_PJ.ECRAIZ_428_en

Rating: Public

Version: 14.0

Date: 01/04/2026

Normative Version

MULTICERT - Serviços de Certificação Electrónica, S.A.,
Alfrapark, Edifício E, Estrada de Alfragide, 67, 2610-008 AMADORA - PORTUGAL
Telephone: +351 217 123 010

Document Identifier: MULTICERT_PJ.ECRAIZ_428_en

Keywords: Certificate ; Profile

Document Type: List

Title: Certificate Profiles List

Original Laguage: Portuguese

Publishing Language: English

Rating: Public

Date: 01/04/2026

Current Version: 14.0

Version History

Version Nº	Date	Details	Author(s)
1.0	10/09/2018	Certificate profiles list creation	Multicert S.A.
1.1-1.5	29/01/2019	Review of application certificate	Multicert S.A.
2.0	29/01/2019	New version published	Multicert S.A.
2.1	30/04/2019	Inclusion of PSD2 certificate profiles	Multicert S.A.
3.0	30/04/2019	New version published	Multicert S.A.
3.1	09/12/2019	Review	Multicert S.A.
4.0	09/12/2019	New version published	Multicert S.A.
4.1	10/12/2020	Review	Multicert S.A.
5.0	17/12/2020	New version published	Multicert S.A.
5.1	04/01/2021	Review of SSL KU field	Multicert S.A.
6.0	04/01/2021	New version published	Multicert S.A.
6.1	31/03/2022	Review	Multicert S.A.
7.0	31/03/2022	New version published	Multicert S.A.
7.1	24/08/2022	Review of services certificate profiles	Multicert S.A.
8.0	24/08/2022	New version published	Multicert S.A.
8.1	30/06/2023	Review	Multicert S.A.
9.0	01/07/2023	Approval	Multicert S.A.
9.1	14/11/2024	Review	Multicert S.A.
10.0	14/11/2024	Approval	Multicert S.A.
10.1	11/02/2025	Review	Multicert S.A.
11.0	13/02/2025	Approval	Multicert S.A.
11.1	18/02/2025	Inclusion of public key and signature algorithm fields	Multicert S.A.
12.0	18/02/2025	Approval	Multicert S.A.
12.1	22/09/2025	Review	Multicert S.A.
13.0	15/12/2025	Approval	Multicert S.A.
13.1	01/04/2026	General review, inclusion of EKU information, inclusion of new EKU in qualified signature certificates, qualified electronic seal, advanced signature	Multicert S.A.
14.0	01/04/2026	Approval	Multicert S.A.

Related Documents

Document ID	Details	Author(s)
MULTICERT_PJ.ECRAIZ_426_en	Multicert Certificate Policy	MULTICERT S.A.
MULTICERT_PJ.ECRAIZ_427_en	Multicert Certification Practice Statement	MULTICERT S.A.

Copyright © 2002- 2026 MULTICERT - All rights reserved.

Summary

Certificate Profiles List 1
Summary 4
1 Root Certification Authority Certificate Profile 5
2 Subordinate Certification Authority Certificate Profile 6
3 Qualified Digital Certificate Profile 8
4 Authentication Digital Certificate Profile 14
5 Services Digital Certificate Profile 17
6 Advanced Digital Certificate Profile 20
7 Timestamp Certificate Profile 23
Approval 26

Copyright © 2002- 2026 MULTICERT - All rights reserved.

1 Root Certification Authority Certificate Profile

Certificate Component[1]	MULTICERT Root Certification Authority 01
Signature Algorithm	
	sha256RSA
Subject Distinguished Name	
Common Name (CN)	Mandatory
	MULTICERT Root Certification Authority 01
Organization (O)	Mandatory
	MULTICERT - Serviços de Certificação Electrónica S.A.
Country (C)	Mandatory
	PT
Public Key	
	RSA (4096 Bits)
Key Usage	
	Certificate Signing (keyCertSign)
	CRL Signing (cRLSign)

[1] n.a. – not applicable

Copyright © 2002- 2026 MULTICERT - All rights reserved.

