multicert
Engineering for digital security

SSL Certificate Policy

Policies

MULTICERT_PJ.CA3_24.1.2_0009_pt.pdf

CA Identification: MULTICERT CA 001

Rating: Public

Version: 3.0

Date: 24/10/2017

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

Document Identification: MULTICERT_PJ.CA3_24.1.2_0009_pt.pdf

Keywords:

Document Type: Policies

Title: SSL Certificate Policy

Original Language: Portuguese

Language of Publication: Portuguese

Rating: Public

Date: 18/02/2016

Current Version: 1.0

CA Identification: MULTICERT CA 001

Version History

Version Nº	Date	Details	Author(s)
1.0	13/01/2014	Approved Version	MULTICERT S.A.
1.1-1.7	12/2/2016	Revision	MULTICERT S.A.
2.0	12/03/2016	Approved Version	MULTICERT S.A.
2.1	24/10/2017	Revision	MULTICERT S.A.
3.0	24/10/2017	Approved Version	MULTICERT S.A.

Related Documents

Document ID	Details	Author(s)
MULTICERT_PJ.CA3_24.1.1_0001_pt.pdf	Certification Practices Statement	MULTICERT S.A

Executive Abstract

Resulting from the implementation of several public and private programs to promote information and communication technologies and introduce new relationship processes into society – between citizens, companies, non-governmental organizations and the State – in order to strengthen the information society, eGovernment and electronic trade, the digital certificates issued by the Certification Authority MULTICERT, accredited by the National Security Authority (as provided by European and national laws), supply the necessary mechanisms for strong digital authentication of the identity of a web server.

The infrastructure of MULTICERT Certification Authority provides a hierarchy of trust which promotes electronic security, as well as a structure of electronic trust, which enables carrying out secure communication of information via the web, namely with regard to the server authentication, the ownership of an Internet domain and the integrity and confidentiality of the transacted information.

Who may access a web server identified with a digital certificate by MULTICERT is assured of the identity of the recipient of the communication (i.e., is sure that he/she is communicating with the intended website and not other website or entity). This verification is guaranteed by the signature of the certificate with the private key of the Certification Authority.

MULTICERT Certification Authority is duly accredited by the National Security Authority (http://www.gns.gov.pt/trusted-lists.aspx),with accreditation number ANS-ECC-7/2014,(as provided by European and national laws, this way being legally empowered to issue all types of digital certificates, namely qualified digital certificates (digital certificates with the highest degree of security provided by law).

This document defines the Certificate Policy in use for issuing the SSL digital certificate.

Table of Contents

Introduction

1.1 Purposes of the document

The purpose of this document is to present the profile of the SSL certificate issued by MULTICERT Certification Authority.

1.2 Target Public

This document shall be read by:

- Human resources assigned to MULTICERT CA's Working Group,
- Third parties in charge of auditing MULTICERT CA,
- Public in general.

1.3 Document Structure

It is assumed that the reader knows the concepts of cryptography, public key infrastructure and electronic signature. Shall this not be the case, it is recommended that deeper knowledge as to the previously mentioned concepts and topics be attained before continuing to read this document.

This document complements the Certification Practices Statement of MULTICERT CA, being assumed that the reader has read its full content before starting to read this document.

2 General Context

This document has the purpose of defining a set of features which define the profile of the Web Server Certificates issued by MULTICERT CA, thus assuring their reliability. It is not meant to name legal rules or obligations, but to inform. Therefore, this document is intended to be simple, straightforward, and understood by a wide public.
The Certificates issued by MULTICERT CA contain a reference to this Certificate Policy, so that the relying parties and other interested entities or individuals may find information on the certificate and the policies of the entity which issued it.

2.1 Overview

This CP meets and complements the requirements imposed by the Certification Practices Statement of MULTICERT CA.

2.2 Designation and Identification of the Document

This document is a Certificate Policy of the Web Server Certificate. The CP is represented in a certificate by a unique number called “object identifier” (OID). The value of the OID associated with this document is “2.16.620.1.1.1.2.4.0.1.8”.

This document is identified by the data included in the following table:

DOCUMENT INFORMATION	
Document Version	Version 3.0
Document State	Approved
OID	1.3.6.1.4.1.25070.1.1.1.0.1.5
Issuing Date	24/07/2017
Validity	1 Year
Location	http://pki.multicert.com/pol/cp/webserver.html

3 Identification and Authentication

3.1 Naming

The naming follows the convention determined by the CPS of MULTICERT CA.

3.1.1 Types of Names

The Web Server Certificate is identified by a unique name (DN – Distinguished Name), that complies with X.500 standard.

