Declaração de Divulgação da PKI

Política

MULTICERT_PJ.CA3_24.1_0001_pt

Identificação do Projeto: PKI da MULTICERT

Identificação da CA: PKI da MULTICERT

Nível de Acesso: Público

Versão: 4.0

Data: 01/07/2023

MULTICERT, Serviços de Certificação Electrónica, S.A.,
Rua Carlos Pinto Coelho, 13, 2720-092 Amadora - Portugal
Telefone: +351 217 123 010

Identificador do documento: MULTICERT_PJ.CA3_24.1_0001_pt

Palavras-chave: MULTICERT CA, EC MULTICERT, Declaração de Divulgação de Princípios

Tipologia documental: Política

Título: Declaração de Divulgação da PKI

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 01/07/2023

Versão atual: 4.0

Identificação do Projeto: PKI da MULTICERT

Identificação da CA: PKI da MULTICERT

Histórico de Versões

N.º de Versão	Data	Detalhes	Autor(es)
1.0	20/10/2008	Rascunho Inicial	MULTICERT
1.1	23/01/2009	Revisão de Conteúdos	MULTICERT
1.2	25/03/2009	Revisão de Conteúdos	MULTICERT
1.3	25/03/2010	Revisão de Conteúdos	MULTICERT
2.0	12/01/2015	Revisão de Conteúdos	MULTICERT
2.1	18/06/2021	Revisão de Conteúdos	MULTICERT
3.0	31/03/2022	Versão aprovada	MULTICERT
3.1	30/06/2023	Revisão de contactos	Multicert S.A.
4.0	01/07/2023	Aprovação	Multicert S.A.

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
MULTICERT_PJ.ECRAIZ_427_pt	Declaração de Práticas de Certificação	MULTICERT
MULTICERT_PJ.ECRAIZ_426_pt	Política de Certificado	MULTICERT
MULTICERT_PR.CQ_1732	Condições Gerais de Emissão de Certificado Digital	MULTICERT

Sumário

Introdução

Este documento foi elaborado de acordo com a norma ETSI EN 319 411-1 – Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, Anexo A.

Este documento pretende resumir, de forma simples e acessível, as características descritas na Declaração de Práticas de Certificação (DPC) da Infraestrutura de Chaves Públicas das Entidades de Certificação (EC) da Multicert. A Declaração de Divulgação da PKI não substitui a Declaração de Práticas de Certificação sob a qual se regem os certificados emitidos pelas Entidades de Certificação da Multicert, pelo que deve ser complementada com a leitura da DPC disponível em https://pki.multicert.com.

1 Informação de Contactos do TSP

MULTICERT – Serviços de Certificação Electrónica, S.A.
Rua Carlos Pinto Coelho, 13
2720-092 Amadora - Portugal
Telefone: +351 217 123 010
Email: ca.forum@multicert.com
Email (certificados PSD2): psd2@multicert.com
Website: https://www.multicert.com

2 Tipos de Certificados, Procedimentos de Validação e Utilização

A Multicert emite os seguintes tipos de certificados digitais:

Tipo de Certificado	Utilização Apropriada
Assinatura Digital Qualificada	Utilização para transações que suportam assinatura digital de formulários eletrónicos, documentos eletrónicos, ou correio eletrónico. Emitido para um indivíduo, com ou sem associação de entidade/organização. Garante o não-repúdio de assinaturas e integridade do conteúdo assinado.
Selo Eletrónico Qualificado	Utilização para transações que suportam assinatura digital de formulários eletrónicos, documentos eletrónicos, ou correio eletrónico. Emitido para entidades legais/organizações. Garante o não-repúdio de assinaturas e integridade do conteúdo assinado.
Autenticação	Utilização específica para autenticação de transações eletrónicas que suportam o acesso a web sites e outro conteúdo online, correio eletrónico, sistemas da organização, etc. Emitido para um indivíduo, com ou sem associação de entidade/organização. Garante a autenticidade de indivíduos (com ou sem associação de entidade/organização).
Assinatura Digital Avançada	Utilização para transações que suportam assinatura digital de formulários eletrónicos, documentos eletrónicos, ou correio eletrónico. Emitido para um indivíduo, com ou sem associação de entidade/organização. Garante o não-repúdio de assinaturas e integridade do conteúdo assinado. Utilização para autenticação de transações eletrónicas que suportam o acesso a web sites e outro conteúdo online, correio eletrónico, sistemas da organização, etc. Emitido para um indivíduo, com ou sem associação de entidade/organização. Garante a autenticidade de indivíduos (com ou sem associação de entidade/organização). Utilização para cifrar informação a ser comunicada, tal como documentos eletrónicos ou conteúdo de correio eletrónico. Emitido para um indivíduo, com ou sem associação de entidade/organização. Garante a confidencialidade do conteúdo.