2 Subordinate Certification Authority Certificate Profile

Certificate Component[2]	MULTICERT Trust Services Certification Authority 005	MULTICERT QWAC Certification Authority 005	MULTICERT Timestamping Certification Authority 005	MULTICERT Advanced Certification Authority 005	Multicert Trust Services Certification Authority 002	Multicert Advanced Certification Authority 001
EU Trusted List Service	CA/QC	CA/QC	TSA/QTST	CA/PKC	CA/QC	CA/PKC
Signature Algorithm						
	sha256RSA	sha256RSA	sha256RSA	sha256RSA	sha256RSA	sha256RSA
Subject Distinguished Name						
Common Name (CN)	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
	MULTICERT Trust Services Certification Authority 005	MULTICERT QWAC Certification Authority 005	MULTICERT Timestamping Certification Authority 005	MULTICERT Advanced Certification Authority 005	MULTICERT Trust Services Certification Authority 002	MULTICERT Advanced Certification Authority 001
Organization (O)	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
	MULTICERT - Serviços de Certificação Electrónica S.A.	MULTICERT - Serviços de Certificação Electrónica S.A.	MULTICERT - Serviços de Certificação Electrónica S.A.	MULTICERT - Serviços de Certificação Electrónica S.A.	MULTICERT - Serviços de Certificação Electrónica S.A.	MULTICERT - Serviços de Certificação Electrónica S.A.
Country (C)	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
	PT	PT	PT	PT	PT	PT
Public Key						
	RSA (4096 Bits)	RSA (4096 Bits)	RSA (4096 Bits)	RSA (4096 Bits)	RSA (4096 Bits)	RSA (4096 Bits)
Key Usage						
	Certificate Signing (keyCertSign)	Certificate Signing (keyCertSign)	Certificate Signing (keyCertSign)	Certificate Signing (keyCertSign)	Certificate Signing (keyCertSign)	Certificate Signing (keyCertSign)

[2] n.a. – not applicable

Copyright © 2002- 2026 MULTICERT - All rights reserved.

	CRL Signing (cRLSign)	CRL Signing (cRLSign)	CRL Signing (cRLSign)	CRL Signing (cRLSign)	CRL Signing (cRLSign)	CRL Signing (cRLSign)
Extended Key Usage						
	Client Authentication (1.3.6.1.5.5.7.3.2)	Client Authentication (1.3.6.1.5.5.7.3.2)	Time Stamping (1.3.6.1.5.5.7.3.8)	Client Authentication (1.3.6.1.5.5.7.3.2)	n.a	n.a
	Email Protection (1.3.6.1.5.5.7.3.4)	Server Authentication (1.3.6.1.5.5.7.3.1)	n.a.	Email Protection (1.3.6.1.5.5.7.3.4)	n.a	n.a
Certificate Policies						
	OID: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: https://pki.multicert.com	OID: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: https://pki.multicert.com	OID: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: https://pki.multicert.com	OID: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: https://pki.multicert.com	OID: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: http://pkiroot.multicert.com	OID: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: http://pkiroot.multicert.com
	n.a.	n.a.	n.a.	n.a.	OID: 1.3.6.1.4.1.25070.1.1.1.0.1.2 URI: http://pkiroot.multicert.com	OID: 1.3.6.1.4.1.25070.1.1.1.0.1.2 URI: http://pkiroot.multicert.com

Copyright © 2002- 2026 MULTICERT - All rights reserved.

