Lista de Perfis de Certificados

Lista

MULTICERT_PJ.ECRAIZ_428_pt.docx

Nível de Acesso: Público

Versão: 12.0

Data: 18/02/2025

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

Identificador do Documento: MULTICERT_PJ.ECRAIZ_428_pt.docx

Palavras-chave: Perfil ; Certificado

Tipologia Documental: Lista

Título: Lista de Perfis de Certificados

Idioma Original: Português

Idioma de Publicação: Português

Nível de Acesso: Público

Data: 18/02/2025

Versão Atual: 12.0

Digitally signed by
[Assinatura Qualificada]
Nuno Miguel Arieiro
Rodrigues da Ponte
Date: 2025.02.18 18:01:31 Z

Histórico de Versões

Nº de Versão	Data	Detalhes	Autor(es)
1.0	10/09/2018	Criação de lista de certificados	Multicert S.A.
1.1-1.5	29/01/2019	Revisão de certificado de aplicação	Multicert S.A.
2.0	29/01/2019	Nova versão publicada	Multicert S.A.
2.1	30/04/2019	Inclusão de perfis de certificados PSD2	Multicert S.A.
3.0	30/04/2019	Nova versão publicada	Multicert S.A.
3.1	09/12/2019	Revisão	Multicert S.A.
4.0	09/12/2019	Nova versão publicada	Multicert S.A.
4.1	10/12/2020	Revisão	Multicert S.A.
5.0	17/12/2020	Nova versão publicada	Multicert S.A.
5.1	04/01/2021	Revisão do campo KU dos certificados SSL	Multicert S.A.
6.0	04/01/2021	Nova versão publicada	Multicert S.A.
6.1	31/03/2022	Revisão	Multicert S.A.
7.0	31/03/2022	Nova versão publicada	Multicert S.A.
7.1	24/08/2022	Revisão perfis de certificados de serviços	Multicert S.A.
8.0	24/08/2022	Nova versão publicada	Multicert S.A.
8.1	30/06/2023	Revisão geral	Multicert S.A.
9.0	01/07/2023	Aprovação	Multicert S.A.
9.1	14/11/2024	Revisão geral	Multicert S.A.
10.0	14/11/2024	Aprovação	Multicert S.A.
10.1	11/02/2025	Revisão geral	Multicert S.A.
11.0	13/02/2025	Aprovação	Multicert S.A.
11.1	18/02/2025	Adição dos campos chave pública e algoritmo de assinatura	Multicert S.A.
12.0	18/02/2025	Aprovação	Multicert S.A.

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
MULTICERT_PJ.ECRAIZ_426_pt	Política de Certificado Multicert	Multicert S.A.
MULTICERT_PJ.ECRAIZ_427_pt	Declaração de Práticas de Certificação Multicert	Multicert S.A.

Sumário

1 Perfil de Certificado de Entidade de Certificação Raiz

Componente do Certificado[1]	MULTICERT Root Certification Authority 01
Algoritmo de Assinatura	
	sha256RSA
Subject Distinguished Name	
Common Name (CN)	Mandatório
	MULTICERT Root Certification Authority 01
Organization (O)	Mandatório
	MULTICERT - Serviços de Certificação Electrónica S.A.
Country (C)	Mandatório
	PT
Chave Pública	
	RSA (4096 Bits)
Key Usage	
	Key certificate sign
	CRL sign

