multicert

Engineering for digital security

Política de Certificado SSL

Política

MULTICERT_PJ.CA3_24.1.2_0009_pt.pdf

Nível de Acesso: Restrito

Versão: 3.0

Data: 24/10/2017

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.CA3_24.1.2_0009_pt.pdf

Palavras-chave: política; ssl

Tipologia Documental: Política

Título: Política de Certificado SSL

Idioma Original: Português

Idioma de Publicação: Português

Nível de Acesso: Restrito

Data: 24/10/2017

Versão Atual: 3.0

Histórico de Versões

Versão	Data	Detalhes	Autor(es)
1.0	13/01/2014	Versão Aprovada	MULTICERT S.A.
1.1-1.7	12/02/2016	Revisões	MULTICERT S.A.
2.0	12/03/2016	Versão Aprovada	MULTICERT S.A.
2.1	27/07/2017	Inclusão requisitos eIDAS	MULTICERT S.A.

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
MULTICERT_PJ.CA3_24.1.1_0001_pt.pdf	Declaração de Práticas de Certificação	MULTICERT S.A.

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, os certificados digitais emitidos pela Entidade de Certificação MULTICERT, credenciada pela Autoridade Nacional de Segurança (conforme previsto na legislação europeia e nacional), fornecem os mecanismos necessários para a autenticação digital forte da identidade de um servidor web.

A infraestrutura da Entidade de Certificação MULTICERT fornece uma hierarquia de confiança, que promove a segurança eletrónica bem como uma estrutura de confiança eletrónica que possibilita a comunicação de informação via web de forma segura, nomeadamente no que diz respeito à autenticação de servidores, à titularidade de um domínio Internet e à integridade e confidencialidade da informação transacionada. Quem acede a um servidor web identificado com um certificado digital MULTICERT tem a garantia da identidade do destinatário da comunicação (i.e., tem a certeza que está a comunicar com o sítio web pretendido e não com outro sítio web ou entidade). Esta verificação é garantida pela assinatura do certificado com a chave privada da Entidade de Certificação

A Entidade de Certificação MULTICERT está devidamente credenciada pela Autoridade Nacional de Segurança (http://www.gns.gov.pt/trusted-lists.aspx), com credenciação número ANS-ECC-7/2014, à data de 20/06/2014, conforme previsto na legislação portuguesa e europeia, estando deste modo habilitada legalmente a emitir todo o tipo de certificados digitais, incluindo os certificados digitais qualificados (certificados digitais de mais elevado grau de segurança previsto na legislação).

Este documento define a Política de Certificados utilizada na emissão do certificado digital SSL.

Renato Isaias Rodrigues Portela

Digitally signed by Renato Isaias Rodrigues Portela
Date: 2017.10.24 19:31:41 +01'00'

[Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A.

Digitally signed by [Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A.
Date: 2017.10.27 08:39:06 +01'00'

Sumário

2 Introdução

Objetivos

O objetivo deste documento é apresentar o perfil do certificado SSL emitido pela Entidade de Certificação da MULTICERT.

Público-Alvo

Este documento deve ser lido por:

- Recursos humanos atribuídos aos grupos de trabalho da EC da MULTICERT;
- Terceiras partes, encarregues de auditar a EC da MULTICERT;
- Todo o público, em geral.

Estrutura do Documento

Assume-se que o leitor é conhecedor dos conceitos de criptografia, infraestruturas de chave pública e assinatura eletrónica. Caso esta situação não se verifique recomenda-se o aprofundar de conceitos e conhecimento nos tópicos anteriormente focado antes de proceder com a leitura do documento.

Este documento complementa a Declaração de Práticas de Certificação da EC da MULTICERT, presumindo-se que o leitor leu integralmente o seu conteúdo antes de iniciar a leitura deste documento.

3 Contexto Geral

O presente documento tem como objetivo a definição de um conjunto características que definem o perfil dos Certificado de Servidor Web emitidos pela EC da MULTICERT, permitindo assim a garantir a fiabilidade dos mesmos. 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.