3 Qualified Digital Certificate Profile

Certificate Component[3]	Collective Person Representative Effects	Professional Quality	Private Quality	Professional Individual	Private Individual	Electronic Seal	Electronic Seal PSD2
Signature Algorithm							
	sha256RSA	sha256RSA	sha256RSA	sha256RSA	sha256RSA	sha256RSA	sha256RSA
Subject Distinguished Name							
Common Name (CN)	Mandatory <certificate subscriber name>	Mandatory Option 1: <certificate subscriber name> Option 2: <certificate subscriber professional name>	Mandatory <certificate subscriber name>	Mandatory <certificate subscriber name>	Mandatory <certificate subscriber name>	Mandatory <organization name>	Mandatory <organization name>
Serial Number (SERIALNUMBER)	Mandatory Option 1: <identification document type><country>-<identification document nº> Option 2: When the QC Statement OID 1.3.6.1.5.5.7.11.2 is present with the syntax https://pki.multicert.com, the Serial Number follows the rules described in Annex A Option 3: When the Residence Title is presented, the Serial Number follows the rule described in line 1 of	Mandatory Option 1: <identification document type><country>-<identification document nº or professional card nº> Option 2: When the QC Statement OID 1.3.6.1.5.5.7.11.2 is present with the syntax https://pki.multicert.com, the Serial Number follows the rules described in Annex A Option 3: When the Residence Title is presented, the Serial Number follows the rule described in line 1 of Annex	Mandatory Option 1: <identification document type><country>-<identification document nº> Option 2: When the QC Statement OID 1.3.6.1.5.5.7.11.2 is present with the syntax https://pki.multicert.com, the Serial Number follows the rules described in Annex A Option 3: TIN<country>-<tax number> Option 4: When the Residence Title is presented, the Serial Number follows the rule	Mandatory Option 1: <identification document type><country>-<identification document nº> Option 2: When the QC Statement OID 1.3.6.1.5.5.7.11.2 is present with the syntax https://pki.multicert.com, the Serial Number follows the rules described in Annex A Option 3: When the Residence Title is presented, the Serial Number follows the rule described in line	Mandatory Option 1: <identification document type><country>-<identification document nº> Option 2: When the QC Statement OID 1.3.6.1.5.5.7.11.2 is present with the syntax https://pki.multicert.com, the Serial Number follows the rules described in Annex A Option 3: When the Residence Title is presented, the Serial Number follows the rule described in line 1 of Annex A	n.a.	n.a.

[3] n.a. – not applicable

Copyright © 2002- 2026 MULTICERT - All rights reserved.

Certificate Component[3]	Collective Person Representative Effects	Professional Quality	Private Quality	Professional Individual	Private Individual	Electronic Seal	Electronic Seal PSD2
	Annex A	A	described in line 1 of Annex A	1 of Annex A			
Title (T)	Mandatory <quality of the certificate subscriber, as part of its use for a qualified digital signature>	Mandatory <quality of the certificate subscriber, as part of its use for a qualified digital signature>	Mandatory <quality of the certificate subscriber, as part of its use for a qualified digital signature>	n.a.	n.a.	n.a.	n.a.
Organizational Unit (OU)	Optional; but it must be present if it is a Qualified Remote Signing Certificate RemoteQSCDManagement	Optional; but it must be present if it is a Qualified Remote Signing Certificate RemoteQSCDManagement	Optional; but it must be present if it is a Qualified Remote Signing Certificate RemoteQSCDManagement	Optional; but it must be present if it is a Qualified Remote Signing Certificate RemoteQSCDManagement	Optional; but it must be present if it is a Qualified Remote Signing Certificate RemoteQSCDManagement	Optional; but it must be present if it is a Qualified Remote Signing Certificate RemoteQSCDManagement	n.a.
Organizational Unit (OU)	Mandatory Certificado para pessoal singular – Assinatura Qualificada	Mandatory Certificado para pessoal singular – Assinatura Qualificada	Mandatory Certificado para pessoal singular – Assinatura Qualificada	Mandatory Certificado para pessoal singular – Assinatura Qualificada	Mandatory Certificado para pessoal singular – Assinatura Qualificada	Mandatory Qualified Certificate for Electronic Seal	Mandatory PSD2 Qualified Certificate for Electronic Seal
Organizational Unit (OU)	n.a.	Optional <area/department/specialty of the Organization to which the certificate subscriber belongs>	Optional; but present if it is a digital signature for electronic invoice Uso limitado a fatura eletrónica/Limited to electronic invoice	n.a.	n.a.	Optional; but present if it is an electronic seal for electronic invoice Uso limitado a fatura eletrónica/Limited to electronic invoice	n.a.
Organization Identifier (2.5.4.97)	Mandatory VAT<country>-<tax number of the Organization>	n.a.	n.a.	n.a.	n.a.	Mandatory VAT<country>-<tax number of the Organization>	Mandatory PSD<country>-<NCA code>-<authorization number>
Organization (O)	Mandatory <name of the Organization to which the certificate subscriber belongs>	Mandatory <name of the Organization to which the certificate subscriber belongs>	n.a.	Mandatory <name of the Organization to which the certificate subscriber belongs>	n.a.	Mandatory <name of the Organization>	Mandatory <name of the Organization>
Country (C)	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory

Copyright © 2002- 2026 MULTICERT - All rights reserved.

