DIGITALSIGN - CERTIFICADORA DIGITAL, SA.

PKI DISCLOSURE STATEMENT

VERSION 3.1 – 18/05/2022
[LANGUAGE: ENGLISH]

VERSION HISTORY

Date	*Edition nr*	*Content*
22/02/2012	1.0	Initial draft
01/07/2016	2.0	Adaptation to the Regulation (EU) n.º 910/2014
14/07/2016	2.1	Revision
18/10/2016	2.2	Revision
20/07/2017	2.3	Revision
22/12/2017	2.4	Revision
29/01/2018	2.5	Revision
27/01/2021	3.0	Review and publication subsequent to the creation of the CAs
18/05/2022	3.1	Revision

RELATED DOCUMENTS

Document Details	*Author(s)*
Certification Practices Statement	DigitalSign

AUTHORIZATIONS

Created by	*Approved by*
Digitally Signed By: ÁLVARO OLIVEIRA DE MATOS Signing Time: 2022/05/18 10:01:25 WEST +0100 Organization: DIGITALSIGN - CERTIFICADORA DIGITAL, SA Certificate Profile - Qualified Certificate - Member Entitlement - DIRETOR GERAL / GENERAL MANAGER Certificado Digital Qualificado Documento assinado eletronicamente. Esta assinatura eletrónica substitui a assinatura autógrafa na UE.	Digitally Signed By: FERNANDO AVELINO LEITE DOS SANTOS MOREIRA Signing Time: 2022/05/18 10:05:19 WEST +0100 Organization: DIGITALSIGN - CERTIFICADORA DIGITAL S.A. Certificate Profile - Qualified Certificate - Representative Entitlement - ASSINAR DOCUMENTOS E CONTRATOS Certificado Digital Qualificado Documento assinado eletronicamente. Esta assinatura eletrónica substitui a assinatura autógrafa na UE.

LEGAL NOTICE

Any question or request for information regarding the content of this document should be directed to suporte@digitalsign.pt.

CONTENT

1. Introduction 4
1.1. Overview 4
1.2. Document Name and Identification 4
2. Certification Authority Contacts 5
3. Certificate Types, Validation Procedures and Usage 5
4. Reliance Limits 6
5. Obligations of Subscribers 6
6. Certificate Status Checking Obligations of Relying Parties 6
7. Limitation of Liability 7
8. Applicable Agreements, CPS and CP 7
9. Privacy Policy 7
10. Applicable law 7
11. Audits and Security Normatives 7

1. INTRODUCTION

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

This PKI Disclosure Statement is not intended to replace a CP or CPS under which the certificates issued by EC DIGITALSIGN are governed. For that purpose, it should be consulted the Certification Practice Statement at https://pki.digitalsign.pt.

1.1. OVERVIEW

This document aims to summarize, in a simple and accessible way, the features described in the Certification Practice Statement of the Public Key Infrastructure of DigitalSign's Certification Authority "EC DIGITALSIGN".

EC DIGITALSIGN's infrastructure provides a hierarchy of trust, promoting safety and electronic trust for conducting secure electronic transactions, strong authentication, a way to electronically sign transactions or information and electronic documents, ensuring their authorship, integrity and non-repudiation, and ensuring the confidentiality of transactions or information.

1.2. DOCUMENT NAME AND IDENTIFICATION

This document is the PKI Disclosure Statement, and it's identified by the following information:

DOCUMENT INFORMATION	
Version/Edition	3.1
Date of Approval	18/05/2022
Expiration date	Not applicable
Location	https://pki.digitalsign.pt

2. CERTIFICATION AUTHORITY CONTACTS

DigitalSign – Certificadora Digital, SA.
Largo Padre Bernardino Ribeiro Fernandes, 26
4835-489 Nespereira – Guimarães
Portugal
Email: suporte@digitalsign.pt
Telefone: +351 253560650
Fax: +351 253560639

3. CERTIFICATE TYPES, VALIDATION PROCEDURES AND USAGE

EC DIGITALSIGN issues the following qualified certificate types (profiles):

- Profile INDIVIDUAL: This certificate profile aims to identify a natural person (individual).
- Profile PROFESSIONAL: This certificate profile aims to identify a natural person (individual), and their entitlement in the fulfillment of his/her profession. Usually this type of certificate is issued to members of professional associations, where the entitlement should be checked with his/her association.
- Profile MEMBER: This certificate profile aims to identify a natural person (individual), and the position or function that takes/plays in a particular organization.
- Profile ORGANIZATION: This certificate profile aims to identify a legal person. It is an electronic seal certificate that is intended solely to be used by a legal person. The electronic seal is not suitable to bind the legal person in the documents in which it is affixed, just as in the physical world a stamp / seal of an organization is not enough to bind that organization.
- Profile REPRESENTATIVE: This certificate profile aims to identify a natural person (individual), as legal representative or attorney of an organization, entitled to, solely, bind a legal person, with any limitations identified in the respective fields of the certificate.