[1] n.a. – não aplicável

2 Perfil de Certificado de Entidade de Certificação Subordinada

Componente do Certificado[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	Multicert Trust Services Certification Authority 001	Multicert Certification Authority 002
Serviço EU Trusted List	CA/QC	CA/QC	TSA/QTST	CA/PKC	CA/QC	CA/PKC	TSA/QTST	CA/QC (withdraw 14/06/2022)
Algoritmo de Assinatura								
	sha256RSA	sha256RSA	sha256RSA	sha256RSA	sha256RSA	sha256RSA	sha256RSA	sha256RSA
Subject Distinguished Name								
Common Name (CN)	Mandatório	Mandatório	Mandatório	Mandatório	Mandatório	Mandatório	Mandatório	Mandatório
	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	MULTICERT Trust Services Certification Authority 001	MULTICERT Certification Authority 002
Organizational Unit (OU)	Mandatório	Mandatório	Mandatório	Mandatório	Mandatório	Mandatório	Mandatório	Mandatório
	Certification Authority	Certification Authority	Certification Authority	Certification Authority	Certification Authority	Certification Authority	MULTICERT Trust Services Provider	Accredited Certification Authority
Organization (O)	Mandatório	Mandatório	Mandatório	Mandatório	Mandatório	Mandatório	Mandatório	Mandatório
	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.	MULTICERT - Serviços de Certificação Electrónica S.A.	MULTICERT - Serviços de Certificação Electrónica S.A.
Country (C)	Mandatório	Mandatório	Mandatório	Mandatório	Mandatório	Mandatório	Mandatório	Mandatório
	PT	PT	PT	PT	PT	PT	PT	PT
Chave Pública								
	RSA (4096 Bits)	RSA (4096 Bits)	RSA (4096 Bits)	RSA (4096 Bits)	RSA (4096 Bits)	RSA (4096 Bits)	RSA (4096 Bits)	RSA (4096 Bits)

[2] n.a. – não aplicável

Componente do Certificado[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	Multicert Trust Services Certification Authority 001	Multicert Certification Authority 002
Key Usage								
	Key certificate sign	Key certificate sign	Key certificate sign	Key certificate sign	Key certificate sign	Key certificate sign	Key certificate sign	Key certificate sign
	CRL sign	CRL sign	CRL sign	CRL sign	CRL sign	CRL sign	CRL sign	CRL sign
Extended Key Usage								
	Client authentication	Client authentication	Timestamping	Client authentication	n.a	n.a	n.a	n.a
	Secure email	Server authentication	n.a.	Secure email	n.a	n.a	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	OID: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: http://pkiroot.multicert.com/pol/index.html	OID: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: http://pkiroot.multicert.com/pol/index.html
	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	n.a.	n.a.

3 Perfil de Certificado Digital Qualificado

Componente do Certificado[3]	Efeitos de Representação de Pessoa Coletiva	Qualidade Profissional	Qualidade Particular	Individual Profissional	Individual Particular	Selo Eletrónico	Selo Eletrónico PSD2
Algoritmo de Assinatura							
	sha256RSA	sha256RSA	sha256RSA	sha256RSA	sha256RSA	sha256RSA	sha256RSA
Subject Distinguished Name							
Common Name (CN)	Mandatório <nome do titular do certificado>	Mandatório Opção 1: <nome do titular do certificado> Opção 2: <nome profissional do titular>	Mandatório <nome do titular do certificado>	Mandatório <nome do titular do certificado>	Mandatório <nome do titular do certificado>	Mandatório <nome da Organização>	Mandatório <nome da Organização>
Serial Number (SERIALNUMBER)	Mandatório Opção 1: <tipo documento de identificação><país>-<nº de documento de identificação> Opção 2: Quando está presente o OID de QC Statement 1.3.6.1.5.5.7.11.2 com a sintaxe https://pki.multicert.com, o Serial Number segue as regras descritas no Anexo A Opção 3: Quando é apresentado o Título de Residência, o Serial Number segue a	Mandatório Opção 1: <tipo documento de identificação><país>-<nº de documento de identificação ou nº de cartão profissional> Opção 2: Quando está presente o OID de QC Statement 1.3.6.1.5.5.7.11.2 com a sintaxe https://pki.multicert.com, o Serial Number segue as regras descritas no Anexo A Opção 3: Quando é apresentado o Título de Residência, o Serial Number segue a regra descrita na linha 1 do	Mandatório Opção 1: <tipo documento de identificação><país>-<nº de documento de identificação> Opção 2: Quando está presente o OID de QC Statement 1.3.6.1.5.5.7.11.2 com a sintaxe https://pki.multicert.com, o Serial Number segue as regras descritas no Anexo A Opção 3: TIN<país>-<nº fiscal> Opção 4: Quando é apresentado o Título de Residência, o Serial Number segue a regra descrita na linha 1	Mandatório Opção 1: <tipo documento de identificação><país>-<nº de documento de identificação> Opção 2: Quando está presente o OID de QC Statement 1.3.6.1.5.5.7.11.2 com a sintaxe https://pki.multicert.com, o Serial Number segue as regras descritas no Anexo A Opção 3: Quando é apresentado o Título de Residência, o Serial Number segue	Mandatório Opção 1: <tipo documento de identificação><país>-<nº de documento de identificação> Opção 2: Quando está presente o OID de QC Statement 1.3.6.1.5.5.7.11.2 com a sintaxe https://pki.multicert.com, o Serial Number segue as regras descritas no Anexo A Opção 3: Quando é apresentado o Título de Residência, o Serial Number segue a regra descrita na linha 1	n.a.	n.a.