Certificate Component[3]	Collective Person Representative Effects	Professional Quality	Private Quality	Professional Individual	Private Individual	Electronic Seal	Electronic Seal PSD2
	<citizenship of the certificate subscriber>	<citizenship of the certificate subscriber or country of the entity>	<citizenship of the certificate subscriber>	<citizenship of the certificate subscriber>	<citizenship of the certificate subscriber>	<citizenship of the certificate subscriber>	<citizenship of the certificate subscriber>
Pseudonym (2.5.4.65)	n.a.	Optional; but it must be present the pseudonym attribute or the givenName and surname attributes <short name of the certificate subscriber>	n.a.	n.a.	n.a.	n.a.	n.a.
GivenName (G)	n.a.	Optional; but it must be present the pseudonym attribute or the givenName and surname attributes <first name of the certificate subscriber>	Optional; but it must be present the pseudonym attribute or the givenName and surname attributes <first name of the certificate subscriber>	Optional; but it must be present the pseudonym attribute or the givenName and surname attributes <first name of the certificate subscriber>	Optional; but it must be present the pseudonym attribute or the givenName and surname attributes <first name of the certificate subscriber>	n.a.	n.a.
Surname (SN)	n.a.	Optional; but it must be present the pseudonym attribute or the givenName and surname attributes <last name of the certificate subscriber>	Optional; but it must be present the pseudonym attribute or the givenName and surname attributes <last name of the certificate subscriber>	Optional; but it must be present the pseudonym attribute or the givenName and surname attributes <last name of the certificate subscriber>	Optional; but it must be present the pseudonym attribute or the givenName and surname attributes <last name of the certificate subscriber>	n.a.	n.a.
emailAddress (E)	n.a.	n.a.	Optional <email address of the certificate subscriber>	n.a.	n.a.	n.a.	n.a.
Locality (L)	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
State or Province (ST)	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
Public Key							
	RSA (2048 Bits until 2025-12-16) RSA (3072 Bits or 4096 Bits after 2025-12-16)	RSA (2048 Bits until 2025-12-16) RSA (3072 Bits or 4096 Bits after 2025-12-16)	RSA (2048 Bits until 2025-12-16) RSA (3072 Bits or 4096 Bits after 2025-12-16)	RSA (2048 Bits until 2025-12-16) RSA (3072 Bits or 4096 Bits after 2025-12-16)	RSA (2048 Bits until 2025-12-16) RSA (3072 Bits or 4096 Bits after 2025-12-16)	RSA (2048 Bits until 2025-12-16) RSA (3072 Bits or 4096 Bits after 2025-	RSA (2048 Bits until 2025-12-16) RSA (3072 Bits or 4096 Bits after 2025-

Copyright © 2002- 2026 MULTICERT - All rights reserved.

