multicert

Engineering for digital security

Certificate Profiles List

List

MULTICERT_PJ.ECRAIZ_428_en

Rating: Public

Version: 1.0

Date: 12/09/2018

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: 12/09/2018

Current Version: 1.0

Version History

Version Nº	Date	Details	Author(s)
1.0	10/09/2018	Certificate profiles list creation	MULTICERT S.A.

Related Documents

Document ID	Details	Author(s)
MULTICERT_PJ.ECRAIZ_426_en.pdf	Multicert Certificate Policy	MULTICERT S.A.
MULTICERT_PJ.ECRAIZ_427_en.pdf	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
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>
Serial Number (SERIALNUMBER)	Mandatory <identification document type><country>-<identification document nº>	Mandatory <identification document type><country>-<identification document nº> <In the EROF and EROM scope: CP<professional card nº>	Optional; Is not used in the ERAR scope <identification document type><country>-<identification document nº>	Mandatory <identification document type><country>-<identification document nº>	Mandatory <identification document type><country>-<identification document nº>	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> <In the EROF scope: "Farmacêutico"> <In the EROM scope: "Médico">	Mandatory <quality of the certificate subscriber, as part of its use for a qualified digital signature> <In the ERAR scope: < quality of the certificate subscriber, as part of its use for a qualified digital signature>	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
Organizational Unit (OU)	Mandatory Certificado para Pessoal	Mandatory Certificado para Pessoal Singular	Optional; Is not used in the ERAR scope Certificado para Pessoal Singular –	Mandatory Certificado para Pessoal	Mandatory Certificado para Pessoal	Mandatory Qualified Certificate for

[1] n.a. – non aplicable

Certificate Component[1]	Collective Person Representative Effects	Professional Quality	Private Quality	Professional Individual	Private Individual	Electronic Seal
	Singular – Assinatura Qualificada	– Assinatura Qualificada	Assinatura Qualificada	Singular – Assinatura Qualificada	Singular – Assinatura Qualificada	Eletronic Seal
Organizational Unit (OU)	n.a.	Optional <area/department/speciality of the Organization to which the certificate subscriber belongs>	Optional; Only used in the ERAR scope <area/department/speciality of the Organization to which the certificate subscriber belongs>	n.a.	n.a.	Opcional <área/departamento da Organização>
Organization Identifier (2.5.4.97)	Mandatory <tax number of the Organization>	n.a.	n.a.	n.a.	n.a.	Mandatory <tax number of the Organization>
Organization (O)	Mandatory <name of the Organization to which the certificate subscriber belongs>	Mandatory <name of the Organization to which the certificate subscriber belongs> <In the EROF scope: “Ordem dos Farmacêuticos”> <In the EROM scope: “Ordem dos Médicos”>	Mandatory <name of the Organization to which the certificate subscriber belongs> <In the ERAR scope: “Assembleia da República">	Mandatory <name of the Organization to which the certificate subscriber belongs>	n.a.	Mandatory <name of the Organization to which the certificate subscriber belongs>
Country (C)	Mandatory <citizenship of the certificate subscriber>	Mandatory <citizenship of the certificate subscriber> <In the EROF and EROM scope: “PT”>	Mandatory <citizenship of the certificate subscriber> <In the ERAR scope: “PT”>	Mandatory <citizenship of the certificate subscriber>	Mandatory <citizenship of the certificate subscriber>	Mandatory <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; Only used in the EROM and EROF scope <short name of the certificate subscriber>	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; Is not used in the ERAR scope <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.
Surname (SN)	n.a.	Optional; but it must be present	Optional; but it must be present the	Optional; but it must be	Optional; but it must be	n.a.

Certificate Component[1]	Collective Person Representative Effects	Professional Quality	Private Quality	Professional Individual	Private Individual	Electronic Seal
		the pseudonym attribute or the givenName and surname attributes	pseudonym attribute or the givenName and surname attributes; Is not used in the ERAR scope	present the pseudonym attribute or the givenName and surname attributes	present the pseudonym attribute or the givenName and surname attributes	
		<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; Only used in the ERAR scope	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.	Optional
						<locality>
State or Province (ST)	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
	<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						
	Extension marked as critical	Extension marked as critical	Extension marked as critical	Extension marked as critical	Extension marked as critical	Extension marked as critical
	Non-repudiation	Non-repudiation	Non-repudiation <In the ERAR scope: Digital Signature>	Non-repudiation	Non-repudiation	Non-repudiation
Certificate Policies						
	Extension marked as non-critical	Extension marked as non-critical	Extension marked as non-critical	Extension marked as non-critical	Extension marked as non-critical	Extension marked as non-critical
	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.7	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.7 URI: http://pki.multicert.com	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.7 URI: http://pki.multicert.com	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.7 URI: http://pki.multicert.com	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.7	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.7

