multicert

Engineering for digital security

PKI Disclosure Statement

Policy

MULTICERT_PJ.CA3_24.1_0001_en

Project Identification: PKI MULTICERT

CA Identification: PKI MULTICERT

Rating: Public

Version: 1.0

Date: 10/07/2017

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_0001_en

Keywords: keyword

Document Type: Policy

Title: PKI Disclosure Statement

Original Language: Portuguese

Language of Publication: English

Rating: Public

Date: 10/07/2017

Current Version: 1.0

Project Identification: PKI MULTICERT

CA Identification: PKI MULTICERT

Client: ---

Version History

Version Nº	Date	Details	Author(s)
1.0	10/07/2017	Appoved version (equivalent version in portuguese language 3.0)	MULTICERT

Related Documents

Document ID	Details	Author(s)
MULTICERT_PJ.CA3_24.1.1_0001_pt.doc	Declaração de Práticas de Certificação	MULTICERT
MULTICERT_PJ.CA3_24.1.2_0002_pt.doc	Política de Certificado de Assinatura Digital Qualificada	MULTICERT
MULTICERT_PJ.CA3_24.1.2_0009_pt	Política de Certificado de Servidor Web	MULTICERT

Executive Abstract

This document was created in accordance with the standard "ETSI EN 319 411-1 - Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, Annex A.

This document is a PKI Disclosure Statement, or PDS document, does not constitute a Certificate Policy under which the certificates issued by MULTICERT CA. For this purpose, the Certificate Policies and Certification Practices Policy should be consulted in http://pki.multicert.com.

Renato Isaias Rodrigues Portela
Digitally signed by Renato Isaias Rodrigues Portela
Date: 2017.07.24 12:15:19 +01'00'

[Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A.
Digitally signed by [Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A.
Date: 2017.07.24 16:15:44 +02'00'

Table of Contents

PKI Disclosure Statement 1
Executive Abstract 3
Table of Contents 4
Introduction 5
1 Statement of Principles Disclosure 6
2 Certification Authority Contacts 6
3 Certificate type, validation procedures and usage 6
4 Reliance limits 7
5 Obligation of Subscribers 8
6 Certificate status checking obligations of relying parties 9
7 Limited warranty and disclaimer/Limitation of liability 9
8 Applicable agreements, CPS, CP 10
9 Privacy policy 10
10 Refund policy 11
11 Applicable law, complaints and dispute resolution 11
12 Repository, Audit and Security Normatives 11

Introduction

The purpose is summarize a set of practices and data for the issuance and validation of certificates, and for the assurance of 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, including people with no technical or legal knowledge. Together with the related CP establishes the features described in the Certification Practice Statement of the Public Key Infrastructure of MULTICERT Certification Authority.

MULTICERT Certification Authority is duly registered in the National Security Authority (http://www.gns.gov.pt/trusted-lists.aspx), with credential number ANS-ECC-7/2014 in 20/06/2014, 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).

Target Public

This document shall be read by:

- Certificate holders issued by the MULTICERT Certification Authority

Document Structure

This document is divided into 12 chapters, in accordance with the standard "ETSI EN 319 411-1 - Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, Annex A.

1 Statement of Principles Disclosure

MULTICERT discloses to all its customers and prospective parties the terms and conditions of use of its digital certification services in accessible and easy-to-understand language. This document should not be understood as a summary of all the practices and policies followed by MULTICERT CA, but rather of a few more important points, so the reading of this document should be complemented by a reading of the Certification Practice Statement available at https://pki.multicert.com/index.html.

2 Certification Authority Contacts

MULTICERT, Serviços de Certificação Electrónica S.A.
Lagoas Park, Edifício 3, Piso 3,
2740-266 Porto Salvo
Oeiras - Portugal
Phone Number: +351 217 123 010
Fax: +351 217 123 011
Email: pki.documentacao@multicert.com

3 Certificate type, validation procedures and usage

The MULTICERT CA issues the following types of digital certificates:

- **Qualified Certificates**
  - **Signature for natural persons** (X.509 Format) - The electronic signature is the only legally accepted means of signing electronic documents. With the digital certificate of qualified signature, the holder can sign electronic mail, electronic documents and even make electronic transactions. By using the digital certificate of qualified signature, the holder guarantees the integrity of the contents, authenticity of its signature and non-repudiation, and cannot deny that it has signed certain content. In this format, MULTICERT offers the following types of certificates:
    - **Particular** - Certificate issued that includes the name of its holder, which will be used to sign documents
    - **Quality** - Certificate with the same characteristics of the Particular, but with a quality attribute associated with an entity/organization (eg Physician, Engineer, Commercial Director, Administrator, etc.).
    - **Representation** - Certificate with the same characteristics of the Particular, but with an attribute in which assigns to the holder the effects of representation of an Organization. These powers of representation are delegated or conferred by the legal representatives of the organization.