Os Certificados emitidos pela EC da MULTICERT contêm uma referência a esta Política de Certificados de modo a permitir que partes confiantes e outras entidades ou pessoas interessadas possam encontrar informação sobre o certificado e sobre as políticas seguidas pela entidade que o emitiu.

3.1 Visão Geral

Esta PC, satisfaz e complementa os requisitos impostos pela Declaração de Práticas de Certificação da EC da MULTICERT[1].

3.2 Designação e Identificação do Documento

Este documento é a Política de Certificados do certificado de Servidor Web. A PC, é representada num certificado através de um número único designado de "identificador de objeto" (OID. Esta Política segue o disposto para certificados OVCP (*Organization Validation Certificate Policy*) referido no ETSI 102 042 v2.4.1.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 3.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.25070.1.1.1.1.0.1.5
Data de Emissão	24/10/2017
Validade	1 Ano
Localização	https://pki.multicert.com/index.html

[1] [1] *cf.* MULTICERT_PJ.CA3_24.1.1_0001_pt.pdf, Declaração de Práticas de Certificação.

4 Identificação e Autenticação

4.1 Atribuição de Nomes

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

4.1.1 Tipos de nomes

O Certificado de Servidor *Web* é identificado por um nome único (DN – *Distinguished Name*) de acordo com *standard* X.500.

O nome único do certificado da EC da MULTICERT é identificado pelos seguintes componentes:

Atributo	Código	Valor
Country	C	<País>
LocalityName	L	<Localidade onde se encontra filiada a Organização>
Organization	O	<Nome legal da Organização>
Organization Unit	OU	Certificado SSL/TLS
Common Name	CN	<*full qualified domain name* do Servidor Web>

4.2 Uso do certificado e par de chaves pelo titular

A EC da MULTICERT é a emissora do Certificado de Servidor *Web*, sendo o mesmo emitido para o servidor web cujo nome qualificado do domínio estiver indicado no campo "*CommonName*". É utilizado na autenticação e estabelecimento de canais cifrados/confidenciais, de acordo com o protocolo SSL/TLS, entre uma aplicação cliente web e o servidor web.

A segurança na identificação do servidor é conseguida através do envio de um "desafio" por este, assinado com a sua chave privada. O *browser*, ao verificar esse "desafio" com a chave pública correspondente, identifica o servidor web, o que no mundo físico equivale à apresentação de um documento de identificação (Bilhete de Identidade ou Passaporte) de um indivíduo.

5 Perfil de Certificado

5.1 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. Essa confiança é dada através do uso de certificados digitais X.509 v3, que são estrutura de dados que fazem a ligação entre a chave pública e o seu titular. Esta ligação é garantida 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, os certificados podem ser distribuídos através de linhas de comunicação e sistemas públicos, assim como podem ser guardados em qualquer tipo de unidades de armazenamento.[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 um certificado adicional para obter a chave pública da EC e validar a chave pública 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, zero ou mais certificados adicionais de EC's assinados por outras EC`s[2].

O perfil do certificado de Servidor Web está de acordo com:

- Recomendação ITU.T X.509[3];
- RFC 5280[2] e
- *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum*, v1.3.0

5.1.1 Número da Versão

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

[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.*

5.1.2 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.

