multicert
Engineering for digital security

Política de Certificado da EC Subordinada da Entidade Certificadora Raiz da Multicert

Políticas

MULTICERT_PJ.ECRAIZ_405_pt

Identificação do Projeto: ECRaiz da Multicert

Identificação da CA: Multicert Root CA

Nível de Acesso: Público

Versão: 1.0

Data: 24/07/2017

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

Identificador do documento: MULTICERT_PJ.ECRAIZ_405_pt

Palavras-chave: Política de Certificados, EC MULTICERT

Tipologia documental: Políticas

Título: Política de Certificado da EC Subordinada da Entidade Certificadora Raiz da Multicert

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 24/07/2017

Versão atual: 1.0

Identificação do Projeto: ECRaiz da Multicert

Identificação da CA: Multicert Root CA

Cliente:

Histórico de Versões

N.º de Versão	Data	Detalhes	Autor(es)
1.0	24/07/2017	Versão inicial para aprovação	Multicert S.A.

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
Multicert_PJ.ECRAIZ_24.1.1_0001_pt.doc	Declaração de Práticas de Certificação Da Entidade de Certificação Raiz da Multicert	Multicert S.A.

1.1 Resumo Executivo

Decorrente da implementação de vários programas públicos e privados para a promoção das tecnologias de informação e comunicação e a introdução de novos processos de relacionamento em sociedade, entre cidadãos, empresas, organizações não-governamentais e o Estado, com vista ao fortalecimento da sociedade de informação, do governo eletrónico (*eGovernment*) e do comércio eletrónico, a Entidade de Certificação Raiz da Multicert, fornece os mecanismos necessários para a emissão de certificados para Entidades de Certificação Subordinadas, constituindo uma hierarquia de confiança, que promove a segurança eletrónica do titular do certificado digital emitido nesta hierarquia.

A Entidade de Certificação Raiz da Multicert estabelece uma estrutura de confiança eletrónica que proporciona a realização de transações eletrónicas seguras, a autenticação forte, um meio de assinar eletronicamente transações ou informações e documentos eletrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transações ou informação.

Este documento define a Política de Certificados utilizada na emissão de certificados para Entidades Subordinadas da Entidade de Certificação Raiz da Multicert, que complementa e está de acordo com a Declaração de Práticas de Certificação da Entidade de Certificação Raiz da Multicert[1].

Renato Isaias Rodrigues Portela
Digitally signed by Renato Isaias Rodrigues Portela
Date: 2017.07.27 19:08:32 +01'00'

[Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A.
Digitally signed by [Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A.
Date: 2017.07.28 13:22:52 +01'00'

[1] Cf. Multicert_PJ.ECRAIZ_24.1.1_0001_pt.doc, 2015, Declaração de Práticas de Certificação da Entidade de Certificação Raiz da Multicert.

Sumário

2 Introdução

O presente documento é um documento de Política de Certificados, ou PC, cujo objetivo se prende com a definição de um conjunto de políticas e dados para a emissão e validação de certificados e para a garantia de fiabilidade desses mesmos certificados. Não se pretende nomear regras legais ou obrigações, mas antes informar, pelo que se pretende que este documento seja simples, direto e entendido por um público alargado, incluindo pessoas sem conhecimentos técnicos ou legais.

Este documento descreve a política de certificados para a emissão e gestão do certificado da EC Subordinada, emitido pela EC Raiz da Multicert.

Os certificados emitidos pela EC Raiz da Multicert contêm uma referência à PC de modo a permitir que Partes confiantes e outras pessoas interessadas, possam encontrar informação sobre o certificado e sobre as políticas seguidas pela entidade que o emitiu.

2.1 Visão Geral

Este documento satisfaz e complementa os requisitos impostos pela Declaração de Práticas de Certificação (DPC) da EC Raiz da Multicert[1].

2.2 Designação e Identificação do Documento

Este documento é a Política de Certificado de EC Subordinada da EC Raiz da Multicert. A PC é representada no certificado através de um número único designado de "identificador de objeto" (OID), sendo o valor do OID associado a este documento identificado na tabela abaixo.

Este documento é identificado pelos seguintes dados:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 1.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.25070.1.1.1.1.0.1.2
Data de Emissão	14/06/2017
Validade	Não Aplicável
Localização	https://pkiroot.multicert.com/index.html

3 Identificação e Autenticação

3.1 Atribuição de Nomes

A atribuição de nomes segue a convenção determinada pela DPC da EC Raiz da Multicert.

3.1.1 Tipos de nomes

O certificado de Entidade Subordinada (SubEC) é identificado por um nome único (DN – *Distinguished Name*) de acordo com *standard* X.500.

De modo geral, o nome único do certificado é identificado pelos seguintes componentes:

Atributo	**Código**	**Valor**
Country	C (obrigatório)	<País de nacionalidade da Entidade Subordinada>
Organization	O (Obrigatório)	<Organização à qual a Entidade Subordinada pertence>
Organization Unit	OU (opcional)	<Área/Departamento da Organização à qual a Entidade Subordinada pertence>
Organization Unit	OU (opcional)	<Outra Área/Departamento da Organização à qual a Entidade Subordinada pertence>
Common Name	CN (obrigatório)	<Nome da Entidade Subordinada>

3.2 Uso do certificado e par de chaves pelo titular

Os titulares de certificados utilizarão a sua chave privada apenas e só para o fim a que estas se destinam (conforme estabelecido no campo de certificado "*Key Usage*") e sempre com propósitos legais.