Selo Eletrónico Qualificado PSD2	Utilização para transações que suportam assinatura digital de formulários eletrónicos, documentos eletrónicos, ou correio eletrónico. Emitido para entidades legais/organizações. Garante o não-repúdio de assinaturas e integridade do conteúdo assinado.
Autenticação de Website Qualificado PSD2	Utilização para comunicações online seguras em que os riscos e consequências do comprometimento de dados é alto. Associa um nome de domínio a uma organização. Garante a autenticidade e confidencialidade.

Os certificados emitidos pela Multicert estão sempre sujeitos a uma validação do indivíduo e/ou organização para a qual o certificado será emitido, assim como outra informação que conste no certificado.

3 Limitação de Confiança

Os certificados podem ser usados para os propósitos para os quais foram emitidos, de acordo com o definido no capítulo 2 deste documento, e na Declaração de Práticas de Certificação e Condições Gerais de Emissão de Certificado Digital disponíveis em https://pki.multicert.com.

Os certificados emitidos podem ser usados para controlo de acessos/autenticação, confidencialidade, integridade, autenticidade ou não-repúdio, dependendo da utilização de chave e utilização estendida de chave existentes no certificado. A utilização apropriada de cada tipo de certificado encontra-se descrita na tabela da secção 2.

Os certificados emitidos pela Multicert não podem ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente.

Os registos de eventos são mantidos por um período de 7 anos após a data de expiração do certificado a que digam respeito.

4 Responsabilidades dos Subscritores / Titulares

O Subscritor/Titular deve cumprir as cláusulas de obrigações que lhe digam respeito constantes no Formulário de Emissão de Certificado Digital, Condições Gerais de Emissão de Certificado Digital, e Declaração de Práticas de Certificação disponível em https://pki.multicert.com, em particular:

- Disponibilizar informação verdadeira para a emissão do certificado, bem como a documentação exigida de forma a comprovar a sua veracidade;
- Limitar e ajustar a utilização do certificado de acordo com as finalidades previstas na Política de Certificado, Condições Gerais de Emissão de Certificado Digital e Declaração de Práticas de Certificação;
- Utilizar a chave privada do certificado apenas dentro do dispositivo criptográfico seguro, quando esta for gerada em tal dispositivo;
- Solicitar de imediato a revogação de um certificado quando ocorra uma das razões de revogação constantes na secção 4.9 da Declaração de Práticas de Certificação, nomeadamente:
    - Sempre que exista comprometimento, suspeita de comprometimento, ou perda da chave privada do certificado e/ou password de acesso à chave privada (i.e. PIN);
    - Quando exista informação do certificado imprecisa ou quando existam alterações com influência nos atributos do certificado.
- Abster-se de utilizar uma chave privada de um certificado que esteja caducado, suspenso ou revogado.

5 Responsabilidades de Verificação do Estado do Certificado pelas *Relying Parties*

Antes de confiarem num certificado, as *Relying Parties* devem:

- Limitar a fiabilidade dos certificados às utilizações permitidas para os mesmos em conformidade com o expresso na correspondente Política de Certificado e secção 1.4 da Declaração de Práticas de Certificação;
- Verificar o estado do certificado no momento no momento de realizar qualquer operação baseada no mesmo, utilizando os mecanismos OCSP e CRL identificados no certificado, e assumir a responsabilidade dessa verificação;
- Obedecer ao especificado na Política de Certificado e Declaração de Práticas de Certificação;
- Notificar qualquer acontecimento ou situação anómala relativa ao certificado, que possa ser considerado como razão para a revogação do mesmo, utilizando os meios que a Multicert indique na sua Declaração de Práticas de Certificação.