The certificates identified above are stored in a Qualified Electronic Signature Creation Device. The validity can be checked through OCSP (Online Certificate Status Protocol) services, where applicable, and/or by consulting the CRL (Certificate Revocation List) available in:

- Certificates issued by EC "DigitalSign Qualified CA": (http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificate/LatestCRL.crl)
- Certificates issued by EC "DigitalSign Qualified CA – G2": (http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG2/LatestCRL.crl)
- Certificates issued by EC "DigitalSign Qualified CA – G3": (http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG3/LatestCRL.crl)
- Certificates issued by "DIGITALSIGN QUALIFIED CA G1": (https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl)
- Certificates issued by "DIGITALSIGN QUALIFIED CA V1": (https://qca-v1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAV1.crl)

4. RELIANCE LIMITS

The usage of issued certificates must comply to that described in the certificate policies published in the EC DIGITALSIGN's DPC, available for consultation at: https://pki.digitalsign.pt.
The certificates issued by EC DIGITALSIGN are qualified certificates, according to Portuguese and European Union legislation, and can be used in any application for qualified electronic signature or qualified electronic seal.

The certificate subscribers are properly identified by the unique name (distinguished name) of the certificate.

5. OBLIGATIONS OF SUBSCRIBERS

The usage of the private key associated to the certificate public key is only allowed when the subscriber agrees and accepts the subscriber agreement. The certificate and keys must be used according to the subscriber agreement.

Subscribers use their private key only for the purpose for which they are intended (as set out in the "keyUsage") and always for lawful purposes.

Subscribers must protect their private key from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate.

Subscriber must request the revocation of a particular certificate, as soon as there is knowledge or suspicion of the private key compromise or any other act that recommends this action.

6. CERTIFICATE STATUS CHECKING OBLIGATIONS OF RELYING PARTIES

Before any act of trust, relying parties should verify:

- The appropriateness of the use of the certificate for any purpose, and determine that the certificate is in fact used for appropriate purposes that are not prohibited, or otherwise restricted by the EC DIGITALSIGN's CPS. DigitalSign is not responsible for assessing the proper adequacy of the certificate.
- If the certificate is being used as specified in the "*KeyUsage*" (eg.: if the digital signature is not enabled, then the certificate cannot be trusted to validate the signature of the subscriber).
- The status of the certificate and all the CA certification chain that issued the certificate. If any of the certificates in the certification chain is revoked, the relying party is solely responsible for assessing whether it is reasonable the trust in a digital signature, performed in prior to the revocation date. Such confidence is fully confident of the responsibility of the relying party.
- Be aware and understand the use and functionality provided by public key cryptography and certificates.
- Read and understand the terms and conditions outlined in policies and certification practices.

7. LIMITATION OF LIABILITY

EC DIGITALSIGN is not responsible for the improper use of digital certificates.

EC DIGITALSIGN is not responsible for any use of digital certificates not listed in the CPS.

The use of issued digital certificates and the protection of private/public key is the sole responsibility of its owner.

8. APPLICABLE AGREEMENTS, CPS AND CP

Every applicable agreements, Certification Practice Statement and Certification Policy are available at: https://pki.digitalsign.pt.

9. PRIVACY POLICY

Subscriber information included in their digital certificates is not published and is processed according to the certification policy of EC DIGITALSIGN.

10. APPLICABLE LAW

EC DIGITALSIGN's public key infrastructure 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, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
- Decreto-Lei n.º 88/2009, of 9 April 2009, making the fourth amendment to the Decreto-Lei n.º 290-D/99, of 2 August 1999, that approves the legal regime for electronic documents and digital signatures.
- Decreto Regulamentar n.º 25/2004, of 15 July 2004, that regulates the Decreto-Lei n.º 290-D/99, of 2 August 1999.

11. AUDITS AND SECURITY NORMATIVES

All interventions to the public key infrastructure of the EC DIGITALSIGN are audited by internal and external auditors, including the Autoridade Nacional de Segurança, as provided in applicable laws and regulations.

The Qualified Digital Certificates issued by EC DIGITALSIGN are in accordance to:

- CWA 14167 - Cryptographic Module for CSP Signing Operations - Protection Profile
- CWA 14169:2004 - Secure signature-creation devices "EAL 4+"
- ETSI EN 319 411 - Electronic Signatures and Infrastructures (ESI)
- ETSI EN 319 401 – General Policy Requirements for Trust Service Providers
- ETSI EN 319 412 - Certificate Profiles

- RFC 3647 - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework
- RFC 3280: Internet X.509 PKI - Certificate and CRL Profile
- CA/Browser Forum, Baseline Requirements, version 1.7.3
- CA/Browser Forum, Network and Certificate System Security Requirements, version 1.7