- **Signature for legal person** - Electronic Seal (X.509 Format) - Certificate issued to the Organization, ie the certificate holder is a legal person. This Certificate can be used, for example, for electronic invoice signing (large volume issuance with added security), electronic statement statements, electronic declarations, certificates and other types of documents issued online by public entities;
- **Website Authentication** (X.509 Format) - A digital certificate whose purpose is to guarantee the authenticity of a website, the ownership of a domain or the confidentiality of the information transacted;

– **Advanced Certificate -** Certificates issued to individuals and professionals, allowing the electronic signature of documents (without probative value) in a safe and unequivocal electronic identification of a person;

– **Certificates of Application -** Certificates used for document signing, for identification of VPNs or for other types of services.

All certificates issued by MULTICERT CA can be verified through the Online Certificate Status Protocol service (OCSP) and/or the LRC (Certificate Revocation Lists) issued for each case and available at https://pki.multicert.com/index.html.

The validation procedures used for the purpose of issuing qualified digital certificates follow the "face-to-face" or equivalent methods as described in chapter 3.2 of the Certification Practice Statement and their Certificate Policies.

The validation methods used in the other types of certificates do not imply the use of the "face-to-face" method or equivalent and are described in chapter 4 of their Certificate Policies.

4 Reliance limits

The use of certificates issued to the holders must comply with the one described in the respective certificate policies.

Certificates issued by MULTICERT CA are also used by the Trusted Parties to verify the trust chain of a certificate issued under MULTICERT CA, as well as to guarantee the authenticity and identity of the issuer of a digital signature generated by the private key corresponding to the public key contained Certificate issued under MULTICERT CA.

Certificates may be used in other contexts only to the extent permitted by applicable law. Certificates issued by MULTICERT CA shall not be used for any function outside the scope of the uses described above.

The services offered by MULTICERT CA have not been designed and are not authorized to be used in high risk activities or that require a faultless activity, such as those related to the operation of hospital, nuclear, air traffic control, control Railroad traffic, or any other activity where a failure could lead to death, personal injury or serious damage to the environment.

5 Obligation of Subscribers

Certificate holders will use their private key only for the purpose for which they are intended (as established in the "*keyUsage*" certificate field) and always for legal purposes.

Its use is only allowed:

a) To whom is designated in the "Subject" field of the certificate and,

b) As long as the certificate remains valid, or is in the Active state.

The holder can request the revocation of a certain certificate, if there is knowledge or suspicion of commitment of the holder's private key or any other act that recommends this action. The Certification Body shall keep all documentation used to verify the identity and authenticity of the entity requesting revocation.

A certificate may be revoked for one of the following reasons:

- Commitment or suspected compromise of the private key or password to access the private key (example: signature PIN);
- Loss of private key;
- Serious inaccuracies in the data provided;
- Commitment or suspected compromise of the private key of the MULTICERT CA or Top Certification Authority (Multicert Root Certification Authority and/or Baltimore CyberTrust Root);
- Loss, destruction or deterioration of the private key support device (eg cryptographic token/support);
- Revocation of the certificate of the MULTICERT CA or the Top Certification Authority (Multicert Root Certification Authority and/or Baltimore CyberTrust Root);
- Failure by the MULTICERT CA or holder of the expected responsibilities;
- where there are credible reasons why certification services may have been compromised in such a way as to call into question the reliability of the certificates;
- By judicial or administrative resolution.

When using the certificate and public key, the following conditions must be met:

a) Be aware of and understand the use and functionality provided by public key cryptography and certificates.

b) Be responsible for its correct use;

c) Read and understand the terms and conditions described in the Certification Policies and Practices;

d) Verify the certificates (validation of trust chains) and Certificate Revocation Lists with special attention to their extensions marked as critical and purpose of the keys;

e) Trust the certificates, using them whenever they are valid.

Users of a public key must have confidence that the associated private key is held by the correct remote owner (person or system) with which they will use digital signature mechanisms. Trust is gained through the use of X.509 v3 digital certificates, which are data structures that link the public key and its holder. This link is affirmed through the digital signature of each certificate by a trusted Certification Authority (CA). The CA may base this assertion on technical means (eg proof of possession of the private key via a challenge-response protocol), on the presentation of the private key, or on the record made by the holder.