Certificate Component[1]	Collective Person Representative Effects	Professional Quality	Private Quality	Professional Individual	Private Individual	Electronic Seal
	URI: http://pki.multicert.com				URI: http://pki.multicert.com	URI: http://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: 0.4.0.2042.1.2	OID: 0.4.0.2042.1.2	OID: 0.4.0.2042.1.2	OID: 0.4.0.2042.1.2	OID: 0.4.0.2042.1.2	OID: 0.4.0.2042.1.2
Basic Constraints						
	Extension marked as critical	Extension marked as critical	Extension marked as critical	Extension marked as critical	Extension marked as critical	Extension marked as critical
Authority Key Identifier						
	Extension marked as non-critical	Extension marked as non-critical	Extension marked as non-critical	Extension marked as non-critical	Extension marked as non-critical	Extension marked as non-critical
Subject Key Identifier						
	Extension marked as non-critical	Extension marked as non-critical	Extension marked as non-critical	Extension marked as non-critical	Extension marked as non-critical	Extension marked as non-critical

2 Authentication Digital Certificate Profile

Certificate Component[2]	Authentication
Subject Distinguished Name	
Common Name (CN)	Mandatory <certificate subscriber name>
Serial Number (SERIALNUMBER)	Mandatory <identification document type><country>-<identification document nº> <In the EROF and EROM scope: CP<professional card nº>>
Title (T)	Optional <quality of the certificate subscriber, as part of its use for a digital certificate> <In the EROF scope: “Farmacêutico”> <In the EROM scope: “Médico”> <In the ERAR scope: <quality of the certificate subscriber, as part of its use for a digital certificate>>
Organizational Unit (OU)	Optional; Is not used in the ERAR scope Certificado para Pessoal Singular – Autenticação
Organizational Unit (OU)	Optional <area/department/speciality of the Organization to which the certificate subscriber belongs>
Organization (O)	Optional <name of the Organization to which the certificate subscriber belongs> <In the EROF scope: “Ordem dos Farmacêuticos”> <In the EROM scope: “Ordem dos Médicos”> <In the ERAR scope: “Assembleia da República">
Country (C)	Mandatory <citizenship of the certificate subscriber> <In the EROF and EROM scope: “PT”> <In the ERAR scope: “PT”>
Pseudonym (2.5.4.65)	Optional; but it must be present the pseudonym attribute or the givenName and surname attributes; Only used in the EROM and EROF scope

[2] n.a. – non aplicable

Certificate Component[2]	Authentication
	<short name of the certificate subscriber>
GivenName (G)	Optional; but it must be present the pseudonym attribute or the givenName and surname attributes; Is not used in the ERAR scope
	<first name of the certificate subscriber>
Surname (SN)	Optional; but it must be present the pseudonym attribute or the givenName and surname attributes; Is not used in the ERAR scope
	<last name of the certificate subscriber>
emailAddress (E)	Optional; Only used in the ERAR scope
	<e-mail address of the certificate subscriber>
Subject Alternative Name	
RFC 822 Name (e-mail address)	Optional; Only used in the ERIGFEJ scope
	<e-mail address of the certificate subscriber>
MS UPN, User Principal Name	<e-mail address of the certificate subscriber>
Key Usage	
	Extension marked as critical
	Digital Signature
Certificate Policies	
	Extension marked as non-critical
	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.7 URI: http://pki.multicert.com
Basic Constraints	
	Extension marked as critical

Certificate Component[2]	Authentication
Authority Key Identifier	
	Extension marked as non-critical
Subject Key Identifier	
	Extension marked as non-critical

3 Application and/or Services Digital Certificate Profile

Certificate Component[3]	TLS/SSL OV	TLS/SSL QWAC	Application	Electronic Invoice
Subject Distinguished Name				
Common Name (CN)	Mandatory <principal domain name>	Mandatory <principal domain name>	Mandatory <Organization name>	Mandatory <name to be certified: Electronic Invoice, Organization name, other>
Serial Number (SERIALNUMBER)	n.a.	n.a.	Mandatory <document type><country>-<tax nº>	Mandatory <document type><country>-<tax nº>
Organizational Unit (OU)	Mandatory Certificado SSL/TLS	Mandatory Certificado SSL/TLS	Mandatory Certificado para Aplicação	Mandatory Certificado para Aplicação
Organizational Unit (OU)	n.a.	n.a.	Optional <department/area/Organization name>	n.a.
Organizational Unit (OU)	n.a.	n.a.	n.a.	n.a.
Organization (O)	Mandatory <name of the Organization to which the domain belongs>	Mandatory <name of the Organization to which the domain belongs>	Mandatory <Organization name>	Mandatory <Organization name>
Country (C)	Mandatory <country of the Organization to which the domain belongs>	Mandatory <country of the Organization to which the domain belongs>	Mandatory <country of the Organization to which the application belongs>	Mandatory <Organization country>
Locality (L)	Mandatory <locality of the Organization to which the domain belongs>	Mandatory <locality of the Organization to which the domain belongs>	n.a.	n.a.
Subject Alternative Name				