[3] n.a. – não aplicável

Componente do Certificado[3]	Efeitos de Representação de Pessoa Coletiva	Qualidade Profissional	Qualidade Particular	Individual Profissional	Individual Particular	Selo Eletrónico	Selo Eletrónico PSD2
	regra descrita na linha 1 do Anexo A	Anexo A	do Anexo A	a regra descrita na linha 1 do Anexo A	do Anexo A		
Title (T)	Mandatório <qualidade do titular do certificado, no âmbito da sua utilização para assinatura digital qualificada>	Mandatório <qualidade do titular do certificado, no âmbito da sua utilização para assinatura digital qualificada>	Mandatório <qualidade do titular do certificado, no âmbito da sua utilização para assinatura digital qualificada>	n.a.	n.a.	n.a.	n.a.
Organizational Unit (OU)	Opcional; mas tem que estar presente se for um Certificado Qualificado Remoto RemoteQSCDManagement	Opcional; mas tem que estar presente se for um Certificado Qualificado Remoto RemoteQSCDManagement	Opcional; mas tem que estar presente se for um Certificado Qualificado Remoto RemoteQSCDManagement	Opcional; mas tem que estar presente se for um Certificado Qualificado Remoto RemoteQSCDManagement	Opcional; mas tem que estar presente se for um Certificado Qualificado Remoto RemoteQSCDManagement	Opcional; mas tem que estar presente se for um Certificado Qualificado Remoto RemoteQSCDManagement	n.a.
Organizational Unit (OU)	Mandatório Certificado para pessoal singular – Assinatura Qualificada	Mandatório Certificado para pessoal singular – Assinatura Qualificada	Mandatório Certificado para pessoal singular – Assinatura Qualificada	Mandatório Certificado para pessoal singular – Assinatura Qualificada	Mandatório Certificado para pessoal singular – Assinatura Qualificada	Mandatório Qualified Certificate for Eletronic Seal	Mandatório PSD2 Qualified Certificate for Electronic Seal
Organizational Unit (OU)	n.a.	Opcional <área/departamento/especialidade da Organização à qual o titular do certificado pertence>	Opcional; presente se for uma assinatura digital para fatura eletrónica Uso limitado a fatura eletrónica/Limited to electronic invoice	n.a.	n.a.	Opcional; presente se for um selo eletrónico para fatura eletrónica Uso limitado a fatura eletrónica/Limited to electronic invoice	n.a.
Organization Identifier (2.5.4.97)	Mandatório VAT<país>-<nº de identificação fiscal da Organização>	n.a.	n.a.	n.a.	n.a.	Mandatório VAT<país>-<nº de identificação fiscal da Organização>	Mandatório PSD<país>-<código NCA>-<nº autorização>
Organization (O)	Mandatório <nome da Organização à qual o titular pertence)	Mandatório <nome da Organização à qual o titular pertence>	n.a.	Mandatório <nome da Organização à qual o titular pertence>	n.a.	Mandatório <nome da Organização à qual o titular pertence>	Mandatório <nome da Organização à qual o titular pertence>
Country (C)	Mandatório <país de nacionalidade	Mandatório <país de nacionalidade do	Mandatório <país de nacionalidade do titular	Mandatório <país de nacionalidade	Mandatório <país de nacionalidade do	Mandatório <país de	Mandatório <país de