A sua utilização apenas é permitida:

a) a quem estiver designado no campo "*subject*" do certificado;

b) De acordo com as condições definidas nos pontos 2.4.1 e 2.4.2 da Declaração de Práticas de Certificação da Entidade de Certificação Raiz da Multicert;

c) Enquanto o certificado se mantiver válido e não estiver na LRC da EC Raiz da Multicert.

4 Perfis de Certificado e LRC

4.1 Perfil de Certificado

Os utilizadores de uma chave pública têm que ter confiança que a chave privada associada, é detida pelo titular remoto correto (pessoa ou sistema) com o qual irão utilizar mecanismos de cifra ou assinatura digital. A confiança é obtida através do uso de certificados digitais X.509 v3, que são a estrutura de dados que fazem a ligação entre a chave pública e o seu titular. Esta ligação é afirmada através da assinatura digital de cada certificado por uma EC de confiança. A EC pode basear esta afirmação em meios técnicos (por exemplo, prova de posse da chave privada através de um protocolo desafio-resposta), na apresentação da chave privada, ou no registo efetuado pelo titular.
Um certificado tem um período limitado de validade, indicado no seu conteúdo e assinado pela EC. Como a assinatura do certificado e a sua validade podem ser verificadas independentemente por qualquer *software* que utilize certificados, estes podem ser distribuídos através de linhas de comunicação e sistemas públicos, assim como guardados no tipo de unidades de armazenamento mais adequados para cada tipo de certificado[2].
O utilizador de um serviço de segurança que requeira o conhecimento da chave pública do utilizador necessita, normalmente, de obter e validar o certificado que contém essa chave. Se o serviço não dispuser de uma cópia fidedigna da chave pública da EC que assinou o certificado, assim como do nome da EC e informação relacionada (tal como o período de validade), então poderá necessitar de um certificado adicional para obter a chave pública da EC e validar a do utilizador. Em geral, para validar a chave pública de um utilizador, pode ser necessária uma cadeia de múltiplos certificados, incluindo o certificado da chave pública do utilizador assinado por uma EC e os certificados das EC's que assinaram este e assim consecutivamente até chegar à EC Raiz

O perfil do certificado de SubEC está de acordo com:

- Recomendação ITU.T X.509[3],
- RFC 5280[3],
- Regulamento 910/2014 e,
- Baseline Requirements do CABForum.

[2] cf. RFC 5280. 2008, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*
[3] cf. ITU-T *Recommendation* X.509. 1997, (1997 E): *Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.*

4.1.1.1 Número da Versão

O campo "*version*" do certificado descreve a versão utilizada na sua codificação. Neste perfil, a versão utilizada é 3 (três).

4.1.1.2 Extensões do Certificado

As componentes e as extensões definidas para os certificados X.509 v3 fornecem métodos para associar atributos a utilizadores ou chaves públicas, assim como para gerir a hierarquia de certificação.

4.2 Perfil de Certificado

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[4]	Comentários
tbsCertificate	**Version**	4.1.2.1	v3	m	Versão do certificado de acordo com o *standard* X.509
	Serial Number	4.1.2.2	<Atribuído pela EC a cada certificado>	m	N.A
	Signature	4.1.2.3	2.16.840.113549.1.1.11	m	Valor TEM que ser igual ao OID no *signatureAlgorithm* (abaixo)
	Issuer	4.1.2.4		m	
	Country (C)		"PT"		País da EC Raiz
	Organization (O)		"Multicert - Serviços de Certificação Electrónica S.A."		Designação formal da organização da EC Raiz
	Common Name (CN)		"Multicert Root Certification Authority <nn>"		<nn> é um valor sequencial iniciado em "01" da EC Raiz.
	Validity	4.1.2.5		m	Validade do Certificado TEM que utilizar tempo UTC até 2049, passando a partir daí a utilizar *GeneralisedTime*

[4] O perfil utilize a terminologia seguinte para cada um dos tipos de campo no certificado X.509:
m – obrigatório (o campo TEM que estar presente)
o – opcional (o campo PODE estar presente)
c – crítico (a extensão é marcada crítica o que significa que as aplicações que utilizem os certificados TÊM que processar esta extensão).

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[4]	Comentários
	Not Before		<data de emissão>		
	Not After		<data de emissão + 4139d >	m	Por defeito a validade será de 4139d, no entanto poderá ter uma validade diferente desde que não exceda a validade da EC Raiz da Multicert
	Subject	4.1.2.6		m	
	Country (C)		<País de nacionalidade da Entidade Subordinada>	m	
	Organization (O)		<Organização à qual a Entidade Subordinada pertence>	m	
	Organization Unit (OU)		<Área/Departamento da Organização à qual a Entidade Subordinada pertence>	o	
	Organization Unit (OU)		<Outra Área/Departamento da Organização à qual a Entidade Subordinada pertence>	o	
	Common Name (CN)		<Nome da Entidade Subordinada>	m	
	Subject Public Key Info	4.1.2.7		m	Utilizado para conter a chave pública e identificar o algoritmo com o qual a chave é utilizada (e.g., RSA, DSA ou Diffie-Hellman).

