multicert

Engineering for digital security

Certificate Profiles List

List

MULTICERT_PJ.ECRAIZ_428_en

Rating: Public

Version: 8.0

Date: 24/08/2022

Normative Version

MULTICERT, Serviços de Certificação Electrónica, S.A.,
Lagoas Park, Edifício 3, Piso 3 – 2740-266 Porto Salvo - Oeiras
Telephone: +351 217 123 010 Facsimile: +351 217 123 011

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: 24/08/2022

Current Version: 8.0

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.

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.

Summary

1 Qualified Digital Certificate Profile

Certificate Component[1]	Collective Person Representative Effects	Professional Quality	Private Quality	Professional Individual	Private Individual	Electronic Seal	Electronic Seal PSD2
Subject Distinguished Name							
Common Name (CN)	Mandatory <certificate subscriber name>	Mandatory <certificate subscriber 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	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	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	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	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>	n.a.	n.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	Optional; but it must be present if it is a Qualified Remote Signing Certificate	Optional; but it must be present if it is a Qualified Remote Signing Certificate	Optional; but it must be present if it is a Qualified Remote Signing	Optional; but it must be present if it is a Qualified Remote Signing Certificate	Optional; but it must be present if it is a Qualified Remote	n.a.

[1] n.a. – not applicable

Certificate Component[1]	Collective Person Representative Effects	Professional Quality	Private Quality	Professional Individual	Private Individual	Electronic Seal	Electronic Seal PSD2
	Certificate			Certificate		Signing Certificate	
	RemoteQSCDManagement	RemoteQSCDManagement	RemoteQSCDManagement	RemoteQSCDManagement	RemoteQSCDManagement	RemoteQSCDManagement	
Organizational Unit (OU)	Mandatory	Mandatory	Optional	Mandatory	Mandatory	Mandatory	Mandatory
	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.	Optional	Optional	n.a.	Optional; but present if it is an digital signature for electronic invoice	Optional; but present if it is an electronic seal for electronic invoice	n.a.
		<area/department/specialty of the Organization to which the certificate subscriber belongs>	<area/department/specialty of the Organization to which the certificate subscriber belongs>		Uso limitado a fatura eletrónica/Limited to electronic invoice	Uso limitado a fatura eletrónica/Limited to electronic invoice	
Organization Identifier (2.5.4.97)	Mandatory	n.a.	n.a.	n.a.	n.a.	Mandatory	Mandatory
	VAT<country>-<tax number of the Organization>					VAT<country>-<tax number of the Organization>	PSD<country>-<NCA code>-<authorization number>
Organization (O)	Mandatory	Mandatory	n.a.	Mandatory	n.a.	Mandatory	Mandatory
	<name of the Organization to which the certificate subscriber belongs>	<name of the Organization to which the certificate subscriber belongs>		<name of the Organization to which the certificate subscriber belongs>		<name of the Organization>	<name of the Organization>
Country (C)	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
	<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>	<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	n.a.	n.a.	n.a.	n.a.	n.a.
		<short name of the certificate subscriber>					
GivenName (G)	n.a.	Optional; but it must be present the pseudonym attribute or the givenName	Optional; but it must be present the pseudonym attribute or the givenName	Optional; but it must be present the pseudonym attribute or the	Optional; but it must be present the pseudonym attribute or the givenName	n.a.	n.a.

Certificate Component[1]	Collective Person Representative Effects	Professional Quality	Private Quality	Professional Individual	Private Individual	Electronic Seal	Electronic Seal PSD2
		and surname attributes	and surname attributes	givenName and surname attributes	and surname attributes		
		<first name of the certificate subscriber>	<first name of the certificate subscriber>	<first name of the certificate subscriber>	<first name of the certificate subscriber>		
Surname (SN)	n.a.	Optional; but it must be present the pseudonym attribute or the givenName and surname attributes	Optional; but it must be present the pseudonym attribute or the givenName and surname attributes	Optional; but it must be present the pseudonym attribute or the givenName and surname attributes	Optional; but it must be present the pseudonym attribute or the givenName and surname attributes	n.a.	n.a.
		<last name of the certificate subscriber>	<last name of the certificate subscriber>	<last name of the certificate subscriber>	<last name of the certificate subscriber>		
emailAddress (E)	n.a.	Optional	n.a.	n.a.	n.a.	n.a.	n.a.
		<email address of the certificate subscriber>					
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.
Subject Alternative Name							
RFC 822 Name (e-mail address)	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory	n.a.
	<email address of the certificate subscriber>	<email address of the certificate subscriber>	<email address of the certificate subscriber>	<email address of the certificate subscriber>	<email address of the certificate subscriber>	<email address of the certificate subscriber>	
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	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