Componente do Certificado[3]	Efeitos de Representação de Pessoa Coletiva	Qualidade Profissional	Qualidade Particular	Individual Profissional	Individual Particular	Selo Eletrónico	Selo Eletrónico PSD2
	do titular do certificado>	titular do certificado>	do certificado>	do titular do certificado>	titular do certificado>	nacionalidade do titular do certificado>	nacionalidade do titular do certificado>
Pseudonym (2.5.4.65)	n.a.	Opcional; mas tem que estar presente o atributo pseudónimo ou os atributos givenName e surname <nome abreviado do titular>	n.a.	n.a.	n.a.	n.a.	n.a.
GivenName (G)	n.a.	Opcional; mas tem que estar presente o atributo pseudónimo ou os atributos givenName e surname <nome próprio do titular do certificado>	Opcional; mas tem que estar presente o atributo pseudónimo ou os atributos givenName e surname <nome próprio do titular do certificado>	Opcional; mas tem que estar presente o atributo pseudónimo ou os atributos givenName e surname <nome próprio do titular do certificado>	Opcional; mas tem que estar presente o atributo pseudónimo ou os atributos givenName e surname <nome próprio do titular do certificado>	n.a.	n.a.
Surname (SN)	n.a.	Opcional; mas tem que estar presente o atributo pseudónimo ou os atributos givenName e surname <apelido do titular do certificado>	Opcional; mas tem que estar presente o atributo pseudónimo ou os atributos givenName e surname <apelido do titular do certificado>	Opcional; mas tem que estar presente o atributo pseudónimo ou os atributos givenName e surname <apelido do titular do certificado>	Opcional; mas tem que estar presente o atributo pseudónimo ou os atributos givenName e surname <apelido do titular do certificado>	n.a.	n.a.
emailAddress (E)	n.a.	n.a.	Opcional <email do titular do certificado>	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.	
Chave Pública							
	RSA (2048 Bits)	RSA (2048 Bits)	RSA (2048 Bits)	RSA (2048 Bits)	RSA (2048 Bits)	RSA (2048 Bits)	RSA (2048 Bits)
Subject Alternative Name							

Componente do Certificado[3]	Efeitos de Representação de Pessoa Coletiva	Qualidade Profissional	Qualidade Particular	Individual Profissional	Individual Particular	Selo Eletrónico	Selo Eletrónico PSD2
RFC 822 Name (e-mail address)	Mandatório	Opcional	Mandatório	Mandatório	Mandatório	Mandatório	n.a.
	<endereço de correio eletrónico do titular do certificado>	<endereço de correio eletrónico do titular do certificado>	<endereço de correio eletrónico do titular do certificado>	<endereço de correio eletrónico do titular do certificado>	<endereço de correio eletrónico do titular do certificado>	<endereço de correio eletrónico do titular do certificado>	
Key Usage							
	Non-repudiation	Non-repudiation	Non-repudiation	Non-repudiation	Non-repudiation	Non-repudiation	Non-repudiation
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: 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
	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	Presente para utilização geral OID: 0.4.0.194112.1.2 Presente se usado para fatura eletrónica OID: 1.3.6.1.4.1.25070.1.1.1.1.0.1.22	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
	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	Presente para utilização geral OID: 1.3.6.1.4.1.25070.1.1.1.1.0.1.14 Presente se usado para fatura eletrónica OID:	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.1.14 (até 18/10/2019) OID: 1.3.6.1.4.1.25070.1.1.1.1.0.1.18 (após 18/10/2019

Componente do Certificado[3]	Efeitos de Representação de Pessoa Coletiva	Qualidade Profissional	Qualidade Particular	Individual Profissional	Individual Particular	Selo Eletrónico	Selo Eletrónico PSD2
						1.3.6.1.4.1.25070.1.1.1.0.1.19	
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
	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	Mandatório se não for um EU QC. Não presente se for um EU QC. 0.4.0.1862.1.7
	n.a.						0.4.0.19495.2
	n.a.						Opcional 0.4.0.19495.1.1:PSP_AS
	n.a.						Opcional 0.4.0.19495.1.2:PSP_PI
	n.a.						Opcional 0.4.0.19495.1.3:PSP_AI
	n.a.						Opcional 0.4.0.19495.1.4:PSP_