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[4]	Comentários
	Algorithm		1.2.840.113549.1.1.1		O OID *rsaEncryption* identifica chaves públicas RSA. *{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}* O OID *rsaEncryption* deve ser utilizado no campo *algorithm* com um valor do tipo *AlgorithmIdentifier*. Os parâmetros do campo TÊM que ter o tipo ASN.1 a NULL para o identificador deste algoritmo.[5]
	subjectPublicKey		<Chave Pública com *modulus* n de 4096 bits>		
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		o	
	keyIdentifier		O *key Identifier* é composto pela *hash* de 160-bit SHA-1 do valor da *BIT STRING* do *subjectPublicKey* (excluindo a tag, *length*, e número de bits não usado)>	m	
	Subject Key Identifier	4.2.1.2	O *key Identifier* é composto pela hash de 160-bit SHA-1 do valor da BIT STRING do *subjectPublicKey* (excluindo a tag, *length*, e número de bits não usado)>	m	
	Key Usage	4.2.1.3		mc	Esta extensão é marcada CRÍTICA.

[5] *cf.* RFC 3279. 2002, *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[4]	Comentários
					Confere o tipo de utilização do certificado (KeyCertSign; CRLSign).
	Digital Signature		"0" selecionado		
	Non Repudiation		"0" selecionado		
	Key Encipherment		"0" selecionado		
	Data Encipherment		"0" selecionado		
	Key Agreement		"0" selecionado		
	Key Certificate Signature		"1" selecionado		
	CRL Signature		"1" selecionado		
	Encipher Only		"0" selecionado		
	Decipher Only		"0" selecionado		
	Certificate Policies	4.2.1.4		o	
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.0.7	m	Identificador da Declaração de Práticas de Certificação da EC Raiz da Multicert

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[4]	Comentários
	policyQualifiers		**policyQualifierID:** 1.3.6.1.5.5.7.2.1 **cPSuri:** http://pkiroot.multicert.com/	m	
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.0.1.2	m	Política de Certificado para Entidades Subordinadas
	policyQualifiers		**policyQualifierID:** 1.3.6.1.5.5.7.2.2 **cPSuri:** http://pkiroot.multicert.com/		
	policyIdentifier		2.5.29.32.0		Any policy
	Basic Constraints	4.2.1.9		c	Esta extensão é marcada CRÍTICA.
	CA		TRUE		
	Path Length Constraint		3		
	CRLDistributionPoints	4.2.1.13		m	
	distributionPoint		http://pkiroot.multicert.com/crl/root_mc_crl.crl	m	
	Internet Certificate Extensions				
	Authority Information Access	4.2.2.1		o	
	accessMethod		1.36.1.5.5.7.48.1	m	Valor do OID: 1.36.1.5.5.7.48.1 (id-ad-ocsp)

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[4]	Comentários
	accessLocation		http://ocsp.multicert.com/ocsp	m	
	accessMethod		1.36.1.5.5.7.48.2	o	Valor do OID: 1.36.1.5.5.7.48.2 (id-ad-caissuers)
	accessLocation		http://pkiroot.multicert.com/cert/MCRootCA.cer	o	
	Signature Algorithm	4.1.1.2	2.16.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo *signature* no campo da sequência tbsCertificate. sha-256WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}
	Signature Value	4.1.1.3	<contém a assinatura digital emitida pela EC>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (*subject*) do certificado.

4.2.1 OID do Algoritmo

O campo "*signatureAlgorithm*" do certificado contém o OID do algoritmo criptográfico utilizado pela EC para assinar o certificado: 2.16.840.113549.1.1.11 (sha-256WithRSAEncryption[6]).

4.2.2 Formato dos Nomes

Tal como definido na secção 3.1.

4.2.3 Condicionamento nos Nomes

Para garantir a total interoperabilidade entre as aplicações que utilizam certificados digitais, aconselha-se (mas não se obriga) a que apenas caracteres alfanuméricos não acentuados, espaço, traço de sublinhar, sinal negativo e ponto final ([a-z], [A-Z], [0-9], ' ', '_', '-', '.') sejam utilizados em entradas do Diretório X.500.

4.2.4 OID da Política de Certificados

A extensão "*certificate policies*" contém a sequência de um ou mais termos informativos sobre a política, cada um dos quais consiste num identificador da política e qualificadores opcionais.

Os qualificadores opcionais ("*policyQualifierID*: 1.3.6.1.5.5.7.2.1" e "*cPSuri*") apontam para o URI onde pode ser encontrada a Declaração de Práticas de Certificação com o OID identificado pelo "*policyIdentifier*". Os qualificadores opcionais ("*policyQualifierID*: 1.3.6.1.5.5.7.2.2" e "*userNotice explicitText*") apontam para o URI onde podem ser encontrados a Política de Certificados com o OID identificado pelo "*policyIdentifier*" (i.e., este documento).

