DIGITALSIGN - CERTIFICADORA DIGITAL, SA.

DECLARAÇÃO DE DIVULGAÇÃO DE PRINCÍPIOS

VERSÃO 3.1 – 18/05/2022

[IDIOMA: PORTUGUÊS]

HISTÓRICO DE VERSÕES

Data	*Edição n.º*	*Conteúdo*
22/02/2012	1.0	Redação Inicial
01/07/2016	2.0	Adaptação ao Regulamento (EU) n.º 910/2014
14/07/2016	2.1	Revisão
18/10/2016	2.2	Revisão
20/07/2017	2.3	Revisão
22/12/2017	2.4	Revisão
29/01/2018	2.5	Revisão
27/01/2021	3.0	Revisão e publicação após criação das ACs
18/05/2022	3.1	Revisão

DOCUMENTOS RELACIONADOS

Document Details	*Author(s)*
Declaração de Práticas de Certificação	DigitalSign

AUTORIZAÇÕES

Elaborado por	*Aprovado por*
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 10:05:20 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.

AVISO LEGAL

Qualquer dúvida ou pedido de informação relativamente ao conteúdo deste documento deverá ser dirigido a suporte@digitalsign.pt.

CONTEÚDO

1. INTRODUÇÃO

Este documento foi elaborado em conformidade com as especificações técnicas constantes do anexo B da norma "*ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements*".

A Declaração de Divulgação de Princípios da EC DIGITALSIGN não constitui uma Política de Certificados sob a qual se regem os certificados emitidos pela EC DIGITALSIGN. Para esse efeito deve ser consultada Declaração de Práticas de Certificação disponível em https://pki.digitalsign.pt.

1.1. CONTEXTUALIZAÇÃO

Este documento pretende resumir, de forma simples e acessível, as características descritas na Declaração de Políticas de Certificação da Infra-estrutura de Chave Pública da Entidade de Certificação da DigitalSign "EC DIGITALSIGN".

A infra-estrutura da EC DIGITALSIGN fornece uma hierarquia de confiança, que promove a segurança e a confiança eletrónica para a realização de transações eletrónicas seguras, a autenticação forte, um meio de assinar eletronicamente transações ou informações e documentos eletrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transações ou informação.

1.2. DESIGNAÇÃO E IDENTIFICAÇÃO DO DOCUMENTO

Este documento é a Declaração de Divulgação de princípios, e é identificado pela seguinte informação:

INFORMAÇÃO DO DOCUMENTO	
Versão/Edição	3.1
Data de Aprovação	18/05/2022
Data de Validade	Não aplicável
Localização	https://pki.digitalsign.pt

2. CONTATOS DA ENTIDADE DE CERTIFICAÇÃO

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. TIPOS DE CERTIFICADOS E PROCEDIMENTOS DE VALIDAÇÃO E UTILIZAÇÃO

A EC DIGITALSIGN emite os seguintes tipos (perfis) de certificados digitais qualificados:

- PERFIL INDIVIDUAL: Este perfil de certificado tem como objetivo identificar uma pessoa singular.
- PERFIL PROFISSIONAL: Este perfil de certificado tem como objetivo identificar uma pessoa singular, e a sua titularidade no desempenho da sua profissão. Normalmente este tipo de certificado é emitido a membros de Ordens Profissionais, onde a titularidade deverá ser verificada junto dessa Ordem.
- PERFIL MEMBRO: Este perfil de certificado tem como objetivo identificar uma pessoa singular, e o cargo ou função que ocupa/desempenha numa determinada organização.
- PERFIL ORGANIZAÇÃO: Este perfil de certificado tem como objetivo identificar uma pessoa coletiva. Trata-se de um certificado de selo eletrónico que se destina exclusivamente a ser usado por uma pessoa coletiva. O selo eletrónico não é adequado para vincular a pessoa coletiva nos documentos em que é aposto, da mesma forma que no mundo físico um carimbo/selo de uma organização não é suficiente para vincular a mesma.
- PERFIL REPRESENTAÇÃO: Este perfil de certificado tem como objetivo identificar uma pessoa singular, como legal representante ou procurador de uma organização, com poderes para obrigar sozinho uma pessoa coletiva, com eventuais limitações identificadas nos respetivos campos do certificado.

Os certificados identificados acima são disponibilizados em Dispositivo Qualificado de Criação de Assinatura Eletrónica, podendo verificar-se o seu estado de validade através do serviço OCSP (Online Certificate Status Protocol), quando aplicável, e/ou da consulta das LRC (Listas de Revogação de Certificados) disponíveis em:

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

4. LIMITAÇÕES DE CONFIANÇA NOS CERTIFICADOS

A utilização dos certificados emitidos deve obedecer ao descrito nas respetivas políticas de certificados publicadas na DPC da EC DIGITALSIGN, disponível para consulta em: https://pki.digitalsign.pt.

