TSL Signer Certificate Policy

Policy

MULTICERT_PJ.CA3_24.1.2_0007_en

Project Identification: MULTICERT CA03

CA Identification: MULTICERT CA

Rating: Public

Version: 2.0

Date: 12/09/2010

MULTICERT, Serviços de Certificação Electrónica, S.A.,
Polo Tecnológico de Lisboa, Sala 101, CID - Lote 1, 1600-546 Lisboa, Portugal
Phone: +351 217 123 010 Facsimile: +351 217 123 011

Document Identification: MULTICERT_PJ.CA3_24.1.2_0007_en

Keywords: EPC TSL signer certificate policy profile

Document Type: Policy

Title: TSL Signer Certificate Policy

Original Language: English

Language of Publication: English

Rating: Public

Date: 12/09/2010

Current Version: 2.0

Project Identification: MULTICERT CA03

CA Identification: MULTICERT CA

Client: MULTICERT S.A.

Version History

Version Number	Date	Details	Author(s)
1.0	06/09/2010	Initial version	Nuno Ponte
2.0	12/09/2012	Versão Aprovada	José Miranda/João Cerdeira

Related Documents

Document Identification	Details	Author(s)

Executive Abstract

This document describes the Certificate Policy (CP) in use by MULTICERT's Certification Authority (CA) for the issuance of Trust-service Status Lists (TSL) signer certificates.

The provisions of this policy are in accordance and/or complement the Certification Practice Statement (CPS) of MULTICERT CA.

The format and semantics of the TSL signer certificates detailed in this document are in accordance with the recommendations of ETSI 102 231.

Table of Contents

1 Introduction

1.1 Goals

This document refers to the Certificate Profile of the TSL Signer certificate and describes its format and semantics.

1.2 Intended Readers

This document should be read by:

- MULTICERT S.A.,
- Human resources assigned to any working group of the MULTICERT CA,
- Third parties in charge of auditing the MULTICERT CA,
- Relying parties processing certificates described in this Certificate Policy.

1.3 Document Structure

The first chapter details the TSL Signer certificate profile. The profiles include the mandatory and optional extensions, as specified in ETSI TS 102 231 (section 6.2) [1].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [2].

2 Certificate profile

Users of a public key shall be confident that the associated private key is owned by the correct remote subject (person or system) with which an encryption or digital signature mechanism will be used. This confidence is obtained through the use of public key X.509 v3 certificates [4], which are data structures that bind public key values to subjects. The binding is asserted by having a trusted CA digitally sign each certificate. The CA may base this assertion upon technical means (a.k.a., proof of possession through a challenge-response protocol), presentation of the private key, or on an assertion by the subject. A certificate has a limited valid lifetime which is indicated in its signed contents. Because a certificate's signature and timeliness can be independently checked by a certificate-using client, certificates can be distributed via untrusted communications and server systems, and can be cached in unsecured storage in certificate-using systems.

A user of a security service requiring knowledge of a public key generally needs to obtain and validate a certificate containing the required public key. If the public-key user does not already hold an assured copy of the public key of the CA that signed the certificate, the CA's name, and related information (such as the validity period or name constraints), then it might need an additional certificate to obtain that public key. In general, a chain of multiple certificates may be needed, comprising a certificate of the public key owner (the end entity) signed by one CA, and zero or more additional certificates of CAs signed by other CAs.

2.1 TSL Signer Certificate Profile

To meet the requirements of ETSI TS 102 231, MULTICERT CA MUST issue digital certificates that conform to the profile specified in Table 1. All security objects MUST be produced in DER format to preserve the integrity of the signatures within them.

The profile uses the following terminology for each of the fields in the X.509 certificate:

m – mandatory (the field MUST be present)

o – optional (the field MAY be present)

c – critical (the extension is marked critical, receiving applications MUST be able to process this extension).