4.2.5 Utilização da extensão Policy Constraints

Nada a assinalar.

4.2.6 Sintaxe e semântica do qualificador de política

A extensão "*certificate policies*" contém um tipo de qualificador de política a ser utilizado pelos emissores dos certificados e pelos escritores da política de certificados. O tipo de qualificador é o "*cPSuri*" que contém um apontador, na forma de URI, para a Declaração de Práticas de Certificação publicada pela

[6] sha-256WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)} }

EC e, o "*userNotice explicitText*" que contém um apontador, na forma de URI, para a Politica de Certificados.

4.2.7 Semântica de processamento para a extensão crítica *Certificate Policies*

Nada a assinalar.

4.3 Perfil da lista de revogação de certificados

Quando um certificado é emitido, espera-se que seja utilizado durante todo o seu período de validade. Contudo, várias circunstâncias podem causar que um certificado se torne inválido antes da expiração do seu período de validade. Tais circunstâncias incluem a mudança de nome, mudança de associação entre o titular e os dados do certificado (por exemplo, um trabalhador que termina o emprego) e, o compromisso ou suspeita de compromisso da chave privada correspondente. Sob tais circunstâncias, a EC tem que revogar o certificado[7].

O protocolo X.509 define um método de revogação do certificado, que envolve a emissão periódica, pela EC, de uma estrutura de dados assinada, a que se dá o nome de Lista de Revogação de Certificados (LRC). A LRC é uma lista com identificação temporal dos certificados revogados, assinada pela EC e disponibilizada livremente num repositório público. Cada certificado revogado é identificado na LRC pelo seu número de série. Quando uma aplicação utiliza um certificado (por exemplo, para verificar a assinatura digital de um utilizador remoto), a aplicação verifica a assinatura e validade do certificado, assim como obtém a LRC mais recente e verifica se o número de série do certificado não faz parte da mesma. Note-se que uma EC emite uma nova LRC numa base regular periódica.

Para o caso de Entidades Subordinadas, a esta lista chama-se CARL (*Certification Authority Revocation List*) e a mesma é emitida a cada 3 meses.

O perfil da CARL está de acordo com o perfil de CRL indicado na presente Política..

[7] cf. RFC 5280. 2008, *Internet* X.509 *Public Key Infrastructure Certificate and Certificate Revocation List* (CRL) *Profile*.

5 Identificação e Autenticação

5.1 Validação de Identidade no registo inicial

São elegíveis como potenciais Entidades de Certificação Subordinadas da EC Raiz da Multicert as entidades, sejam pessoa singular ou coletiva credenciadas, que criam ou fornecem meios para a criação das chaves, emitam certificados digitais, asseguram a respetiva publicidade e prestam outros serviços relativos a assinaturas digitais.

5.1.1 Método de Comprovação da Posse da Chave Privada

Como método de comprovação da posse da chave privada, a EC Raiz da Multicert verifica se a entidade certificadora a credenciar detém a chave privada correspondente à chave pública para a qual foi solicitado o certificado digital. É considerado um mecanismo aceitável como método de comprovação a utilização do *Certificate Management Protocol* (CMP) definido no RFC 4210. Igualmente é de considerar que pode ser comprovada a posse da chave privada do emissor do pedido de certificado, uma vez que este formato de pedido de certificado vem assinado pela chave privada.

5.1.2 Autenticação da Identidade de um Pessoa Coletiva

O pedido de emissão de certificado por uma Entidade Subordinada à EC Raiz da Multicert deve ser instruído pelos seguintes documentos, sempre que verificado legalmente:

- Estatutos da pessoa coletiva e, tratando-se de sociedade, contrato de sociedade ou, tratando-se de pessoa singular, a respetiva identificação e domicílio;
- Tratando-se de sociedade, relação de todos os sócios, com especificação das respetivas participações, bem como dos membros dos órgãos de administração e de fiscalização, e, tratando-se de sociedade anónima, relação de todos os acionistas com participações significativas, diretas ou indiretas;
- Prova do substrato patrimonial e dos meios financeiros disponíveis e, designadamente, tratando-se de sociedade, da realização integral do capital social;
- Designação do auditor de segurança para cada tipo de certificado emitido e respetivas declarações de conformidade atestado por uma Entidade acreditada para o efeito;
- Prova de contrato de seguro válido para cobertura adequada da responsabilidade civil emergente da atividade de certificação;

5.1.3 Informação de subscritor/titular não verificada

Nada a assinalar.

5.1.4 Validação de Autoridade

Nada a assinalar.

5.1.5 Critérios para filiação

Nos processos relativos a acordos de filiação, será analisada a seguinte documentação:

a) A Política de Certificados;
b) Declaração de Conformidade emitida por uma entidade acreditada para o efeito de acordo com o 8.2 *Baseline Requirements Certificate Policy* e/ou de acordo com o Regulamento nº 910/2014 do Parlamento Europeu e do Conselho de 23 de Julho de 2014.
c) Aceitação do protocolo fornecido pela EC Raiz das Multicert, Declaração de Práticas de Certificação da EC Raiz da Multicert e o presente documento.

