

# Lista de Perfis de Certificados

Lista

---

MULTICERT\_PJ.ECRAIZ\_428\_pt.docx

**Nível de Acesso:** Público

**Versão:** 6.0

**Data:** 04/01/2021

**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:** 04/01/2021

**Versão Atual:** 6.0

#### 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.

#### 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

Lista de Perfis de Certificados .....	1
Sumário.....	3
1 Perfil de Certificado Digital Qualificado .....	4
2 Perfil de Certificado Digital de Autenticação .....	9
3 Perfil de Certificado Digital de Aplicação e/ou Serviços .....	11
4 Perfis de Certificado Digital Avançado .....	14

# 1 Perfil de Certificado Digital Qualificado

Componente do Certificado <sup>1</sup>	Efeitos de Representação de Pessoa Coletiva	Qualidade Profissional	Qualidade Particular	Individual Profissional	Individual Particular	Selo Eletrónico	Selo Eletrónico PSD2
<b>Subject Distinguished Name</b>							
Common Name (CN)	Mandatório <nome do titular do certificado>	Mandatório <nome do titular do certificado>	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	Mandatório	Opcional; Apenas não é utilizado no âmbito da ERAR	Mandatório	Mandatório	n.a.	n.a.
	<p>Opção 1: &lt;tipo documento de identificação&gt;&lt;país&gt;-&lt;nº de documento de identificação&gt;</p> <p>Opção 2: Quando está presente o OID de QC Statement 1.3.6.1.5.5.7.11.2 com a sintaxe <a href="https://pki.multicert.com">https://pki.multicert.com</a>, o Serial Number segue as regras descritas no Anexo A</p>	<p>Opção 1: &lt;tipo documento de identificação&gt;&lt;país&gt;-&lt;nº de documento de identificação ou nº de cartão profissional&gt;</p> <p>Opção 2: Quando está presente o OID de QC Statement 1.3.6.1.5.5.7.11.2 com a sintaxe <a href="https://pki.multicert.com">https://pki.multicert.com</a>, o Serial Number segue as regras descritas no Anexo A</p>	<p>Opção 1: &lt;tipo documento de identificação&gt;&lt;país&gt;-&lt;nº de documento de identificação&gt;</p> <p>Opção 2: Quando está presente o OID de QC Statement 1.3.6.1.5.5.7.11.2 com a sintaxe <a href="https://pki.multicert.com">https://pki.multicert.com</a>, o Serial Number segue as regras descritas no Anexo A</p>	<p>Opção 1: &lt;tipo documento de identificação&gt;&lt;país&gt;-&lt;nº de documento de identificação&gt;</p> <p>Opção 2: Quando está presente o OID de QC Statement 1.3.6.1.5.5.7.11.2 com a sintaxe <a href="https://pki.multicert.com">https://pki.multicert.com</a>, o Serial Number segue as regras descritas no Anexo A</p>	<p>Opção 1: &lt;tipo documento de identificação&gt;&lt;país&gt;-&lt;nº de documento de identificação&gt;</p> <p>Opção 2: Quando está presente o OID de QC Statement 1.3.6.1.5.5.7.11.2 com a sintaxe <a href="https://pki.multicert.com">https://pki.multicert.com</a>, o Serial Number segue as regras descritas no Anexo A</p> <p>Opção 3: TIN&lt;país&gt;-&lt;nº fiscal&gt;</p>		
Title (T)	Mandatório <qualidade do titular do certificado, no âmbito da sua utilização para	Mandatório <qualidade do titular do certificado, no âmbito da sua utilização para	Mandatório <qualidade do titular do certificado, no âmbito da sua utilização para assinatura digital	n.a.	n.a.	n.a.	n.a.