Certificate Component[1]	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	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: 0.4.0.194112.1.3	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 18/10/2019)
						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 18/10/2019
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

Certificate Component[1]	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
	n.a.						Optional 0.4.0.19495.1.1:PSP_AS
	n.a.						Optional 0.4.0.19495.1.2:PSP_PI
	n.a.						Optional 0.4.0.19495.1.3:PSP_AI
	n.a.						Optional 0.4.0.19495.1.4:PSP_IC

2 Authentication Digital Certificate Profile

Certificate Component[2]	Authentication
Subject Distinguished Name	
Common Name (CN)	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> Option 3: TIN<country>-<tax number>
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 <name of the Organization to which the certificate subscriber belongs, if applicable>
Country (C)	Mandatory <citizenship of the certificate subscriber>
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>

[2] n.a. – not applicable

Certificate Component[2]	Authentication
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>
Subject Alternative Name	
RFC 822 Name (e-mail address)	Optional <e-mail address of the certificate subscriber>
MS UPN, User Principal Name	Optional <e-mail address of the certificate subscriber>
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

3 Services Digital Certificate Profile

Certificate Component[3]	TLS/SSL OV / Wildcard	TLS/SSL QWAC PSD2
Subject Distinguished Name		
Common Name (CN)	Mandatory <principal domain name/IP address>	Mandatory <principal domain name>
Serial Number (SERIALNUMBER)	n.a.	Mandatory <document type><country>-<tax nº>
Organization Identifier (2.5.4.97)	n.a.	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)	Mandatory <locality of the Organization to which the domain belongs>	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>
Subject Alternative Name		
DNS Name	Mandatory if a domain name is present in CN <same domain name present in the Common Name>	Mandatory <same domain name present in the Common Name>
DNS Name	Optional (up to 99 fields) <domain name>	Optional (up to 6 fields) <domain name>

[3] n.a. – not applicable

Certificate Component[3]	TLS/SSL OV / Wildcard	TLS/SSL QWAC PSD2
IP Address	Mandatory if a IP address is present in CN <same IP address present in the Common Name>	n.a.
IP Address	Optional (until 7 fields) <IP address>	n.a.
Key Usage		
	Digital Signature	Digital Signature
	Key encipherment	Key encipherment
	Data encipherment (present until 01/01/2021, absent after that date)	Data encipherment (present until 01/01/2021, absent after that date)
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: 1.3.6.1.4.1.25070.1.1.1.1.0.1.17	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.1.12
	OID: 2.23.140.1.2.2	OID: 0.4.0.194112.1.4
	OID: 0.4.0.2042.1.7	n.a.
QC Statements		
	n.a.	1.3.6.1.5.5.7.11.2
	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

Certificate Component[3]	TLS/SSL OV / Wildcard	TLS/SSL QWAC PSD2
	n.a.	0.4.0.1862.1.6.3
	n.a.	0.4.0.1862.1.5
	n.a.	Mandatory in Non EU QC. Not present in EU QC. 0.4.0.1862.1.7
	n.a.	0.4.0.19495.2
	n.a.	Optional 0.4.0.19495.1.1:PSP_AS
	n.a.	Optional 0.4.0.19495.1.2:PSP_PI
	n.a.	Optional 0.4.0.19495.1.3:PSP_AI
	n.a.	Optional 0.4.0.19495.1.4:PSP_IC

4 Advanced Digital Certificate Profile

Certificate Component[4]	Professional Individual	Private Individual
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>
Subject Alternative Name		
	Mandatory	Mandatory

[4] n.a. – not applicable

Certificate Component[4]	Professional Individual	Private Individual
RFC 822 Name (e-mail address)	<e-mail address of the certificate subscriber>	<e-mail address of the certificate subscriber>
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	

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.

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.