multicert

Engineering for digital security

PKI Disclosure Statement

Policy

MULTICERT_PJ.CA3_24.1_0001_en

Project Identification: PKI MULTICERT
Rating: Public
Version: 3.0
Date: 31/03/2022

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: MULTICERT CA, PKI Disclosure Statement
Document Type: Policy
Title: PKI Disclosure Statement
Original Language: Portuguese
Language of Publication: English
Rating: Public
Date: 31/03/2022
Current Version: 3.0

Project Identification: PKI MULTICERT
CA Identification: PKI MULTICERT

Version History

Version Nº	Date	Details	Author(s)
1.0	20/10/2008	Initial draft	MULTICERT
1.1	23/01/2009	Content review	MULTICERT
1.2	25/03/2009	Content review	MULTICERT
1.3	25/03/2010	Content review	MULTICERT
2.0	12/01/2015	Content review	MULTICERT
2.1	18/06/2021	Content Review	MULTICERT
3.0	31/03/2022	Approval	MULTICERT

Related Documents

Document ID	Details	Author(s)
MULTICERT_PJ.ECRAIZ_427	Certification Practices Statement	MULTICERT
MULTICERT_PJ.ECRAIZ_426	Certificate Policy	MULTICERT
MULTICERT_PR.CQ_1732	General Terms and Conditions of Digital Certificate Issuance	MULTICERT

Summary

Introduction

This document was elaborated 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 intends to summarize, in a simple and accessible way, the characteristics described in the Certification Practices Statement (CPS) of the Public Key Infrastructure of Multicert Certification Authority (CA).

The PKI Disclosure Statement does not replace the Certification Practices Statement governing the certificates issued by Multicert`s Certification Authorities, so it must be complemented by reading the CPS available at https://pki.multicert.com.

1 TSP Contact Information

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: ca.forum@multicert.com
Email (PSD2 certificates): psd2@multicert.com
Website: https://www.multicert.com

2 Certificate Type, Validation Procedures and Usage

Multicert issues the following types of digital certificates:

Certificate	Appropriate Use
Qualified Digital Signature	Used for transactions that support digital signing of electronic forms, electronic documents, or electronic email. When The Serial Number field in the Subject Distinguished Name contains the prefix “TIN”, the certificate should be used for signing electronic invoices and request forms for same usage certificates. Issued for an individual, with or without an associated entity/organization. Guarantees the non-repudiation of signatures and integrity of signed content by individuals. This signature has the same probative legal value as a handwritten signature.
Qualified Electronic Seal	Used for transactions that support digital signing of electronic forms, electronic documents, or electronic email. Issued for a legal person/entity/organization. Guarantees the non-repudiation of signatures and integrity of signed content by entities/organizations.
Authentication	Used for specific electronic authentication transactions that support accessing web sites and other online content, electronic email, organizational systems, etc. Issued for an individual, with or without an associated entity/organization. Guarantee the authenticity of individuals (with or without an associated entity/organization).
Confidentiality	Used to cipher information to be communicated, such as electronic documents or email content. Issued for an individual, with or without an associated entity/organization. Guarantee the confidentiality of content.

Advanced Digital Signature	Used for transactions that support digital signing of electronic forms, electronic documents, or electronic email. Issued for an individual, with or without an associated entity/organization. Guarantees the non-repudiation of signatures and integrity of signed content by individuals. Used for specific electronic authentication transactions that support accessing web sites and other online content, electronic email, organizational systems, etc. Guarantee the authenticity of individuals (with or without an associated entity/organization). Used to cipher information to be communicated, such as electronic documents or email content. Guarantee the confidentiality of content.
PSD2 Qualified Electronic Seal	Used for transactions that support digital signing of electronic forms, electronic documents, or electronic email. Issued for a legal person/entity/organization. Guarantees the non-repudiation of signatures and integrity of signed content by entities/organizations.
PSD2 Qualified Website Authentication	Used to secure online communication where risks and consequences of data compromise are high. Associates a domain name with an organization. Issued for a legal person/entity/organization. Guarantee the authenticity and confidentiality.

The certificates issued by Multicert are always subject to validation by the individual and/or Organization to which the certificate will be issued, as well as other information contained in the certificate.

3 Reliance Limits

The certificates can be used for the purposes for which they were issued, as defined in chapter 2 of this document, and in the Certification Practices Statement and General Terms and Conditions of Digital Certificate Issuance available at https://pki.multicert.com.

The issued certificates can be used for access control/authentication, confidentiality, integrity, authenticity or non-repudiation, depending on the key usage and extended key usage existing in the certificate. The proper use of each type of certificate is described in the table in section 2 .

The certificates issued by Multicert shall not be used for any function outside the scope of the uses described above.

The event logs are maintained for a period of 7 years after the expiry date of the certificate to which they relate.