<sup>1</sup> n.a. – não aplicável

Componente do Certificado <sup>1</sup>	Efeitos de Representação de Pessoa Coletiva	Qualidade Profissional	Qualidade Particular	Individual Profissional	Individual Particular	Selo Eletrónico	Selo Eletrónico PSD2
	assinatura digital qualificada>	assinatura digital qualificada>	qualificada>				
Organizational Unit (OU)	Opcional; mas tem que estar presente se for um Certificado Qualificado Remoto	Opcional; mas tem que estar presente se for um Certificado Qualificado Remoto	Opcional; mas tem que estar presente se for um Certificado Qualificado Remoto	Opcional; mas tem que estar presente se for um Certificado Qualificado Remoto	Opcional; mas tem que estar presente se for um Certificado Qualificado Remoto	Opcional; mas tem que estar presente se for um Certificado Qualificado Remoto	n.a.
	RemoteQSCDManagement	RemoteQSCDManagement	RemoteQSCDManagement	RemoteQSCDManagement	RemoteQSCDManagement	RemoteQSCDManagement	
Organizational Unit (OU)	Mandatário	Mandatário	Opcional	Mandatário	Mandatário	Mandatário	Mandatário
	Certificado para Pessoal Singular – Assinatura Qualificada	Certificado para Pessoal Singular – Assinatura Qualificada	Certificado para Pessoal Singular – Assinatura Qualificada	Certificado para Pessoal Singular – Assinatura Qualificada	Certificado para Pessoal Singular – Assinatura Qualificada	Qualified Certificate for Electronic Seal	PSD2 Qualified Certificate for Electronic Seal
Organizational Unit (OU)	n.a.	Opcional	Opcional	n.a.	n.a.	Opcional; presente se for um selo eletrónico para fatura eletrónica	n.a.
		<área/departamento/especialidade da Organização à qual o titular do certificado pertence>	<área/departamento/especialidade da Organização à qual o titular do certificado pertence>			Uso limitado a fatura eletrónica/Limited to electronic invoice	
Organization Identifier (2.5.4.97)	Mandatário	n.a.	n.a.	n.a.	n.a.	Mandatário	Mandatário
	VAT<país>-<nº de identificação fiscal da Organização>					VAT<país>-<nº de identificação fiscal da Organização>	PSD<país>-<código NCA>-<nº autorização>
Organization (O)	Mandatário	Mandatário	n.a.	Mandatário	n.a.	Mandatário	Mandatário
	<nome da Organização à qual o titular pertence>	<nome da Organização à qual o titular pertence>		<nome da Organização à qual o titular pertence>		<nome da Organização à qual o titular pertence>	
Country (C)	Mandatário	Mandatário	Mandatário	Mandatário	Mandatário	Mandatário	Mandatário
	<país de nacionalidade do titular do certificado>	<país de nacionalidade do titular do certificado>	<país de nacionalidade do titular do certificado>	<país de nacionalidade do titular do certificado>	<país de nacionalidade do titular do certificado>	<país de nacionalidade do titular do certificado>	<país de nacionalidade do titular do certificado>
Pseudonym (2.5.4.65)	n.a.	Opcional; mas tem que estar presente o atributo pseudónimo ou os atributos	n.a.	n.a.	n.a.	n.a.	n.a.

Componente do Certificado <sup>1</sup>	Efeitos de Representação de Pessoa Coletiva	Qualidade Profissional	Qualidade Particular	Individual Profissional	Individual Particular	Selo Eletrónico	Selo Eletrónico PSD2
		givenName e surname <nome abreviado do titular>					
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.	Opcional <email do titular do certificado>	n.a.	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.	
<b>Subject Alternative Name</b>							
RFC 822 Name (e-mail address)	Mandatário <endereço de correio eletrónico do titular do certificado>	Mandatário <endereço de correio eletrónico do titular do certificado>	Mandatário <endereço de correio eletrónico do titular do certificado>	Mandatário <endereço de correio eletrónico do titular do certificado>	Mandatário <endereço de correio eletrónico do titular do certificado>	Mandatário <endereço de correio eletrónico do titular do certificado>	n.a.
<b>Key Usage</b>							