5.2 Identificação e Autenticação para pedido de revogação

Qualquer entidade pode pedir a revogação do seu certificado pelas seguintes razões:

- Cessação de Funções;
- Compromisso da Chaves.

Em qualquer uma das situações o pedido de revogação é efetuado de forma formal obedecendo aos estatutos que vinculam a entidade.

Qualquer entidade integrada no domínio da Multicert pode solicitar a revogação de um determinado certificado, havendo conhecimento ou suspeita de comprometimento da chave privada do titular. Neste caso, a entidade solicitante deverá solicitar o pedido acompanhado de comprovativos, no caso de conhecimento, ou motivações que levam a sustentem a suspeita de comprometimento da chave privada.

A Multicert, irá avaliar de imediato o pedido, sendo que em 5 dias úteis publicará um veredicto à entidade solicitante bem como à entidade titular do certificado a revogar.

A Multicert pode ainda determinar a revogação das suas Entidades Subordinadas perante os seguintes cenários:

- Ausência de declaração de conformidade;

- Identificação de emissão de certificados fraudulentos;
- Identificação de emissão de certificados não conformes com a legislação e/ou normas internacionais aplicáveis.

Para cada situação, a Multicert informará de imediato a Entidade Subordinada acordando o tempo para resolução da mesma, de acordo com o nível de criticidade.

A Multicert procede à revogação das chaves, sempre que o motivo for Compromisso da Chaves e este esteja devidamente comprovado.

6 Requisitos operacionais do ciclo de vida do certificado

6.1 Pedido de Certificado

Só é possível efetuar o pedido de certificado para uma EC Subordinada, após aceitação das condições impostas pela EC Raiz da Multicert, nomeadamente aceitação de um protocolo a ser fornecido, leitura do presente documento e a consequente autorização de entrada em funcionamento da EC Subordinada por parte da EC Raiz da Multicert.

Assim que a aceitação seja formalizada, será disponibilizado pela Multicert o **Formulário de Emissão de certificado de EC Subordinada da EC Raiz da Multicert** ao requerente, que deverá ser preenchido e assinado pelo(s) representante(s) legal(is) da entidade.

6.2 Emissão de Certificado

6.2.1 Procedimentos para a emissão de certificado

A emissão do certificado é efetuada por meio de uma intervenção que decorre na zona de alta segurança da EC Raiz da Multicert após aceitação de contrato de assinatura, em que se encontram presentes:

- 4 Membros dos Grupos de Trabalho da PKI da Multicert, já que a segregação de funções não possibilita a presença de um número inferior de elementos;
- Quaisquer observadores, aceites simultaneamente pelo Grupo de Gestão da EC Raiz da Multicert e pelos representantes da entidade subordinada requerente.

A intervenção de emissão de certificado é constituída pelos seguintes passos:

a) Identificação e autenticação de todas as pessoas presentes, garantindo que o(s) representante(s) da EC Subordinada requerente e os membros dos Grupos de Trabalho têm os poderes necessários para os atos a praticar;

b) Representante(s) da EC Subordinada requerente entregam, o pedido de certificado em formato PKCS#10, acompanhado do **Formulário de Emissão de certificado de EC Subordinada da EC Raiz da Multicert**, devidamente preenchido e assinado, aos membros do Grupo de

Trabalho da EC Raiz da Multicert. O formulário é datado e assinado pelos membros do Grupo de Trabalho que o devolvem ao(s) representante(s) da entidade subordinada requerente;

c) Os membros do Grupo de Trabalho efetuam o procedimento de arranque de processamento da EC Raiz da Multicert e emitem o certificado (correspondente ao PKCS#10 fornecido no CD/DVD) em formato PEM;

d) Os membros do Grupo de Trabalho armazenam o certificado em formato PEM num CD/DVD e preenchem e assinam o Formulário de Receção do Certificado da EC Subordinada;

e) Os membros dos Grupos de Trabalho solicitam a assinatura do **Formulário de Receção do Certificado da EC Subordinada** ao(s) representante(s) da entidade subordinada e entregam o CD/DVD com o certificado emitido;

f) A cerimónia de emissão fica terminada com a execução do procedimento de finalização de processamento da EC Raiz da Multicert, pelos membros do Grupo de Trabalho da EC Raiz da Multicert.

A entidade subordinada tem, após a receção do certificado, três dias úteis para efetuar as validações que achar convenientes e formalizar a aceitação do mesmo, através do preenchimento do **Formulário de Aceitação do Certificado da EC Subordinada** devolvendo-o devidamente preenchido e assinado, aos elementos dos Grupos de Trabalho da EC Raiz da Multicert.

O certificado só poderá ser disponibilizado ao utilizador final após assinado um acordo entre as entidades envolvidas (nomeadamente as que beneficiam, direta ou indiretamente, das sua hierarquia)

O certificado emitido inicia a sua vigência após a formalização da aceitação do mesmo pela entidade subordinada.

6.2.2 Notificação da emissão do certificado ao titular

A emissão do certificado é efetuada de acordo com secção anterior, sendo que fica notificado o titular do certificado no ato da entrega do mesmo.