The Distinguished Name of the certificate by MULTICERT CA consists of the following components:

Attribute	Code	Value
Country	C	<Country>
LocalityName	L	<Locality where the Organization is affiliated>
Organization	O	<Legal name of the Organization>
Organization Unit	OU	Certificado SSL
Organization Unit	OU	<Another name of the holder organization. >
Common Name	CN	<*full qualified domain name* of the Web Server>

3.2 Use of the certificate and key pair by the titleholder

MULTICERT CA is the issuer of the Web Server Certificate, this being issued for the web server whose Qualified Domain Name is stated in the field "*CommonName*". It is used in the authentication process and the establishment of encrypted / private channels, according to the SSL/TLS protocol between a client web application and the web server.

The security in the identification of the server is achieved by sending a "challenge" through it, signed with its private key. The browser, by checking this "challenge" with the corresponding public key, identifies the web server, which in the physical world is equivalent to showing the Identity Card or Passport of an individual.

4 Certificate Profile

4.1 Certificate Profile

The users of a public key have to trust that the associated private key is held by the correct remote titleholder (person or system) with which they will use the encipher mechanism or digital signature. The trust is obtained through the use of X.509 v3 digital certificates, which are a data structure that makes the connection between the public key and its titleholder. This connection is stated through the digital signature of each certificate by a trusted CE. The CE may base this statement on technical means (for example, proof of the possession of the private key through a challenge-response protocol), on the presentation of the private key or on the registration made by the titleholder.

A certificate has a limited validity period, indicated in its content and signed by the CE. Since the signature of the certificate and its validity may be independently verified by any software that uses certificates, the certificates may be distributed through communication lines and public systems, and may also be stored in any type of storage units.

The user of a security system that requires the knowledge of the user's public key usually has to obtain and validate the certificate holding that key. If the service does not hold a trustful copy of the public key from the CE that signed the certificate, as well as the name of the CE and related information (such as the validity period), then there may be required an additional certificate to obtain a public key from the CE and validate the user's public key. Generally, to validate the public key from a user, there may be needed a network of multiple certificates, including the public key certificate of the user signed by a CE, and zero or more additional certificates from CEs signed by other CEs.

The profile of the web server certificate is compliant with:

- ITU.T recommendationX.509[1] ;
- RFC 5280[2] and
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum, v1.3.0

4.1.1 Version Number

The *"version"* certificate field describes the version used in encoding the certificate. In this profile, the version used is 3 (three).

[1] cf. ITU-T Recommendation X.509. 1997, (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.

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

4.1.2 Certificates Extensions

The components and extensions defined for X.509 v3 certificates provide methods for associating additional attributes to users or public keys, as well as for managing the certification hierarchy.

Certificate Component		Section in RFC 3280	Value	Field Type	Comments
tbsCertificate	**Version**	4.1.2.1	v3	m	Certificate version according to the standard X.509
	Serial Number	4.1.2.2	<assigned by the CA to each certificate>	m	
	Signature	4.1.2.3	1.2.840.113549.1.1.5	m	Value MUST match the OID in *signatureAlgorithm* (below)
	Issuer	4.1.2.4		m	
	Country (C)		"PT"		Holder Country
	Organization (O)		"MULTICERT - Serviços de Certificação Eletrónica S.A."		Formal designation of the holder's organization
	Organization Unit (OU)		"Accredited Certifying Entity"		Another name of the holder organization.
	Common Name (CN)		"MULTICERT – Certification Authority <nnn>"		Name of the organization – Name of the CA
	Validity	4.1.2.5		m	Validity of the certificate MUST use UTC time scale until 2049, from then on using GeneralisedTime
	Not Before		<issuing date>		
	Not After		<issuing date + (1year or 2 years or 3 years)>		Validity of approximately 3 years and a month. Renewed (with generation of a new key pair) a month before its expiration date.
	Subject	4.1.2.6		m	
	Country (C)		<Country>	m	Home country of the Organization
	Locality Name(L)		<Locality>	m	Locality where the Organization is affiliated

	Organization (O)		<Organization Name>	m	Organization Name according to the Commercial Register
	Organization Unit (OU)		Certificado SSL/TLS	m	Certificate designation type
	Organization Unit (OU)) (		<Other organization name> <TIN of the Organization>	o	Another name of the holder organization
	Common Name (CN)		<full qualified domain name of Web server or IP Address>	m	
	Subject Public Key Info	4.1.2.7		m	Used to hold the public key and identify the algorithm with which the key is used (e.g., RSA, DSA or Diffie-Hellman).
	Algorithm		1.2.840.113549.1.1.1		The rsaEncryption OID identifies RSA public keys. pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 } rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1} The rsaEncryption OID shall be used in the field algorithm with a value of type AlgorithmIdentifier. The parameters of the field MUST have ASN. 1type NULL for this algorithm identifier.[3]
	subjectPublicKey		<Public key with modulus n of 2048 bits>		
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		o	