Componente do Certificado <sup>1</sup>	Efeitos de Representação de Pessoa Coletiva	Qualidade Profissional	Qualidade Particular	Individual Profissional	Individual Particular	Selo Eletrónico	Selo Eletrónico PSD2
	Non-repudiation	Non-repudiation	Non-repudiation	Non-repudiation	Non-repudiation	Non-repudiation	Non-repudiation
<b>Certificate Policies</b>							
	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: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: https://pki.multicert.com	OID: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: https://pki.multicert.com
	OID: 0.4.0.194112.1.2	OID: 0.4.0.194112.1.2	OID: 0.4.0.194112.1.2	OID: 0.4.0.194112.1.2	OID: 0.4.0.194112.1.2	OID: 0.4.0.194112.1.3	OID: 0.4.0.194112.1.1
	OID: 1.3.6.1.4.1.25070.1.1.1.0.1.2	OID: 1.3.6.1.4.1.25070.1.1.1.0.1.2	OID: 1.3.6.1.4.1.25070.1.1.1.0.1.2	OID: 1.3.6.1.4.1.25070.1.1.1.0.1.2	OID: 1.3.6.1.4.1.25070.1.1.1.0.1.2	Presente para utilização geral OID: 1.3.6.1.4.1.25070.1.1.1.0.1.14  Presente se usado para fatura eletrónica OID: 1.3.6.1.4.1.25070.1.1.1.0.1.19	OID: 1.3.6.1.4.1.25070.1.1.1.0.1.14 (até 18/10/2019)  OID: 1.3.6.1.4.1.25070.1.1.1.0.1.18 (após 18/10/2019)
<b>QC Statements</b>							
	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

Componente do Certificado <sup>1</sup>	Efeitos de Representação de Pessoa Coletiva	Qualidade Profissional	Qualidade Particular	Individual Profissional	Individual Particular	Selo Eletrónico	Selo Eletrónico PSD2
			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	Mandatário 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_IC



## 2 Perfil de Certificado Digital de Autenticação

Componente do Certificado <sup>2</sup>	Autenticação
<b>Subject Distinguished Name</b>	
Common Name (CN)	Mandatário ----- <nome do titular do certificado>
Serial Number (SERIALNUMBER)	Mandatário ----- 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 ----- <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>
Country (C)	Mandatário ----- <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>

<sup>2</sup> n.a. – não aplicável

Componente do Certificado <sup>2</sup>	Autenticação
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>
<b>Subject Alternative Name</b>	
RFC 822 Name (e-mail address)	Opcional ----- <endereço de correio eletrónico do titular do certificado>
MS UPN, User Principal Name	Opcional ----- <endereço de correio eletrónico do titular do certificado>
<b>Key Usage</b>	
	Digital Signature
<b>Certificate Policies</b>	
	----- OID: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: https://pki.multicert.com ----- OID: 1.3.6.1.4.1.25070.1.1.1.0.1.3

## 3 Perfil de Certificado Digital de Aplicação e/ou Serviços

Componente do Certificado <sup>3</sup>	TLS/SSL OV / Wildcard	TLS/SSL QWAC PSD2
<b>Subject Distinguished Name</b>		
Common Name (CN)	Mandatório ----- <nome do domínio principal/Endereço IP>	Mandatório ----- <nome do domínio principal>
Serial Number (SERIALNUMBER)	n.a.	Mandatory ----- <tipo documento><país>-<nº fiscal>
Organizational Unit (OU)	Mandatório ----- Website Authentication Certificate	Mandatório ----- PSD2 Qualified Website Authentication
Organizational Unit (OU)	Opcional	n.a.
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)	Mandatório ----- <localidade da Organização à qual o domínio pertence>	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>
<b>Subject Alternative Name</b>		