6.3 Aceitação do Certificado

6.3.1 Procedimentos para a aceitação de certificado

A aceitação do certificado é feita de acordo com o descrito no capítulo 6.2.1 alínea e).

6.3.2 Publicação do certificado

A Multicert publicará os certificados emitidos a entidades subordinadas através do seu depositário público pki.multicert.com na sua Declaração de Práticas de Certificação.

6.3.3 Notificação da emissão de certificado a outras entidades

A Multicert publicará a emissão de certificados a entidades subordinadas através da publicação de novas versões da DPC da EC Raiz da Multicert.

6.4 Uso do certificado e par de chaves

6.4.1 Uso do certificado e da chave privada pelo titular

A chave privada associada ao certificado emitido no âmbito desta política é utilizada apenas e só para o fim a que esta se destina (conforme estabelecido no campo do certificado "*keyUsage*") e sempre com propósitos legais e estabelecidos no âmbito desta política.

A sua utilização apenas é permitida:

a) à Entidade Subordinada à qual foi emitido o certificado;

b) Enquanto o certificado se mantiver válido e não estiver na LRA da EC Raiz da Multicert.

6.4.2 Uso do certificado e da chave pública pelas partes confiantes

Ver secção 5.3.5 da Declaração de Práticas de Certificação da Entidade de Certificação da Raiz da Multicert.

6.5 Renovação de certificado com geração de novo par de chaves

A renovação de chaves do certificado (*certificate re-key*) é o processo em que um titular (ou representante legal) gera um novo par de chaves e submete o pedido para emissão de novo certificado que certifica a nova chave pública. Este processo, no âmbito desta Política de Certificado, é designado por renovação de certificado com geração de novo par de chaves.

Esta secção encontra-se de acordo com a secção 5.2 do documento de Declaração de Práticas de Certificação da EC Raiz da Multicert.

6.5.1 Motivo para a renovação de certificado com geração de novo par de chaves

De acordo com a secção 5.5.1 do documento de Declaração de Práticas da EC Raiz da Multicert.

6.5.2 Quem pode submeter o pedido de certificação de uma nova chave pública

De acordo com a secção 5.1 do documento de Declaração de Práticas da EC Raiz da Multicert.

6.5.3 Processamento do pedido de renovação de certificado com geração de novo par de chaves

De acordo com a secção 5.2. do documento de Declaração de Práticas da EC Raiz da Multicert.

6.5.4 Notificação da emissão de novo certificado ao titular

De acordo com a secção 6.2.2 deste documento.

6.5.5 Procedimentos para aceitação de um certificado renovado com geração de novo par de chaves

De acordo com a secção 5.3.1 do documento de Declaração de Práticas da EC Raiz da Multicert.

6.5.6 Publicação de certificado renovado com geração de novo par de chaves

De acordo com a secção 5.3.2 do documento de Declaração de Práticas da EC Raiz da Multicert.

6.5.7 Notificação da emissão de certificado renovado a outras entidades

De acordo com a secção 5.3.1 do documento de Declaração de Práticas da EC Raiz da Multicert.

6.6 Suspensão e revogação de certificado

De acordo com a secção 5.7 do documento de Declaração de Práticas da EC Raiz da Multicert.

7 Auditoria e Avaliações de Conformidade

Todas as Entidades de Certificação integradas na hierarquia da EC Raiz da Multicert devem construir, obrigatoriamente, as suas Declarações de Práticas de Certificação em conformidade com os requisitos mínimos definidos neste documento assim como os definidos da Declaração de Práticas de Certificação da EC Raiz da Multicert.

7.1 Frequência ou motivo da auditoria

De acordo com o ponto anterior, as diversas entidades são alvo de auditoria nas seguintes situações:

a) No processo de integração na EC Raiz da Multicert;

b) Anualmente;

c) A qualquer momento, sem aviso prévio.

A secção 9.2 da Declaração de Práticas de Certificação da EC Raiz da Multicert explícita a regularidade e a ocorrência das diversas auditorias.

7.2 Identidade e Qualificações do auditor

O auditor é uma pessoa ou organização, de reconhecida idoneidade, com experiência e qualificações comprovadas na área de segurança de informação e dos sistemas de informação, infraestruturas de chaves públicas e devidamente acreditados por uma Entidade Acreditadora ao abrigo do Regulamento 910/2014.

7.3 Âmbito da Auditoria

São alvo de auditoria todas as entidades que, direta ou indiretamente, exerçam atividades de certificação nos termos definidos desta política.

As auditorias devem ser efetuadas de acordo com o estipulado no regulamento 910/2014 e legislação aplicável, sendo que anualmente a Multicert recebe uma Declaração de Conformidade das Entidades a si subordinadas. Igualmente a Entidades Subordinadas devem submeter-se a um teste de penetração, anualmente, que englobe todos os serviços disponibilizados.

Para além das auditorias da conformidade, a Multicert poderá efetuar outras fiscalizações e investigações para assegurar a conformidade, das Entidades de Certificação integradas na PKI da Multicert, com a legislação nacional bem como normativos internacionais aplicáveis. A execução destas auditorias internas, fiscalizações e investigações poderá ser delegada a uma entidade externa de auditoria.