Certificate Component[3]	Collective Person Representative Effects	Professional Quality	Private Quality	Professional Individual	Private Individual	Electronic Seal	Electronic Seal PSD2
						12-16)	12-16)
Subject Alternative Name							
RFC 822 Name (e-mail address)	Mandatory <email address of the certificate subscriber>	Optional <email address of the certificate subscriber>	Mandatory <email address of the certificate subscriber>	Mandatory <email address of the certificate subscriber>	Mandatory <email address of the certificate subscriber>	Mandatory <email address of the certificate subscriber>	n.a.
Key Usage							
	Non-Repudiation (nonRepudiation)	Non-Repudiation (nonRepudiation)	Non-Repudiation (nonRepudiation)	Non-Repudiation (nonRepudiation)	Non-Repudiation (nonRepudiation)	Non-Repudiation (nonRepudiation)	Non-Repudiation (nonRepudiation)
Extended Key Usage							
	Email Protection (1.3.6.1.5.5.7.3.4) MS Document Signing (1.3.6.1.4.1.311.3.10.3.12) (after 2026-04-07) Adobe Authentic Document Trust (1.2.840.113583.1.1.5) (after 2026-04-07) Document Signing (1.3.6.1.5.5.7.3.36) (after 2026-04-07)	Email Protection (1.3.6.1.5.5.7.3.4) MS Document Signing (1.3.6.1.4.1.311.3.10.3.12) (after 2026-04-07) Adobe Authentic Document Trust (1.2.840.113583.1.1.5) (after 2026-04-07) Document Signing (1.3.6.1.5.5.7.3.36) (after 2026-04-07)	Email Protection (1.3.6.1.5.5.7.3.4) MS Document Signing (1.3.6.1.4.1.311.3.10.3.12) (after 2026-04-07) Adobe Authentic Document Trust (1.2.840.113583.1.1.5) (after 2026-04-07) Document Signing (1.3.6.1.5.5.7.3.36) (after 2026-04-07)	Email Protection (1.3.6.1.5.5.7.3.4) MS Document Signing (1.3.6.1.4.1.311.3.10.3.12) (after 2026-04-07) Adobe Authentic Document Trust (1.2.840.113583.1.1.5) (after 2026-04-07) Document Signing (1.3.6.1.5.5.7.3.36) (after 2026-04-07)	Email Protection (1.3.6.1.5.5.7.3.4) MS Document Signing (1.3.6.1.4.1.311.3.10.3.12) (after 2026-04-07) Adobe Authentic Document Trust (1.2.840.113583.1.1.5) (after 2026-04-07) Document Signing (1.3.6.1.5.5.7.3.36) (after 2026-04-07)	Email Protection (1.3.6.1.5.5.7.3.4) MS Document Signing (1.3.6.1.4.1.311.3.10.3.12) (after 2026-04-07) Adobe Authentic Document Trust (1.2.840.113583.1.1.5) (after 2026-04-07) Document Signing (1.3.6.1.5.5.7.3.36) (after 2026-04-07)	n.a.
Certificate Policies							
	OID: 1.3.6.1.4.1.25070.1.1.1.0.7	OID: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: https://pki.multicert.com	OID: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: https://pki.multicert.com	OID: 1.3.6.1.4.1.25070.1.1.1.0.7	OID: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: https://pki.multicert.com	OID: 1.3.6.1.4.1.25070.1.1.1.0.7	OID: 1.3.6.1.4.1.25070.1.1.1.0.7

Copyright © 2002- 2026 MULTICERT - All rights reserved.

Certificate Component[3]	Collective Person Representative Effects	Professional Quality	Private Quality	Professional Individual	Private Individual	Electronic Seal	Electronic Seal PSD2
	URI: https://pki.multicert.com			URI: https://pki.multicert.com		URI: https://pki.multicert.com	URI: https://pki.multicert.com
	n.a					OID: 1.3.6.1.4.1.25070.1.1.1.1.0.7 URI: https://pki.multicert.com	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.7 URI: https://pki.multicert.com
	OID: 0.4.0.194112.1.2	OID: 0.4.0.194112.1.2	Present for general usage OID: 0.4.0.194112.1.2	OID: 0.4.0.194112.1.2	OID: 0.4.0.194112.1.2	OID: 0.4.0.194112.1.3	OID: 0.4.0.194112.1.1
			Present if used for electronic invoice OID: 1.3.6.1.4.1.25070.1.1.1.1.0.1.22				
	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.1.2	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.1.2	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.1.2	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.1.2	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.1.2	Present for general usage OID: 1.3.6.1.4.1.25070.1.1.1.1.0.1.14	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.1.14 (until 2019-10-18)
						Present if used for electronic invoice OID: 1.3.6.1.4.1.25070.1.1.1.1.0.1.19	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.1.18 (after 2019-10-18)
QC Statements							
	1.3.6.1.5.5.7.11.2					1.3.6.1.5.5.7.11.2	1.3.6.1.5.5.7.11.2
	0.4.0.1862.1.1					0.4.0.1862.1.1	0.4.0.1862.1.1
	0.4.0.1862.1.3 :07					0.4.0.1862.1.3 :07	0.4.0.1862.1.3 :07
	0.4.0.1862.1.4					0.4.0.1862.1.4	0.4.0.1862.1.6

Copyright © 2002- 2026 MULTICERT - All rights reserved.