Componente do Certificado[3]	Efeitos de Representação de Pessoa Coletiva	Qualidade Profissional	Qualidade Particular	Individual Profissional	Individual Particular	Selo Eletrónico	Selo Eletrónico PSD2
							IC

4 Perfil de Certificado Digital de Autenticação

Componente do Certificado[4]	Autenticação
Algoritmo de Assinatura	
	sha256RSA
Subject Distinguished Name	
Common Name (CN)	Mandatório Opção 1: <nome do titular do certificado> Opção 2: <nome profissional do titular do certificado>
Serial Number (SERIALNUMBER)	Mandatório Opção 1: <tipo documento de identificação><país>-<nº de documento de identificação> Opção 2: Ver anexo A sobre detalhes das regras de referências locais Opção 3: TIN<país>-<nº fiscal> Opção 4: Ver linha 1 do anexo A sobre detalhes das regras quando é apresentado o Título de Residência
Title (T)	Opcional <qualidade do titular do certificado, no âmbito da sua utilização do certificado digital>
Organizational Unit (OU)	Opcional Certificado para pessoal singular – Autenticação
Organizational Unit (OU)	Opcional <área/departamento/especialidade da Organização à qual o titular do certificado pertence>
Organization (O)	Opcional <nome da Organização à qual o titular pertence, se aplicável>

[4] n.a. – não aplicável

Componente do Certificado[4]	Autenticação
Country (C)	Mandatório <país de nacionalidade do titular do certificado>
Pseudonym (2.5.4.65)	Opcional; mas tem que estar presente o atributo pseudónimo ou os atributos givenName e surname <nome abreviado do titular>
GivenName (G)	Opcional; mas tem que estar presente o atributo pseudónimo ou os atributos givenName e surname <nome próprio do titular do certificado>
Surname (SN)	Opcional; mas tem que estar presente o atributo pseudónimo ou os atributos givenName e surname <apelido do titular do certificado>
emailAddress (E)	Opcional <email do titular do certificado>
Chave Pública	
	RSA (2048 Bits)
Subject Alternative Name	
RFC 822 Name (e-mail address)	Opcional <endereço de correio eletrónico do titular do certificado>
Key Usage	
	Digital Signature
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

5 Perfil de Certificado Digital de Serviços

Componente do Certificado[5]	QWAC	QWAC PSD2
Algoritmo de Assinatura		
	sha256RSA	sha256RSA
Subject Distinguished Name		
Common Name (CN)	Mandatório <nome do domínio principal>	Mandatório <nome do domínio principal>
Serial Number (SERIALNUMBER)	n.a.	Mandatório <tipo documento><país>-<nº fiscal>
Organization Identifier (2.5.4.97)	Mandatório <tipo documento><país>-<nº fiscal>	Mandatório PSD<country>-<NCA code>-<authorization number>
Organization (O)	Mandatório <nome da Organização à qual o domínio pertence>	Mandatório <nome da Organização à qual o domínio pertence>
Country (C)	Mandatório <país da Organização à qual o domínio pertence>	Mandatório <país da Organização à qual o domínio pertence>
Locality (L)	n.a.	Mandatório <localidade da Organização à qual o domínio pertence>
Business Category	n.a.	Mandatório <categoria de negócio>
Jurisdiction Country Code	n.a.	Mandatório <país de jurisdição da Organização>
Chave Pública		
	RSA (2048 Bits)	RSA (2048 Bits)

[5] n.a. – não aplicável

Componente do Certificado[5]	QWAC	QWAC PSD2
Subject Alternative Name		
DNS Name	Mandatório <mesmo nome de domínio presente no Common Name>	Mandatório <mesmo nome de domínio presente no Common Name>
DNS Name	Opcional até 6 campos) <nome de domínio>	Opcional até 6 campos) <nome de domínio>
IP Address	n.a.	n.a.
Key Usage		
	Digital Signature	Digital Signature
	Key encipherment	Key encipherment
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 (até 17/03/2025) OID: 0.4.0.194112.1.6 (a partir de 17/03/2025)	OID: 0.4.0.194112.1.4 (até 17/03/2025) OID: 0.4.0.194112.1.6 (a partir de 17/03/2025)
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