6 Limitação de Responsabilidades

A Multicert, enquanto Entidade de Certificação:

a) Responde pelos atos e omissões no exercício da sua atividade de acordo com o Artigo 15 do Decreto-Lei 12/2021;

b) Responde pelos prejuízos que cause aos Subscritores/Titulares ou a terceiros pela falta ou atraso na inclusão de um certificado revogado ou suspenso no serviço de consulta de validade dos certificados, uma vez que tenha conhecimento dele;

c) Assume toda a responsabilidade mediante terceiros pelas funções necessárias à prestação de serviços de confiança, no âmbito da atuação dos Subscritores/Titulares;

d) A sua responsabilidade da administração / gestão assenta sobre base objetiva e abrange todo o risco que os particulares sofram sempre que este seja consequência do funcionamento normal ou anormal dos seus serviços;

e) Só responde pelos danos e prejuízos causados pelo uso indevido do certificado reconhecido, quando os limites da utilização possível não tenham sido consignados no certificado, de forma clara reconhecida por terceiros;

f) Não responde quando o Subscritor/Titular supera os limites que constam no certificado quanto às suas possíveis utilizações, de acordo com as condições estabelecidas e comunicadas ao Subscritor/Titular;

g) Não responde se o destinatário dos documentos assinados eletronicamente não os comprovar e tiver em conta as restrições que constam no certificado quanto às suas possíveis utilizações;

h) Não assume qualquer responsabilidade no caso de perda ou prejuízo:

   i) Dos serviços prestados, em caso de guerra, desastre natural ou qualquer outro motivo de força maior;

   ii) Resultante da utilização dos certificados quando esta utilização exceda os limites estabelecidos na DPC e PC;

   iii) Resultante do uso indevido ou fraudulento dos certificados ou CRL`s emitidas pelas EC`s da PKI Multicert.

7 Acordos Aplicáveis, Declaração de Práticas de Certificação e Política de Certificado

Todos os acordos e condições aplicáveis, Declaração de Práticas de Certificação e Política de Certificado encontram-se disponíveis em https://pki.multicert.com.

8 Política de Privacidade

A Multicert tem implementadas medidas que garantem a privacidade dos dados pessoais, de acordo com a legislação Portuguesa e Europeia.

A Política de Privacidade encontra-se disponível em https://www.multicert.com/pt/termos-de-utilizacao-e-politicas/.

9 Indemnizações

De acordo com a legislação em vigor.

10 Legislação Aplicável, Reclamações e Resolução de Conflitos

A Multicert, enquanto entidade que presta serviços de confiança, tais como os serviços de certificação digital, cumpre os requisitos estabelecidos na atual legislação portuguesa e europeia.

Em caso de litígio o consumidor pode recorrer a uma Entidade de Resolução Alternativa de Litígios de consumo. A lista oficial de tais entidades está disponível no Portal do Consumidor em www.consumidor.pt.

Sem prejuízo da possibilidade de recurso prévio à mediação, caso não seja obtido acordo entre as partes no âmbito de tal procedimento, qualquer uma das partes poderá recorrer à via judicial, ficando desde já fixado como foro competente para o efeito a Comarca de Lisboa.

11 TSP e Licenças de Repositório, Marcas de Confiança e Auditoria

A conformidade das Entidades de Certificação da Multicert é auditada relativamente ao Regulamento Europeu nº 910/2014 e principais normas ETSI EN 319 401, ETSI EN 319 411-1 e ETSI EN 319 411-2. As auditorias são realizadas por auditores externos independentes, pertencentes a um CAB (*Conformity Assessment Body*) acreditado, cujo método de avaliação de conformidade está de acordo com a norma EN ISO/IEC 17065 conforme perfil da ETSI EN 319 403.

Os resultados da auditoria de conformidade são comunicados à Entidade Supervisora Portuguesa (Gabinete Nacional de Segurança), que confirma a inclusão da Multicert na Trusted List Europeia conforme requerido pelo Regulamento Europeu nº 910/2014. As Entidades de Certificação da Multicert podem ser consultadas na Trusted List Europeia em https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/PT/5.

Aprovação

Nuno Ponte (Grupo de Trabalho de Gestão)

[Assinatura Qualificada] Nuno Miguel Arieiro Rodrigues da Ponte

Digitally signed by [Assinatura Qualificada] Nuno Miguel Arieiro Rodrigues da Ponte
Date: 2023.07.10 17:38:12 +01'00'