Certificate Component[3]	Collective Person Representative Effects	Professional Quality	Private Quality	Professional Individual	Private Individual	Electronic Seal	Electronic Seal PSD2
	0.4.0.1862.1.6					0.4.0.1862.1.6	0.4.0.1862.1.6.2
	0.4.0.1862.1.6.1					0.4.0.1862.1.6.2	0.4.0.1862.1.5
	0.4.0.1862.1.5					0.4.0.1862.1.5	Mandatory in Non EU QC. Not present in EU QC. 0.4.0.1862.1.7
	n.a.						0.4.0.19495.2
							Optional 0.4.0.19495.1.1:PSP_AS
							Optional 0.4.0.19495.1.2:PSP_PI
							Optional 0.4.0.19495.1.3:PSP_AI
							Optional 0.4.0.19495.1.4:PSP_IC

Copyright © 2002- 2026 MULTICERT - All rights reserved.

4 Authentication Digital Certificate Profile

Certificate Component[4]	Authentication
Signature Algorithm	
	sha256RSA
Subject Distinguished Name	
Common Name (CN)	Mandatory Option 1: <certificate subscriber name> Option 2: <certificate subscriber professional name>
Serial Number (SERIALNUMBER)	Mandatory Option 1: <identification document type><country>-<identification document nº> Option 2: <See annex A for details of the rules for locally defined identity type reference> Option 3: TIN<country>-<tax number> Option 4: <See line 1 of annex A for details of the rules when the Residence Title is presented>
Title (T)	Optional <quality of the certificate subscriber, as part of its use for a digital certificate>
Organizational Unit (OU)	Optional Certificado para Pessoal Singular – Autenticação
Organizational Unit (OU)	Optional <area/department/specialty of the Organization to which the certificate subscriber belongs>
Organization (O)	Optional

[4] n.a. – not applicable

Copyright © 2002- 2026 MULTICERT - All rights reserved.

Certificate Component[4]	Authentication
	<name of the Organization to which the certificate subscriber belongs, if applicable>
Country (C)	Mandatory <citizenship of the certificate subscriber or country of the entity >
Pseudonym (2.5.4.65)	Optional; but it must be present the pseudonym attribute or the givenName and surname attributes <short name of the certificate subscriber>
GivenName (G)	Optional; but it must be present the pseudonym attribute or the givenName and surname attributes <first name of the certificate subscriber>
Surname (SN)	Optional; but it must be present the pseudonym attribute or the givenName and surname attributes <last name of the certificate subscriber>
emailAddress (E)	Optional <e-mail address of the certificate subscriber>
Public Key	
	RSA (2048 Bits until 2025-12-16) RSA (3072 Bits or 4096 Bits after 2025-12-16)
Subject Alternative Name	
RFC 822 Name (e-mail address)	Optional <e-mail address of the certificate subscriber>
Key Usage	
	Digital Signature (digitalSignature)
Extended Key Usage	
	Client Authentication (1.3.6.1.5.5.7.3.2)

Copyright © 2002- 2026 MULTICERT - All rights reserved.

Certificate Component[4]	Authentication
Certificate Policies	
	OID: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: https://pki.multicert.com
	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.1.3

Copyright © 2002- 2026 MULTICERT - All rights reserved.

5 Services Digital Certificate Profile

Certificate Component[5]	QWAC	QWAC PSD2
Signature Algorithm		
	sha256RSA	sha256RSA
Subject Distinguished Name		
Common Name (CN)	Mandatory <principal domain name>	Mandatory <principal domain name>
Serial Number (SERIALNUMBER)	n.a.	Mandatory <document type><country>-<tax nº>
Organization Identifier (2.5.4.97)	Mandatory <document type><country>-<tax nº>	Mandatory PSD<country>-<NCA code>-<authorization number>
Organization (O)	Mandatory <name of the Organization to which the domain belongs>	Mandatory <name of the Organization to which the domain belongs>
Country (C)	Mandatory <country of the Organization to which the domain belongs>	Mandatory <country of the Organization to which the domain belongs>
Locality (L)	n.a.	Mandatory <locality of the Organization to which the domain belongs>
Business Category	n.a.	Mandatory <business category>
Jurisdiction Country Code	n.a.	Mandatory <country of jurisdiction of the Organization>

[5] n.a. – not applicable

Copyright © 2002- 2026 MULTICERT - All rights reserved.