<sup>3</sup> n.a. – não aplicável

Componente do Certificado <sup>3</sup>	TLS/SSL OV / Wildcard	TLS/SSL QWAC PSD2
DNS Name	Mandatório se estiver presente um nome de domínio no CN <mesmo nome de domínio presente no Common Name>	Mandatório <mesmo nome de domínio presente no Common Name>
DNS Name	Opcional (até 99 campos) <nome de domínio>	Opcional até 6 campos <nome de domínio>
IP Address	Mandatório se estiver presente um endereço IP no CN <mesmo endereço IP presente no Common Name >	n.a.
IP Address	Opcional (até 7 campos) <endereço IP>	n.a.
<b>Key Usage</b>		
	Digital Signature	Digital Signature
	Key encipherment	Key encipherment
	Data encipherment (presente até 01/01/2021, ausente a partir dessa data)	Data encipherment (presente até 01/01/2021, ausente a partir dessa data)
<b>Certificate Policies</b>		
	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: 1.3.6.1.4.1.25070.1.1.1.0.1.17	OID: 1.3.6.1.4.1.25070.1.1.1.0.1.12
	OID: 2.23.140.1.2.2	OID: 0.4.0.194112.1.4
	OID: 0.4.0.2042.1.7	n.a.
<b>QC Statements</b>		
	n.a.	1.3.6.1.5.5.7.11.2

Componente do Certificado <sup>3</sup>	TLS/SSL OV / Wildcard	TLS/SSL QWAC PSD2
	n.a.	0.4.0.1862.1.1
	n.a.	0.4.0.1862.1.3:07
	n.a.	0.4.0.1862.1.6
	n.a.	0.4.0.1862.1.6.3
	n.a.	0.4.0.1862.1.5
	n.a.	Mantório 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_IC

## 4 Perfis de Certificado Digital Avançado

Componente do Certificado <sup>4</sup>	Individual Profissional	Individual Particular
<b>Subject Distinguished Name</b>		
Common Name (CN)	Mandatório ----- <nome do titular do certificado>	Mandatório ----- <nome 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	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
Title (T)	Opcional ----- <qualidade do titular do certificado, no âmbito da sua utilização para assinatura digital>	n.a.
Organizational Unit (OU)	Mandatório ----- Certificado para Pessoa Singular	Mandatório ----- Certificado para Pessoa Singular
Organizational Unit (OU)	Opcional ----- <área/departamento/especialidade da Organização à qual o titular do certificado pertence>	n.a.
Organization (O)	Mandatório ----- <nome da Organização à qual o titular do certificado pertence>	n.a.
Country (C)	Mandatório ----- <país de nacionalidade do titular do certificado>	Mandatório ----- <país de nacionalidade do titular do certificado>
<b>Subject Alternative Name</b>		
	Mandatório	Mandatório

<sup>4</sup> n.a. – não aplicável

Componente do Certificado <sup>4</sup>	Individual Profissional	Individual Particular
RFC 822 Name (e-mail address)	<endereço de correio eletrônico do titular do certificado>	<endereço de correio eletrônico do titular do certificado>
<b>Key Usage</b>		
	Digital Signature	Digital Signature
	Non-repudiation	Non-repudiation
	Key encipherment	Key encipherment
	Data encipherment	Data encipherment
	Key agreement	Key agreement
<b>Certificate Policies</b>		
	OID: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: <a href="https://pki.multicert.com">https://pki.multicert.com</a>	
	OID: 1.3.6.1.4.1.25070.1.1.1.0.7 URI: <a href="https://pki.multicert.com">https://pki.multicert.com</a>	
	OID: 1.3.6.1.4.1.25070.1.1.1.0.1.4	

## Anexo A

Quando o atributo serial number segue um tipo de referência definida localmente, o serial number segue a estrutura descrita na 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
MC:PT-OM<número único>
MC:PT-AR<número único>
MJ:PT-<número único>
MC:PT-ON<número único>
MC:PT-OA<número único>
MC:PT-IGCP<número único>
MC:PT-AP<número único>
MC:PT-AC<número único>
MC:PT-AL<número único>
MC:PT-AE<número único>
MC:PT-AX<número único>
MC:PT-AR<número único>
MC:PT-AS<número único>