Certificate Component	Section in RFC 5280	Value	Field Type	Comments
Version	4.1.2.1	3	m	
Serial Number	4.1.2.2	*assigned by the CA*	m	
Signature	4.1.2.3	`1.2.840.113549.1.1.11`	m	value MUST match the OID in signatureAlgorithm (below)
Issuer	4.1.2.4		m	
Country (C)		PT		PrintableString ASN.1 encoding
Organization (O)		`MULTICERT - Serviços de Certificação Electrónica S.A.`		UTF8String ASN.1 encoding
Organization Unit (OU)		`Entidade de Certificação Credenciada`		UTF8String ASN.1 encoding
Common Name (CN)		`MULTICERT - Entidade de Certificação 001`		UTF8String ASN.1 encoding
Validity	4.1.2.5		m	UTC time until 2049, from then on using GeneralisedTime
Not Before		*issuing date*		
Not After		*issuing date* + ***1900*** *days*		approximately five years and two months.
Subject	4.1.2.6		m	
Country (C)		PT		PrintableString ASN.1 encoding
Organization (O)		`MULTICERT - Serviços de Certificação Electrónica S.A.`		UTF8String ASN.1 encoding
Organization Unit (OU)		`TSL Services`		UTF8String ASN.1 encoding
Serial Number (SN)		*3-digit sequence number starting in* ***001***		PrintableString ASN.1 encoding

Common Name (CN)		EPC e-Mandates e-Operating Model TSL Service		UTF8String ASN.1 encoding
Subject Public Key Info	4.1.2.7		m	holds the public key and identify the algorithm with which the key is used (e.g., RSA)
algorithm		1.2.840.113549.1.1.1		corresponds to rsaEncryption. The parameters field MUST have ASN.1 type NULL for this algorithm identifier.
subjectPublicKey		*RSA key with modulus n of **2048** bits*		
X.509v3 Extensions	4.1.2.9		m	
Authority Key Identifier	4.2.1.1		m	
keyIdentifier		7f 33 72 7f 4c da 34 c8 0e a7 75 cb 2e 83 98 1b 06 b8 a6 90	m	same as the subject key identifier value of the issuer's certificate
Subject Key Identifier	4.2.1.2		m	160-bit SHA-1 hash of the subject public key BIT STRING value (excluding tag, length, and number of unused bits)
Key Usage	4.2.1.3		mc	this extension is marked CRITICAL
Digital Signature		1		
Non Repudiation		0		
Key Encipherment		0		
Data Encipherment		0		
Key Agreement		0		
Key Certificate Signature		0		

CRL Signature		0		
Encipher Only		0		
Decipher Only		0		
Certificate Policies	4.2.1.4		m	
policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.7	m	MULTICERT CA Certificate Practice Statement
policyQualifiers		policyQualifierID: **1.3.6.1.5.5.7.2.1** cPSuri: **http://pki.multicert.com/pol/cps/MULTICERT_CA.html**	m	CPS Pointer Qualifier
policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.1.7	m	TSL Signing Certificate Policy OID
policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.2 userNotice explicitText: Certificate issued in accordance with the Certificate Policy in http://pki.multicert.com/pol/cp/tsl.htm	m	the user notice is recommended to be displayed to a relying party when the certificate is used.
Basic Constraints	4.2.1.10		c	this extension is marked CRITICAL
CA		FALSE		
Extended Key Usage	4.2.1.12		m	
keyPurposeID		0.4.0.2231.3.0		id-tsl-kp-tslSigning,, as in ETSI TS 102 231.
CRLDistributionPoints	4.2.1.13		m	
distributionPoint		http://pki.multicert.comt/crl/crl001.crl		
Freshest CRL	4.2.1.15		m	

distributionPoint		http://pki.multicert.comt/crl/crl001_delta.crl		
Internet Certificate Extensions				
Authority Information Access	4.2.2.1		m	
accessMethod		1.3.6.1.5.5.7.48.1	m	Online Certificate Status Protocol (OCSP)
accessLocation		http://ocsp.multicert.com/ocsp	m	
Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	corresponds to sha-256WithRSAEncryption
Signature Value	4.1.1.3	*digital signature issued by the CA*	m	by imprinting this signature, the CA certifies the binding between the public key material and the subject of the certificate.

Table 1 - TSL Signer Certificate Profile

Bibliography

ID	Document Number	Title	Issued by
[1]	TS 102 231	Provision of harmonized Trust-service status information, version 3.1.2	ETSI
[2]	RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	IETF
[3]	RFC 5280	Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile	IETF
[4]	X.509	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks	ITU-T

[Assinatura Qualificada] João António Figueira Cerdeira

Digitally signed by [Assinatura Qualificada] João António Figueira Cerdeira
DN: c=PT, o=MULTICERT - Serviços de Certificação Electrónica S.A., ou=Certificado para pessoa singular - Assinatura Qualificada, sn=Figueira Cerdeira, givenName=João António, serialNumber=11401790, cn=[Assinatura Qualificada] João António Figueira Cerdeira
Date: 2012.09.28 11:07:30 +01'00'