8 Outras situações e Assuntos Legais

8.1 Taxas

8.1.1 Taxas Por Emissão ou Renovação de Certificados

De acordo com o que se encontra definido na secção 11.1.1 da Declaração de Práticas de Certificação da EC Raiz da Multicert.

8.1.2 Taxas para Acesso a Certificado

Nada a assinalar

8.1.3 Taxas para Acesso a Informação do estado Certificado ou de Revogação

De acordo com o que se encontra definido na secção 11.1.3 da Declaração de Práticas de Certificação da EC Raiz da Multicert.

8.1.1 Política de reembolso

Nada a assinalar.

8.1.2 Taxas para outros Serviços

De acordo com o que se encontra definido na secção 11.1.4 da Declaração de Práticas de Certificação da EC Raiz da Multicert.

8.1.3 Política de reembolso

Nada a assinalar

9 Responsabilidade Financeira

9.1 Seguro de Cobertura

A Entidades Subordinadas da EC Raiz da Multicert devem respeitar a legislação em vigor no que se concerne aos seguros de cobertura de responsabilidade civil.

9.2 Outros Seguros

Nada a Assinalar.

10 Confidencialidade da Informação Processada

De acordo com a secção 11.3 da Declaração de Práticas de Certificação da EC Raiz da Multicert.

10.1 Privacidade dos Dados Pessoais

De acordo com a secção 11.4 da Declaração de Práticas de Certificação da EC Raiz da Multicert.

10.2 Direitos de Propriedade Intelectual

De acordo com a secção 11.5 da Declaração de Práticas de Certificação da EC Raiz da Multicert.

10.3 Representações e garantias

10.3.1 Representação e garantias das entidades certificadoras

As EC's da hierarquia da PKI da Multicert estão obrigadas a:

a) Realizar as suas operações de acordo com esta Política;
b) Declarar de forma clara todas as suas Práticas de Certificação no documento apropriado,
c) Proteger as suas chaves privadas;
d) Emitir certificados de acordo com o *standard* X.509;
e) Emitir certificados que estejam conformes com a informação conhecida no momento de sua emissão e livres de erros de entrada de dados;
f) Garantir a confidencialidade no processo da geração dos dados da criação da assinatura e a sua entrega por um procedimento seguro ao titular;
g) Utilizar sistemas e produtos fiáveis que estejam protegidos contra toda a alteração e que garantam a segurança técnica e criptográfica dos processos de certificação;
h) Utilizar sistemas fiáveis para armazenar certificados reconhecidos que permitam comprovar a sua autenticidade e impedir que pessoas não autorizadas alterem os dados;
i) Arquivar sem alteração os certificados emitidos;
j) Garantir que podem determinar com precisão da data e hora em que emitiu ou extinguiu ou suspendeu um certificado;
k) Empregar pessoal com qualificações, conhecimentos experiência necessárias para a prestação de serviços de certificação;

l) Revogar os certificados nos termos definidos na sua DPC e publicar os certificados revogados na LRC do seu repositório, com a frequência estipulada da sua DPC;

m) Publicar a sua DPC e as Políticas de Certificado aplicáveis no seu repositório garantindo o acesso às versões atuais assim como as versões anteriores;

n) Notificar com a rapidez necessária, por correio eletrónico os titulares dos certificados em caso da EC proceder à revogação ou suspensão dos mesmos, indicando o motivo que originou esta ação;

o) Colaborar com as auditorias dirigidas pela EC Raiz da Multicert;

p) Operar de acordo com a legislação aplicável;

q) Proteger, caso existam, as chaves que estejam sobre sua custódia;

r) Garantir a disponibilidade da LRC de acordo com as disposições da secção 5.7.10 da DPC da EC Raiz da Multicert;

s) Em caso de cessar a sua atividade deverá comunicar com uma antecedência mínima de dois meses a todos os titulares dos certificados emitidos assim como à EC Raiz da Multicert;

t) Ter um plano devidamente definido para a Cessação de funções;

u) Cumprir com as especificações contidas na norma sobre Proteção de Dados Pessoais;

v) Conservar toda a informação e documentação relativa a um certificado reconhecido e as Declarações de Práticas de Certificação vigentes em cada momento e durante quinze anos desde o momento da emissão e,

w) Atuar em conformidade com a ETSI EN 319 411-1, ETSI EN 319 411-2 e com os Requisitos do CabForum (cada uma, conforme alteradas e retificadas periodicamente),

x) Garantir que os perfis de Certificado emitidos pelo Afiliado e Sub-Afiliados estão em conformidade com:

   a. a ETSI EN 319 412-2 ou ETSI EN 319 412-3, para Certificados Qualificados e

   b. para Certificados de Autenticação, apenas *keyUsage* *digitalSignature* e EKU *clientAuth*.

y) Proceder a toda a validação exigida pelas Normas do Setor antes da emissão do Certificado,

z) Emitir cada tipo de certificado a partir de uma SubEC separada,

aa) Garantir que todos os Certificados contenham um valor *extendedKeyUsage* diferente de *anyExtendedKeyUsage*.