Componente do Certificado		Secção RFC 5280	Valor	Tipo	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	
	Signature	4.1.2.3	1.2.840.113549.1.1.11	m	Valor TEM que ser igual ao OID no *signatureAlgorithm* (abaixo)
	Issuer	4.1.2.4		m	
	Country (C)		"PT"		País do titular
	Organization (O)		"MULTICERT - Serviços de Certificação Electrónica S.A."		Designação formal da organização do titular
	Organization Unit (OU)		"Accredited Certification Authority"		Outra designação da organização do titular
	Common Name (CN)		"MULTICERT Certification Authority <nnn>"		Nome da Organização – Nome da CA
	Validity	4.1.2.5		m	Validade do certificado TEM que utilizar tempo UTC até 2049, passando a partir daí a utilizar GeneralisedTime
	Not Before		<data de emissão>		
	Not After		<data de emissão + (1ano ou 2 anos ou 3 anos)>		Validade de aproximadamente 3 anos e um mês. Renovado (com geração de novo par de chaves) um mês antes do final da validade.
	Subject	4.1.2.6		m	
	Country (C)		<País>	m	País origem da Organização
	Locality Name(L)		<Localidade >	m	Localidade onde se encontra filiada a Organização
	Organization (O)		<Nome da Organização>	m	Nome da Organização de acordo com o Registo comercial

Componente do Certificado		Secção RFC 5280	Valor	Tipo	Comentários
	Organization Unit (OU)		Certificado SSL/TLS	m	Designação do tipo de certificado
	Organization Unit (OU)		<Outro Nome da Organização>	o	Outro Nome da Organização
	Common Name (CN)		<full qualified domain name do Servidor Web ou IPAddress>	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).
	algorithm		1.2.840.113549.1.1.1		O OID rsaEncryption identifica chaves públicas RSA. pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 } rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 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 param o identificador deste algoritmo.[4]
	subjectPublicKey		<Chave Pública com modulus n de 2048 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 *subjectKeydentifier* do	m	

[4] *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 RFC 5280	Valor	Tipo	Comentários
			certificado do emissor (excluindo a tag, length, e número de bits não usado)>		
	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. Confere o tipo de utilização do certificado.
	Digital Signature		"1" selecionado		
	Non Repudiation		"0" selecionado		
	Key Encipherment		"1" selecionado		
	Data Encipherment		"1" selecionado		
	Key Agreement		"0" selecionado		
	Key Certificate Signature		"0" selecionado		
	CRL Signature		"0" selecionado		
	Encipher Only		"0" selecionado		
	Decipher Only		"0" selecionado		
	Certificate Policies	4.2.1.5		m	
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.7	m	Identificador da Declaração de Práticas de Certificação da EC MULTICERT.
	policyQualifiers		*policyQualifierID*: 1.3.6.1.5.5.7.2.1	o	Valor do OID: 1.3.6.1.5.5.7.2.1 (id-qt-cps PKIX CPS *Pointer Qualifier*)

Componente do Certificado		Secção RFC 5280	Valor	Tipo	Comentários
			cPSuri: pki.multicert.com/pol/cps/MULTICERT_PJ.CA3_24.1.1_0001_pt.pdf		Descrição do OID: "O atributo cPSuri contém um apontador para a Declaração de Práticas de Certificação publicada pela EC. O apontador está na forma de um URI." (http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.1.html)
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.1.5	m	Identificador da Política de Certificados de Servidor Web (SSL).
	policyQualifiers		*policyQualifierID*: 1.3.6.1.5.5.7.2.2 *userNotice explicitText:*"Certificado emitido de acordo com a Política de Certificados em /Certificate issued in accordance with the Certificate Policy in pki.multicert.com/pol/cp/webserver.html	m	Valor do OID: 1.3.6.1.5.5.7.2.2 (id-qt-unotice) Descrição do OID: "*User notice* é utilizado para apresentar às partes confiantes quando um certificado é utilizado" (http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.2.html)
	policyIdentifier		2.23.140.1.2.2	m	{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) subject-identity-validated(2)} Certificado emitido de acordo com os requisitos do CA/Browser Forum O OID indica que o certificado contém informações verificadas sobre a identidade jurídica do titular do certificado.
	policyIdentifier		0.4.0.194112.1.4	m	Valor do OID: 0.4.0.194112.1.3[5], identifica que o certificado é emitido para autenticação de sítios web conforme certificado qualificado definido no artigo 3 e 45 do Regulamento (E)U) Nº 910/2014.. {itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies

[5] ETSI EN 319 411-2 V2.1.1 - *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates*

Componente do Certificado		Secção RFC 5280	Valor	Tipo	Comentários
					(194112) policy-identifiers(1) qcp-web (4)}
	Subject Alternative Name	4.2.1.7		o	
	GeneralName		DNS = <*full qualified domain name* do servidor Web>	o	Máximo 7 Domínios
	IPAddress		IPAddress = <*IPAddress* do servidor Web>	o	Apenas domínios externos
	Basic Constraints	4.2.1.10		c	Esta extensão é marcada CRÍTICA.
	CA		FALSE		
	PathLenConstraint		0		
	Extended Key Usage	4.2.1.13		m	
	keyPurposeID		id-kp-serverAuth		Descrição do OID: Autenticação do servidor: 1.3.6.1.5.5.7.3.1
	keyPurposeID		id-kp-clientAuth		Descrição do OID: Autenticação do cliente: 1.3.6.1.5.5.7.3.2
	CRLDistributionPoints	4.2.1.14		om	
	distributionPoint		http://ec2pki.multicert.com/crl/crl_mca002.crl	m	URL para aceder à CRL
	Freshest CRL	4.2.1.15			
	distributionPoint		http://ec2pki.multicert.com/crl/crl_mca002_delta.crl	m	URL para aceder à Delta CRL
	Qualified Certificate Statement		id-pe-qcStatements = "1.3.6.1.5.5.7.1.3"[6]		A extensão *QCStatements* é uma extensão introduzida pelo PKIX Qualified Certificate Profile[7] e ETSI[8].

[6] http://www.alvestrand.no/objectid/1.3.6.1.5.5.7.1.3.html

[7] *cf.* RFC 3739. 2004, *Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.*

[8] *cf.* ETSI EN 319 412-5 V2.1.1 - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*

Componente do Certificado		Secção RFC 5280	Valor	Tipo	Comentários
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcCompliance = "0.4.0.1862.1.1"		Declaração da EC MULTICERT, representada por um OID, indicando que este certificado é emitido de acordo com o Anexo IV do Regulamento (EU) 910/2014).
	id-qcs-pkixQCSyntax-v2		id-etsi-qct-web="0.4.0.1862.1.6.3" Text="Certificate for website authentication as defined in Regulation (EU) No 910/2014"		Declaração da EC MULTICERT, representada por um OID, indicando que este certificado é emitido como um certificado qualificado de para autenticação de sítio web, de acordo com o Anexo IV do Regulamento (EU) 910/2014.
	Internet Certificate Extensions				
	Authority Information Access	4.2.2.1		m	
	accessMethod		1.3.6.1.5.5.7.48.1	m	Valor do OID do OCSP value: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp) Descrição do OID: *Online Certificate Status Protocol*
	accessLocation		http://ocsp.multicert.com/ocsp	m	URL para aceder ao OCSP
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	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.

5.1.3 OID do Algoritmo

O campo "*signatureAlgorithm*" do certificado contém o OID do algoritmo criptográfico utilizado pela EC para assinar o certificado: 1.2.840.113549.1.1.11 (*sha-2WithRSAEncryption*[9]).

5.1.4 Formato dos Nomes

Tal como definido na secção 2.1.

5.1.5 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.

5.1.6 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 pode ser encontrados a Politica de Certificados com o OID identificado pelo "*policyIdentifier*" (i.e., este documento).

O qualificador 0.4.0.194112.1.4 aponta para a Política de Certificado para certificados qualificados de autenticação de servidor web ao abrigo do Regulamento EU nº 910/2014.

5.1.7 Utilização da extensão *Policy Constraints*

Nada a assinalar.

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

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

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

Nada a assinalar.