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

	keyIdentifier		<The *key Identifier* is composed of the 160-bit SHA-1 hash of the value of the BIT STRING *subjectKeydentifier* of the issuer's certificate (excluding tag, length, and number of unused bits)>	m	
	Subject Key Identifier	4.2.1.2	<The *key Identifier* is composed of the 160-bit SHA-1hash of the value of the *BIT STRING subjectPublicKey* (excluding *tag*, *length*, and number of unused bits)>	m	
	Key Usage	4.2.1.3		mc	This extension is marked CRITICAL. Check the certificate use type.
	Digital Signature		"1" selected		
	Non Repudiation		"0" selected		
	Key Encipherment		"1" selected		
	Data Encipherment		"1" selected		
	Key Agreement		"0" selected		
	Key Certificate Signature		"0" selected		
	CRL Signature		"0" selected		
	Encipher Only		"0" selected		
	Decipher Only		"0" selected		
	Certificate Policies	4.2.1.5		m	
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.7	m	Identifier of the Certification Practices Statement of MULTICERT CA.

	policyQualifiers		*policyQualifierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: pki.multicert.com/pol/cps/MULTICERT_PJ.CA3_24.1.1_0001_pt.pdf	o	OID Value: 1.3.6.1.5.5.7.2.1 (id-qt-cps PKIX CPS *Pointer Qualifier*) OID Description: "The cPSuri qualifier contains a pointer to the Certification Practices Statement, published by the CA. The pointer is in the form of a URI." (http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.1.html)
	policyIdentifier		1.3.6.1.4.1.2507.1.1.1.1.0.1.5	m	Identifier of the Web Server Certificate Policy (SSL)
	policyQualifiers		*policyQualifierID*: 1.3.6.1.5.5.7.2.2 *userNotice explicitText*: "Certificate issued in accordance with the Certificate Policy in pki.multicert.com/pol/cp/webserver.html	o	OID Value: 1.3.6.1.5.5.7.2.2 (id-qt-unotice) OID Description: "*User notice* is used to display to a relying party when a certificate is used." (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)} Certificate published according to the requirements of the CA/Browser Forum The OID indicates that the certificate contains verified information about the legal identity of the certificate holder.
	policyIdentifier		0.4.0.194112.1.4	m	OID Value: 0.4.0.194112.1.3[4], identifies that the certificate for web site authentication according to the qualified certificate defined in

[4] 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

					article 3 and 45 of Regulation (E) U) Nº. 910/2014 . {itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies
	Subject Alternative Name	4.2.1.7		m	
	GeneralName		DNS = <*full qualified domain name* of the Web server>	o	Maximum of 7 Domains
	IPAddress		IPAddress = <*IPAddress* of the Web Server>	o	Only external Domains
	rfc822name		rfc822name = <*email associated with the Web server*>	o	
	Basic Constraints	4.2.1.10		c	This extension is marked CRITICAL.
	CA		FALSE		
	PathLenConstraint		0		
	Extended Key Usage	4.2.1.13		m	
	KeyPurpose		Id-Kp-serverAuth		OID Description: server authentication:1.3.6.1.5.5.7.3.1
	KeyPurpose		Id-kp-clientAuth		OID Description: client authentication:1.3.6.1.5.5.7.3.2
	CRLDistributionPoints	4.2.1.14		m	
	distributionPoint		Ec2pki.multicert.com/crl/crl-mca002.crl	m	URL to access the CRL
	Freshest CRL	4.2.1.15			
	distributionPoint		crl.mca002_delta.crl	o	URL to access the Delta CRL
	Internet Certificate Extensions				
	Authority Information	4.2.2.1		m	

	Access				
	accessMethod		1.3.6.1.5.5.7.48.1	m	OID OCSP value: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp) OID Description: *Online Certificate Status Protocol*
	accessLocation		http://ocsp.multicert.com/ocsp	m	URL to access the OCSP
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	MUST contain the same algorithm identifier OID as the *signature* field in the sequence *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	<contains the digital signature issued by the CA>	m	By generating this signature, the CA certifies the binding between the public key and the titleholder (*subject*) of the certificate.

4.1.3 Algorithm OID

The "*signatureAlgorithm*" certificate field contains the OID for the cryptographic algorithm used by the CA to sign the certificate: 1.2.840.113549.1.1.11 (*sha-2WithRSAEncryption*[5])

4.1.4 Name Forms

As defined in section 2.1.