Os certificados digitais emitidos pela EC DIGITALSIGN são certificados digitais qualificados, nos termos do definido na Legislação Portuguesa e Europeia aplicável para o efeito, sendo

utilizado em qualquer aplicação para efeitos de assinatura eletrónica qualificada ou selo eletrónico qualificado.

O titular do certificado encontra-se devidamente identificado pelo nome único (distinguished name) do respetivo certificado.

5. RESPONSABILIDADES DOS TITULARES

O uso da chave privada correspondente à chave pública do certificado é apenas permitido quando o titular acordar e aceitar o contrato de subscrição do certificado. Este deve ser usado licitamente, de acordo com o contrato de subscrição da DigitalSign.

Os titulares de certificados utilizarão a sua chave privada apenas e só para o fim a que estas se destinam (conforme estabelecido no campo do certificado "keyUsage") e sempre com propósitos legais.

Os titulares devem proteger a sua chave privada contra o uso não autorizado, e devem suspender o uso da chave privada na sequência da expiração ou revogação do certificado.

O titular deve solicitar a revogação de um determinado certificado, havendo conhecimento ou suspeita de comprometimento da chave privada ou qualquer outro ato que recomende esta ação.

6. VERIFICAÇÃO DO ESTADO DO CERTIFICADO PELAS PARTES CONFIANTES

Antes de qualquer ato de confiança, as partes confiantes devem independentemente avaliar:

- A adequação do uso do certificado para quaisquer propósitos, e determinar que o certificado será, de facto, usado para propósitos adequados que não sejam proibidos, ou de outra forma restritos pela DPC da EC DIGITALSIGN. A DigitalSign não é responsável por avaliar a devida adequação do uso do certificado.
- Se o certificado está a ser usado de acordo com o especificado no campo "*KeyUsage*" incluído no certificado (ex.: se a assinatura digital não é ativada, então o certificado pode não ser confiável para validação da assinatura do titular).
- O estado do certificado e de todas as EC na cadeia de certificação que emitiu o certificado. Se qualquer um dos certificados da cadeia de certificação está revogado, a parte confiante é unicamente responsável por avaliar se é razoável a confiança numa assinatura digital, efetuada em data anterior à revogação. Tal confiança é totalmente da responsabilidade da parte confiante.
- Ter conhecimento e perceber a utilização e funcionalidades proporcionadas pela criptografia de chave pública e certificados.
- Ler e perceber os termos e as condições descritas nas politicas e práticas de certificação.

7. LIMITAÇÃO DE RESPONSABILIDADES

A EC DIGITALSIGN não se responsabiliza pelo uso indevido dos certificados digitais.

A EC DIGITALSIGN não se responsabiliza por qualquer utilização dos certificados digitais que não conste na DPC.

A utilização dos certificados digitais emitidos e a proteção das chaves privada/pública é da exclusiva responsabilidade do seu titular.

8. ACORDOS APLICÁVEIS, DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO E POLÍTICAS DE CERTIFICAÇÃO

Todos os acordos aplicáveis, Declarações de Política de Certificação e Políticas de Certificação encontram disponíveis em https://pki.digitalsign.pt.

9. POLÍTICA DE PRIVACIDADE

A informação do titular constante nos respetivos certificados digitais não se encontra publicada e é processada de acordo com a política de certificação da EC DIGITALSIGN.

10. LEGISLAÇÃO E NORMAS

A PKI da EC DIGITALSIGN baseia-se, essencialmente, nos seguintes documentos jurídicos:

- Regulamento (EU) 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.
- Decreto-Lei n.º 88/2009, de 9 de abril, que procede à quarta alteração ao Decreto-Lei n.º 290-D/99, de 2 de agosto, que estabelece o regime jurídico dos documentos eletrónicos e da assinatura digital.
- Decreto Regulamentar nº 25/2004 de 15 de Julho de 2004, que regulamenta o Decreto-Lei n.º 290-D/99, de 2 de agosto.

11. AUDITORIAS E NORMAS DE SEGURANÇA

Todas as intervenções realizadas à PKI da EC DIGITALSIGN são devidamente auditadas por auditores internos e externos, incluindo a Autoridade Nacional de Segurança, conforme disposto na legislação e normas aplicáveis.

Os Certificados Digitais Qualificados emitidos pela EC DIGITALSIGN cumprem todos os requisitos técnicos definidos nas seguintes normas:

- 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