A certificate has a limited validity period, indicated in its content and signed by the Certification Authority. Because the certificate signature and its validity can be independently verified by any software that uses certificates, certificates can be distributed over communication lines and public systems, as well as can be stored in any type of storage units.

The user of a security service that requires knowledge of the user's public key usually needs to obtain and validate the certificate that contains that key. If the service does not have a trusted copy of the Certificate Authority (CA) public key that signed the certificate as well as the name of the CA and related information (such as the expiration date), then you may need an additional certificate to obtain the public key of the CA and validate the user's public key. In general, to validate a user's public key, a multi-certificate string may be required, including the certificate of the user's public key signed by a CA, the certificate that signed the certificate, and so on consecutively until it reaches the root CA.

6 Certificate status checking obligations of relying parties

Other parties who rely on the certificates issued by the MULTICERT CA shall:

- Verify the status of the certificate at the time of its use, using the OCSP and LRC mechanisms listed above, and assume responsibility for that verification;
- Comply with that specified in the Certificate Policies of the certificate in question;
- Use the certificate appropriately in accordance with the objectives of its issuance.

7 Limited warranty and disclaimer/Limitation of liability

The MULTICERT CA:

a) Shall answer for the damages caused to any person exercising its activity in accordance with applicable Regulations and to uses specifies in CPS

b) Shall answer for the damages caused to holders or third parties due to lack or delay of including in the consultation service the validity of the certificates, and revocation or suspension of a certificate, once it has knowledge of it;

c) Shall assume all liability before third parties for the actions of the holder for functions necessary to provide certification services;

d) The responsibility for the administration/management rests on an objective base and covers the risks that a private individual may undergo whenever this is a consequence of the normal or abnormal operation of its services;

e) Shall only answer for damages caused by misuse of the recognized certificate, when the limits of its possible use have not been clearly consigned on the certificate, in a clear recognized way by third parties;

f) Shall not respond when the holder exceeds the limits set out in the certificate as to their possible uses, in accordance with the conditions laid down and communicated to the holder.

g) It shall not respond if the recipient of the electronically signed documents does not prove them and takes into account the restrictions on the certificate as to their possible uses and,

h) Shall not assume any responsibility in case of loss or damage:

   ii) Of the services it provides, in case of war, natural disasters or any other case of force majeure;

   iii) Resulting from the use of certificates when these exceed the limits set forth in the Certificates Policy and corresponding CPS;

   iv) Resulting from the undue or fraudulent use of the certificates or CRLs issued by MULTICERT CA.

8 Applicable agreements, CPS, CP

Every applicable agreements, Certification Practice Statement and Certification Policy are available in: http://pki.multicert.com.

9 Privacy policy

MULTICERT has implemented measures that guarantee the privacy of personal data, in accordance with Portuguese legislation, ensuring that the information of the holder, contained in

the respective digital certificates is not published, and is processed in accordance with the Certificate Policies of the MULTICERT CA.

10 Refund policy

In accordance with the legislation in force.

11 Applicable law, complaints and dispute resolution

MULTICERT CA is based on the following legal documents:

- Regulation (EU) n.º 910/2014 of the European Parliament and of the Council, of 23 July 2014, in electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
- CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.3..

12 Repository, Audit and Security Normatives

All information regarding the MULTICERT CA is publicly available in the repository accessible at https://pki.multicert.com/.

All interventions made to the MULTICERT CA are scrutinized by internal auditors. The Certification Body of MULTICERT is audited by a Conformity Assessment Body (duly registered with the National Accreditation Body), which issues a Compliance Report (CAR) to be made available to the Supervisory Entity, who will evaluate the continuity of the provision of services reliable.

Compliance Audits shall be carried out at least every 12 months in order to confirm that MULTICERT CA, as a qualified provider of reliable services and the reliable services it provides, complies with the requirements established by Regulation 910/2014.

Qualified Digital Certificates issued by the MULTICERT CA comply with all the technical requirements defined in the following standards:

- CWA 14167- Cryptographic Module for CSP Signing Operations — Protection Profile;
- CWA 14169:2004 - Secure signature-creation devices "EAL 4+" ;

- ETSI EN 319 401 v2.1.1 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- 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 providers issuing EU qualified certificates;
- ETSI EN 319 412-1 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;
- ETSI EN 319 412-2 v2.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;
- ETSI EN 319 412-3 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons;
- ETSI EN 319 412-4 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates;
- ETSI EN 319 412-5 v2.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;
- ETSI EN 319 421 (v1.1.1) – Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps;
- ETSI EN 319 422 (v1.1.1) – Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles;
- Regulamento (UE) n.º 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 for the Issuance and Management of Publicly-Trusted Certificates, v.1.3.4.