[3] n.a. – non aplicable

Certificate Component[3]	TLS/SSL OV	TLS/SSL QWAC	Application	Electronic Invoice
	Optional	Optional	Optional	Mandatory
IP Address	<IP address>	<IP address>	n.a.	n.a.
IP Address	<IP address>	<IP address>	n.a.	n.a.
IP Address	<IP address>	<IP address>	n.a.	n.a.
IP Address	<IP address>	<IP address>	n.a.	n.a.
IP Address	<IP address>	<IP address>	n.a.	n.a.
IP Address	<IP address>	<IP address>	n.a.	n.a.
IP Address	<IP address>	<IP address>	n.a.	n.a.
DNS Name	<domain name>	<domain name>	n.a.	n.a.
DNS Name	<domain name>	<domain name>	n.a.	n.a.
DNS Name	<domain name>	<domain name>	n.a.	n.a.
DNS Name	<domain name>	<domain name>	n.a.	n.a.
DNS Name	<domain name>	<domain name>	n.a.	n.a.
DNS Name	<domain name>	<domain name>	n.a.	n.a.
DNS Name	<domain name>	<domain name>	n.a.	n.a.
RFC 822 Name (e-mail address)	n.a.	n.a.	<e-mail address>	<e-mail address>

Certificate Component[3]	TLS/SSL OV	TLS/SSL QWAC	Application	Electronic Invoice
Key Usage				
	Extension marked as critical	Extension marked as critical	Extension marked as critical	Extension marked as critical
	Digital Signature	Digital Signature	Digital Signature	Digital Signature
	Non-repudiation	Non-repudiation	Non-repudiation	Non-repudiation
	n.a.	n.a.	Key encipherment	Key encipherment
	n.a.	n.a.	Data encipherment	Data encipherment
Certificate Policies				
	Extension marked as non-critical	Extension marked as non-critical	Extension marked as non-critical	Extension marked as non-critical
	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.7 URI: http://pki.multicert.com	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.7 URI: http://pki.multicert.com	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.7 URI: http://pki.multicert.com	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.7 URI: http://pki.multicert.com
	OID: 2.23.140.1.2.2	OID: 2.23.140.1.2.2	n.a.	n.a.
	OID: 0.4.0.2042.1.7	OID: 0.4.0.194112.1.4	n.a.	n.a.
CT Precertificate SCTs				
	Extension marked as non-critical	Extension marked as non-critical	n.a.	n.a.
Basic Constraints				
	Extension marked as critical	Extension marked as critical	Extension marked as critical	Extension marked as critical
Authority Key Identifier				
	Extension marked as non-critical	Extension marked as non-critical	Extension marked as non-critical	Extension marked as non-critical

Certificate Component[3]	TLS/SSL OV	TLS/SSL QWAC	Application	Electronic Invoice
Subject Key Identifier				
	Extension marked as non-critical	Extension marked as non-critical	Extension marked as non-critical	Extension marked as non-critical

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 <identification document type><country>-<identification document nº>	Mandatory <identification document type><country>-<identification document nº>
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
RFC 822 Name (e-mail address)	<e-mail address of the certificate subscriber>	<e-mail address of the certificate subscriber>

[4] n.a. – non aplicable

Certificate Component[4]	Professional Individual	Private Individual
Key Usage		
	Extension marked as critical	Extension marked as critical
	Digital Signature	Digital Signature
	Non-repudiation	Non-repudiation
	Key encipherment	Key encipherment
	Data encipherment	Data encipherment
	Key agreement	Key agreement
Certificate Policies		
	Extension marked as non-critical	Extension marked as non-critical
	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.7 URI: http://pki.multicert.com	OID: 1.3.6.1.4.1.25070.1.1.1.1.0.7 URI: http://pki.multicert.com
Basic Constraints		
	Extension marked as critical	Extension marked as critical
Authority Key Identifier		
	Extension marked as non-critical	Extension marked as non-critical
Subject Key Identifier		
	Extension marked as non-critical	Extension marked as non-critical