4.1.5 Name Constraints

To guarantee full interoperability between the applications that use digital certificates, it is advisable (not mandatory) to use only unaccented alphanumeric characters, space, underscore, minus sign and full stop ([a-z], [A-Z], [0-9], ' ', '_', '-', '.') in X.500 Directory entries.

4.1.6 Certificate Policy OID

The "*certificate policies*" extension contains a sequence of one or more informative terms about the policy, each consisting in a policy identifier and optional qualifiers.

The optional qualifiers ("*policyQualiflierID*: 1.3.6.1.5.5.7.2.1" and "*cPSuri*") point to the URI where the Certification Practices Statement with the OID identified by the "*policyIdentifier*" can be found. The optional qualifiers ("*policyQualiflierID*: 1.3.6.1.5.5.7.2.2" and "*userNotice explicitText*") point to the URI where the Certificate Policy with the OID identified by the policyIdentifier" can be found (i.e., this document).

The qualifier 0.4.0.194112.1.4 refers to Certificate Politic for qualified certificates authentication of web server, under the regulation EU nº 910/2014.

4.1.7 Usage of Policy Constraints extension

Nothing to remark.

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

4.1.8 Policy qualifier sytanx and semantics

The "*certificate policies*" extension contains a type of policy qualifier to be used by the certificate issuers and the writers of the certificate policy. The type of qualifier is the "*CPSuri*", which contains a pointer, in the form of URI, to the Certification Practices Statement published by the CA; and the "*userNotice explicitText*", which contains a pointer, in the form of URI, to the Certificate Policy.

4.1.9 Processing semantics for the Certificate Policies critical extension

Nothing to remark.

5 Domain validation

5.1 Authorization by the Responsible of the *Domain Name*

The CA confirms that, to date of issuance of the certificate, the certificate applicant is the *Domain Name* responsible or has control over the *Full Qualified Domain Name*, through following procedures:

- Confirmation that the certificate applicant has the *Domain Name* registration directly at the domain registrar[6];
- Direct communication with the responsible for the *Domain Name*, using the address, email or phone number provided by the domain registrar;
- Direct communication with the responsible for the *Domain Name* using the contact information listed in the file "*registrant*", "*technical*" or "*administrative*" of WHOIS database[7];
- Communication with the domain administrator using the email address created with the prefix "*admin*", "*administrator*", "*webmaster*", "*hostmaster*" or "*postmaster*", followed by the "@" symbol and the *Domain Name*;
- Trust in a Domain Authorization Document;
- Statement by the Applicant that he/she has practical control over the *Fully Qualified Domain Name*, by pre-agreement on an amendment to certain information contained in an online Web page identified by a URI[8] that contains the *Fully Qualified Domain Name*; or
- Using any other method of confirmation (as long as it provides the same level of reliability of the verification methods mentioned above), and the CA will keep the record as evidence to confirm that the Applicant is responsible for the *Domain Name* or has control over the *Fully Qualified Domain Name*.

5.2 Authorization for a IP Address

For each IP address listed in the certificate, the CA confirms that, to date of issuance of the certificate, the Applicant has control over the IP address, through following procedures:

- Statement by the Applicant that he/she has practical control over the *Fully Qualified Domain Name*, by pre-agreement on an amendment to certain information contained in an online Web page identified by a URIthat contains the *Fully Qualified Domain Name*;

[6]Entity which manages the domain registration of a certain country.
[7]Database which allows the IP query to access information about its owner.
[8]Uniform Resource Identifier

- Obtaining information about the assignment of the IP address from the *Internet Assigned Numbers Authority* (IANA) or *Regional Internet Registry* (RIPE, APNIC, ARIN, AfriNIC, LACNIC).
- Research on the IP address followed by verification of control over the resulting Domain Name;
- Using any other method of confirmation (as long as it provides the same level of reliability of the verification methods mentioned above), and the CA will keep the record as evidence to confirm that the Applicant is responsible for the *Domain Name* or has control over the *Fully Qualified Domain Name*

Conclusion

This document defines the certificate policy of a web server certificate, used by MULTICERT CA in the support to its activity of digital certification. The hierarchy of trust of MULTICERT Certification Authority:

- Supplies a hierarchy of trust, which will promote the security in electronic communication via the web;
- Provides the conduction of safe electronic transactions, strong authentication, a means to digitally sign transactions or information and electronic documents, ensuring its authorship, integrity and non-repudiation, and ensuring the confidentiality of the transactions or information.

Bibliographic References

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*.

6 Approval of the Executive Board

Renato Isaias Rodrigues Portela

Digitally signed by Renato Isaias Rodrigues Portela
Date: 2017.10.24 19:30:39 +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 08:39:38 +01'00'