Componente do Certificado[5]	QWAC	QWAC PSD2
	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.	Mandatório se não for um EU QC. Não presente se for um EU QC. 0.4.0.1862.1.7
		0.4.0.19495.2
		Opcional 0.4.0.19495.1.1:PSP_AS
		Opcional 0.4.0.19495.1.2:PSP_PI
		Opcional 0.4.0.19495.1.3:PSP_AI
		Opcional 0.4.0.19495.1.4:PSP_IC

6 Perfis de Certificado Digital Avançado

Componente do Certificado[6]	Individual Profissional	Individual Particular
Algoritmo de Assinatura		
	sha256RSA	sha256RSA
Subject Distinguished Name		
Common Name (CN)	Mandatório	Mandatório
	<nome do titular do certificado>	<nome do titular do certificado>
Serial Number (SERIALNUMBER)	Mandatório	Mandatório
	Opção 1: <tipo documento de identificação><país>-<nº de documento de identificação> Opção 2: Ver anexo A sobre detalhes das regras de referências locais	Opção 1: <tipo documento de identificação><país>-<nº de documento de identificação> Opção 2: Ver anexo A sobre detalhes das regras de referências locais
Title (T)	Opcional	n.a.
	<qualidade do titular do certificado, no âmbito da sua utilização para assinatura digital>	
Organizational Unit (OU)	Mandatório	Mandatório
	Certificado para Pessoa Singular	Certificado para Pessoa Singular
Organizational Unit (OU)	Opcional	n.a.
	<área/departamento/especialidade da Organização à qual o titular do certificado pertence>	
Organization (O)	Mandatório	n.a.
	<nome da Organização à qual o titular do certificado pertence>	
Country (C)	Mandatório	Mandatório
	<país de nacionalidade do titular do certificado>	<país de nacionalidade do titular do certificado>

[6] n.a. – não aplicável

Componente do Certificado[6]	Individual Profissional	Individual Particular
Chave Pública		
	RSA (2048 Bits)	RSA (2048 Bits)
Subject Alternative Name		
	Mandatório	Mandatório
RFC 822 Name (e-mail address)	<endereço de correio eletrónico do titular do certificado>	<endereço de correio eletrónico do titular do certificado>
Key Usage		
	Digital Signature	
	Non-repudiation	
	Key encipherment	
	Data encipherment	
	Key agreement	
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	

7 Perfil de Certificado de Selo Temporal

Componente do Certificado[7]	Selo Temporal
Algoritmo de Assinatura	
	sha256RSA
Subject Distinguished Name	
Common Name (CN)	Mandatório MULTICERT Qualified Time Stamping Authority
Serial Number (SERIALNUMBER)	Mandatório <número sequencial>
Organizational Unit (OU)	Mandatório Time Stamping Services
Organization (O)	Mandatório MULTICERT - Serviços de Certificação Electrónica S.A.
Country (C)	Mandatório PT
Chave Pública	
	RSA (2048 Bits)
Key Usage	
	Digital Signature Non-repudiation

[7] n.a. – não aplicável

Componente do Certificado[7]	Selo Temporal
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

Anexo A

Quando o atributo serial number segue um tipo de referência definida localmente, o serial number segue a estrutura descrita nas secções 5.1.3/5.1.4 da norma ETSI EN 319 412-1, de acordo com a tabela abaixo.
Quando o certificado é um certificado qualificado, é incluído o OID 1.3.6.1.5.5.7.11.2 com o *uniformResourceIdentifier* https://pki.multicert.com nos QC Statements.

#	Estrutura do Serial Number
1.	TR:PT-<número do título de residência>
2.	MC:PT-APDCA:<número único>
3.	CP<número profissional>
4.	MC:PT-OA:<número profissional>