Certificate Component[5]	QWAC	QWAC PSD2
Public Key		
	RSA (2048 Bits until 2025-12-16) RSA (3072 Bits after 2025-12-16)	RSA (2048 Bits until 2025-12-16) RSA (3072 Bits after 2025-12-16)
Subject Alternative Name		
DNS Name	Mandatory <same domain name present in the Common Name>	Mandatory <same domain name present in the Common Name>
DNS Name	Optional (up to 6 fields) <domain name>	Optional (up to 6 fields) <domain name>
IP Address	n.a.	n.a.
Key Usage		
	Digital Signature (digitalSignature)	Digital Signature (digitalSignature)
	Key Encipherment (keyEncipherment)	Key Encipherment (keyEncipherment)
Extended Key Usage		
	Server Authentication (1.3.6.1.5.5.7.3.1)	Server Authentication (1.3.6.1.5.5.7.3.1)
	Client Authentication (1.3.6.1.5.5.7.3.2)	Client Authentication (1.3.6.1.5.5.7.3.2)
Certificate Policies		
	OID: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: https://pki.multicert.com	OID: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: https://pki.multicert.com
	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.1.15	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.1.12
	OID: 0.4.0.194112.1.4 (until 2025-03-17) OID: 0.4.0.194112.1.6 (after 2025-03-17)	OID: 0.4.0.194112.1.4 (until 2025-03-17) OID: 0.4.0.194112.1.6 (after 2025-03-17)

Copyright © 2002- 2026 MULTICERT - All rights reserved.

Certificate Component[5]	QWAC	QWAC PSD2
QC Statements		
	1.3.6.1.5.5.7.11.2	1.3.6.1.5.5.7.11.2
	0.4.0.1862.1.1	0.4.0.1862.1.1
	0.4.0.1862.1.3:07	0.4.0.1862.1.3:07
	0.4.0.1862.1.6	0.4.0.1862.1.6
	0.4.0.1862.1.6.3	0.4.0.1862.1.6.3
	0.4.0.1862.1.5	0.4.0.1862.1.5
	n.a.	Mandatory in Non EU QC. Not present in EU QC. 0.4.0.1862.1.7
		0.4.0.19495.2
		Optional 0.4.0.19495.1.1:PSP_AS
		Optional 0.4.0.19495.1.2:PSP_PI
		Optional 0.4.0.19495.1.3:PSP_AI
		Optional 0.4.0.19495.1.4:PSP_IC

Copyright © 2002- 2026 MULTICERT - All rights reserved.

6 Advanced Digital Certificate Profile

Certificate Component[6]	Professional Individual	Private Individual
Signature Algorithm		
	sha256RSA	sha256RSA
Subject Distinguished Name		
Common Name (CN)	Mandatory <certificate subscriber name>	Mandatory <certificate subscriber name>
Serial Number (SERIALNUMBER)	Mandatory Option 1: <identification document type><country>-<identification document nº> Option 2: See annex A for details of the rules for locally defined identity type reference	Mandatory Option 1: <identification document type><country>-<identification document nº> Option 2: See annex A for details of the rules for locally defined identity type reference
Title (T)	Optional <quality of the certificate subscriber, as part of its use for a digital certificate>	n.a.
Organizational Unit (OU)	Mandatory Certificado para Pessoa Singular	Mandatory Certificado para Pessoa Singular
Organizational Unit (OU)	Optional <area/department/speciality of the Organization to which the certificate subscriber belongs>	n.a.
Organization (O)	Mandatory <name of the Organization to which the certificate subscriber belongs>	n.a.
Country (C)	Mandatory <citizenship of the certificate subscriber>	Mandatory <citizenship of the certificate subscriber>
Public Key		

[6] n.a. – not applicable

Copyright © 2002- 2026 MULTICERT - All rights reserved.