6 Validação de Domínios

6.1 Autorização pelo Responsável do *Domain Name*

A EC confirma que, à data da emissão do certificado, o requerente do certificado é o responsável do *Domain Name* ou tem controlo sobre o *Full Qualified Domain Name*, através de:

- Confirmação de que o requerente do certificado tem o registo do *Domain Name* diretamente na entidade de registo de domínios[10];
- Comunicação direta com o responsável do *Domain Name*, utilizando a morada, email ou número de telefone fornecido pela entidade de registo de domínios;
- Comunicação direta com o responsável do *Domain Name* utilizando a informação de contacto listada no campo "*registrant*","*technical*" ou "*administrative*" dos registos do WHOIS[11];
- Comunicação com o administrador do domínio utilizando o endereço de *email* criado com o prefixo "admin", "administrator", "webmaster", "*hostmaster*" ou "*postmaster*", seguido do sinal "@", e terminado pelo *Domain Name*;
- Um Documento de Autorização de Domínio fidedigno;
- Demonstração por parte do Requerente de que possui controlo prático sobre o *Fully Qualified Domain Name*, através do pré-acordo sobre uma alteração a determinada informação contida numa página Web online identificada por um URI[12] que contém o *Fully Qualified Domain Name*; ou
- Utilização de qualquer outro método de confirmação (desde que providencie o mesmo nível de confiança que os métodos de verificação referidos anteriormente), sendo que a EC preservará o registo que servirá de evidência da confirmação de que o Requerente é o responsável do *Domain Name* ou tem controlo sobre o *Fully Qualified Domain Name*.

6.2 Autorização para um Endereço IP

- Para cada endereço de IP listado no certificado, a EC confirma que, à data de emissão do certificado, o Requerente tem controlo sobre o endereço IP, através de:
- Demonstração por parte do Requerente de que possui controlo sobre o Endereço IP, através do pré-acordo sobre uma alteração a determinada informação contida numa página Web *online* identificada por um URI[12] que contém o Endereço IP;
- Obtenção de documentação sobre a atribuição do endereço de IP a partir da Internet *Assigned Numbers Authority* (IANA) ou a *Regional Internet Registry* (RIPE, APNIC, ARIN, AfriNIC, LACNIC).
- Realização de uma pesquisa sobre o endereço IP e, em seguida, verificação do controlo sobre o *Domain Name* resultante;

[10] Entidade que gere o registo de domínios de determinado país.
[11] Base de dados que permite a consulta de IP`s para consultar informação sobre o seu proprietário.
[12] Uniform Resource Identifier

- Utilização de qualquer outro método de confirmação (desde que providencie o mesmo nível de confiança que os métodos de verificação referidos anteriormente), sendo que a EC preservará o registo que servirá de evidência da confirmação de que o Requerente é o responsável do Endereço IP ou tem controlo sobre o Endereço IP.

7 Conclusão

Este documento define a Política de Certificado do certificado de Servidor Web, utilizada pela EC da MULTICERT no suporte à sua atividade de certificação digital. A hierarquia de confiança da Entidade de Certificação MULTICERT:

- Fornece uma hierarquia de confiança, que promoverá a segurança na comunicação eletrónica via web;
- 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.

8 Referências Bibliográficas

- ITU-T *Recommendation* X.509. 1997, (1997 E): *Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.*
- NIST FIPS PUB 180-2. 2002, *Secure Hash Standard, U. S. Department of Commerce, Technology Administration, National Institute of Standards and Technology.*
- RFC 3279. 2002, *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*
- RFC 5280. 2008, Internet X.509 *Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*
- Regulamento (UE) nº 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 - relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE;
- CA/Browser Forum – Baseline Requirements, v1.3.3;
- ETSI EN 319 411-2 v2.1.1 (2016-02) – *Electronic Signatures and Infrastructures (ESI);Policy and security requirements for Trust Service Providers issuing certificates ; Part 2 : Requirements for trust service providrs issuing EU qualified certificates;*
- ETSI EN 319 412-5 v2.1.1 (2016-02) - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;*
- ETSI EN 319 412-4 V1.1.1 (2016-02) - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates;*