4 Obligations of Subscribers

The Subscriber must comply with the obligations clauses concerning him contained in the Digital Certificate Issuance Form, General Terms and Conditions of Digital Certificate Issuance, and Certification Practices Statement available at https://pki.multicert.com, in particular:

- Provide true information for issuing the certificate, as well as the required documentation in order to prove its veracity;
- Limit and adjust the use of the certificate in accordance with the purposes provided for in the Certificate Policy, General Terms and Conditions of Digital Certificate Issuance and Certification Practices Statement;
- Use the certificate`s private key only within the secure cryptographic device, when it is generated on such device;
- Immediately request the revocation of a certificate when one of the reasons for revocation listed in section 4.9 of the Certification Practices Statement occurs, namely:
    - Whenever there is compromise, suspected compromise, or loss of the certificate`s private key and/or password to access the private key (i.e. PIN);
    - When there is inaccurate certificate information or when there are changes that influence the certificate attributes.
- Refrain from using a private key from a certificate that has expired, suspended or revoked.

5 Certificate Status Checking Obligations of Relying Parties

Before trusting a certificate, the Relying Parties must:

- Limit the reliability of certificates to the permitted uses for them in accordance with the terms of the corresponding Certificate Policy and section 1.4 of the Certification Practices Statement;
- Verify the status of the certificate at the time of performing any operation based on it, using the OCSP and CRL mechanisms identified in the certificate, and assume the responsibility for that verification;
- Comply with the specified in the Certificate Policy and Certification Practices Statement;
- Notify any event or anomalous situation regarding the certificate, which may be considered as a reason for its revocation, using the means that Multicert indicates in its Certification Practices Statement.

6 Limited Warranty and Disclaimer / Limitation of Liability

The Multicert Certification Authority:

a) Respond for acts and omissions in the exercise of its activity in accordance with Article 15 of Decree-Law 12/2021;

b) Respond for damages caused to Subscribers or third parties due to the lack or delay in including a revoked or suspended certificate in the certificate validity consultation service, once it becomes aware of it;

c) Assumes all responsibility through third parties for the functions necessary for the provision of trust services, within the scope of action of Subscribers;

d) Its administration / management responsibility is based on an objective basis and covers all the risk that individuals suffer whenever this is a consequence of the normal or abnormal functioning of its services;

e) It is only liable for damages caused by the misuse of the recognized certificate, when the limits of possible use have not been recorded in the certificate, clearly recognized by third parties;

f) Does not respond when the Subscriber exceeds the limits set out in the certificate regarding its possible uses, in accordance with the conditions established and communicated to the Subscriber;

g) Does not respond if the recipient of electronically signed documents does not prove them and takes into account the restrictions contained in the certificate regarding their possible uses;

h) It assumes no responsibility in the event of loss or damage:

    i) Of the services provided, in case of war, natural disaster or any other reason of force majeure;

    ii) Resulting from the use of certificates when this use exceeds the limits established in the CPS and CP;

    iii) Resulting from the misuse or fraudulent use of certificates or CRL`s issued by the Multicert PKI CA`s.

7 Applicable Agreements, CPS, CP

All the applicable agreements and conditions, Certification Practices Statement and Certificate Policy are available at https://pki.multicert.com.

8 Privacy Policy

Multicert has implemented measures that guarantee the privacy of personal data, in accordance with Portuguese and European legislation.

The Privacy Policy is available at https://www.multicert.com/en/use-terms-and-policies/.

9 Refund Policy

In accordance with the legislation in force.

10 Applicable Law, Complaints and Dispute Resolution

Multicert, as an entity that provides trust services, such as digital certification services, complies with the requirements established in current portuguese and european legislation.

In case of dispute, the consumer may resort to an Alternative Dispute Resolution Entity. The official list of such entities is available on the Consumer website at www.consumidor.pt.

Without prejudice to the possibility of prior use of mediation, if no agreement is reached between the parties within the scope of such procedure, either party may appeal to the courts, being set as competent jurisdiction for the purpose the District Court of Lisbon.

11 TSP and Repository Licenses, Trust Marks, and Audit

The compliance of Multicert Certification Authorities is audited according to the European Regulation nº 910/2014 and the main standards ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2. Audits are carried out by independent external auditors, belonging to an accredited CAB (Conformity Assessment Body), whose method of conformity assessment is in accordance with EN ISO/IEC 17065, according to the profile of ETSI EN 319 403.

The results of the compliance audit are communicated to the Portuguese Supervisory Body (National Security Office), which confirms the inclusion of Multicert in the European Trusted List as required by European Regulation nº 910/2014. Multicert`s Certification Authorities can be consulted on the European Trusted List at https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/PT/5.

Approval

Nuno Ponte (Management Working Group)

[Assinatura Qualificada] Nuno Miguel Arieiro Rodrigues da Ponte

Digitally signed by [Assinatura Qualificada] Nuno Miguel Arieiro Rodrigues da Ponte
Date: 2022.04.08 17:13:42 +01'00'