10.3.2 Representações e garantias das Entidades de Registo

Nada a assinalar.

10.3.3 Representação e garantias dos titulares

De acordo com a secção 11.6.3 da Declaração de Práticas de Certificação da EC Raiz da Multicert.

10.3.4 Representação e garantias das partes confiantes

De acordo com a secção 11.6.4 da Declaração de Práticas de Certificação da EC Raiz da Multicert.

11 Lista de Definições e Acrónimos

11.1 Definições

Assinatura digital	Modalidade de assinatura eletrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento eletrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento eletrónico foi alterado depois de aposta a assinatura.
Assinatura eletrónica	Resultado de um processamento eletrónico de dados, suscetível de constituir objeto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento eletrónico.
Assinatura eletrónica avançada	Assinatura eletrónica que preenche os seguintes requisitos: i) Identifica de forma unívoca o titular como autor do documento; ii) A sua aposição ao documento depende apenas da vontade do titular; iii) É criada com meios que o titular pode manter sob seu controlo exclusivo; iv) A sua conexão com o documento permite detetar toda e qualquer alteração superveniente do conteúdo deste.
Assinatura eletrónica qualificada	Assinatura digital ou outra modalidade de assinatura eletrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura.
Autoridade Credenciadora	Entidade competente para a credenciação e fiscalização das entidades certificadoras.
Certificado	Documento eletrónico que liga os dados de verificação de assinatura ao seu titular e confirma a identidade desse titular.

Certificado qualificado	Certificado que contém os elementos referidos no artigo 29.° do DL 62/2003 [7] e é emitido por entidade certificadora que reúne os requisitos definidos no artigo 24.° do DL 62/2003.
Chave privada	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a correspondente chave pública.
Chave pública	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves.
Credenciação	Ato pelo qual é reconhecido a uma entidade que o solicite e que exerça a atividade de entidade certificadora o preenchimento dos requisitos definidos no presente diploma para os efeitos nele previstos.
Dados de criação de assinatura	Conjunto único de dados, como chaves privadas, utilizado pelo titular para a criação de uma assinatura eletrónica.
Dados de verificação de assinatura	Conjunto de dados, como chaves públicas, utilizado para verificar uma assinatura eletrónica.
Dispositivo de criação de assinatura	Suporte lógico ou dispositivo de equipamento utilizado para possibilitar o tratamento dos dados de criação de assinatura.
Dispositivo seguro de criação de assinatura	Dispositivo de criação de assinatura que assegure, através de meios técnicos e processuais adequados, que: i) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura só possam ocorrer uma única vez e que a confidencialidade desses dados se encontre assegurada; ii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura não possam, com um grau razoável de segurança, ser deduzidos de outros dados e que a assinatura esteja protegida contra falsificações realizadas através das tecnologias disponíveis; iii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura possam ser eficazmente protegidos pelo titular contra a utilização ilegítima por terceiros; iv) Os dados que careçam de assinatura não sejam modificados e

	possam ser apresentados ao titular antes do processo de assinatura.
Documento eletrónico	Documento elaborado mediante processamento eletrónico de dados.
Endereço eletrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos.
Estampilha temporal	Estrutura de dados que liga a representação eletrónica de um *datum* com uma data/hora particular, estabelecendo evidência de que o *datum* existia nessa data/hora.
Parte confiante	Recetor de uma estampilha temporal que confia na mesma.
Sistema TSA (*TSA system*)	Composição de produtos IT e componentes, organizados de modo a suportar o fornecimento de serviços de validação cronológica.
UTC (*Coordinated Universal Time*)	Escala de tempo baseada no segundo, como definido na *ITU-R Recommendation TF.460-5* [10].
UTC(k)	Escala de tempo fornecida pelo laboratório "k" que garante ±100 ns em relação ao UTC (conforme *ITU-R Recommendation TF.536-1* [11])
Validação cronológica	Declaração de uma EVC que atesta a data e hora da criação, expedição ou receção de um documento eletrónico.

11.2 Acrónimos

ANSI	*American National Standards Institute*
C	*Country*
CA	*Certification Authority* (o mesmo que EC)
CN	*Common Name*
CRL	Ver LRC
DL	Decreto Lei
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação

DR	Decreto Regulamentar
EC	Entidade de Certificação
ECD	Entidade Certificadora de Documentos
ER	Entidade de Registo
GMT	Tempo Médio de Greenwich (*Greenwich Mean Time*)
GNS	*Gabinete Nacional de Segurança*
LRC	Lista de Revogação de Certificados
MAC	*Message Authentication Codes*
O	*Organization*
OCSP	*Online Certificate Status Protocol*
OID	Identificador de Objecto
PC	Política de Certificado
PKCS	*Public-Key Cryptography Standards*
PKI	*Public Key Infrastructure* (Infra-estrutura de Chave Pública)
SHA	*Secure Hash Algorithm*
SGCVC	*Sistema de Gestão de Ciclo de Vida de Certificados*
SSCD	*Secure Signature-Creation Device*
TSA	*Time-Stamping Authority* (o mesmo que EVC)