Certificate Component[6]	Professional Individual	Private Individual
	RSA (2048 Bits until 2025-12-16) RSA (3072 Bits or 4096 Bits after 2025-12-16)	RSA (2048 Bits until 2025-12-16) RSA (3072 Bits or 4096 Bits after 2025-12-16)
Subject Alternative Name		
	Mandatory	Mandatory
RFC 822 Name (e-mail address)	<e-mail address of the certificate subscriber>	<e-mail address of the certificate subscriber>
Key Usage		
	Digital Signature (digitalSignature)	
	Non-Repudiation (nonRepudiation)	
	Key Encipherment (keyEncipherment)	
	Data Encipherment (dataEncipherment)	
	Key Agreement (keyAgreement)	
Extended Key Usage		
	Client Authentication (1.3.6.1.5.5.7.3.2)	
	Email Protection (1.3.6.1.5.5.7.3.4)	
	MS Document Signing (1.3.6.1.4.1.311.3.10.3.12) (after 2026-04-07)	
	Adobe Authentic Document Trust (1.2.840.113583.1.1.5) (after 2026-04-07)	
	Document Signing (1.3.6.1.5.5.7.3.36)	

Copyright © 2002- 2026 MULTICERT - All rights reserved.

Certificate Component[6]	Professional Individual	Private Individual
	(after 2026-04-07)	
Certificate Policies		
	OID: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: https://pki.multicert.com	
	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.7 URI: https://pki.multicert.com	
	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.1.4	

Copyright © 2002- 2026 MULTICERT - All rights reserved.

7 Timestamp Certificate Profile

Certificate Component[7]	Timestamp
Signature Algorithm	
	sha256RSA
Subject Distinguished Name	
Common Name (CN)	Mandatory MULTICERT Qualified Time Stamping Authority
Serial Number (SERIALNUMBER)	Mandatory <sequential number>
Organizational Unit (OU)	Mandatory Time Stamping Services
Organization (O)	Mandatory MULTICERT - Serviços de Certificação Electrónica S.A.
Country (C)	Mandatory PT
Public Key	
	RSA (2048 Bits until 2025-12-16) RSA (3072 Bits after 2025-12-16)
Key Usage	
	Digital Signature (digitalSignature)
	Non-Repudiation (nonRepudiation)

[7] n.a. – not applicable

Copyright © 2002- 2026 MULTICERT - All rights reserved.

Certificate Component[7]	Timestamp
Extended Key Usage	
	Time Stamping (1.3.6.1.5.5.7.3.8)
Certificate Policies	
	OID: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: https://pki.multicert.com
	OID: 1.3.6.1.4.1.25070.1.2.1.0.1 URI: https://pki.multicert.com
	OID: 0.4.0.2023.1.1
QC Statements	
	1.3.6.1.5.5.7.11.2
	0.4.0.1862.1.1
	0.4.0.1862.1.3:13
	0.4.0.19422.1.1

Copyright © 2002- 2026 MULTICERT - All rights reserved.

Annex A

When the serial number attribute follows a locally defined identity type reference, the serial number has the following structure described in sections 5.1.3/5.1.4 of the standard ETSI EN 319 412-1, according to the table below.

When the certificate is a qualified certificate, it is included the OID 1.3.6.1.5.5.7.11.2 with the *uniformResourceIdentifier* https://pki.multicert.com in the QC Statements.

#	Serial Number Structure
1.	TR:PT-<residence title number>
2.	MC:PT-APDCA:<unique number>
3.	CP<professional number>
4.	MC:PT-OA:<professional number>

Copyright © 2002- 2026 MULTICERT - All rights reserved.

Approval

Nuno Ponte (Management Working Group)

Digitally signed by [Assinatura Qualificada] Nuno Miguel Arieiro Rodrigues da Ponte
Date: 2026.04.06 15:25:44 +01'00'

Copyright © 2002- 2026 MULTICERT - All rights reserved.