Declaração de Práticas de Certificação da Multicert Biz Certification Authority

Política

MULTICERT_PJ.ECRAIZ_815_pt

Identificação de projeto: MULTICERT PKI

Nível de acesso: Público

Versão: 3.0

Data: 01/07/2023

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

Identificador de documento: MULTICERT_PJ.ECRAIZ_815_pt

Palavras-chave: MULTICERT Biz CA, Declaração de Práticas de Certificação

Tipologia documental: Política

Título: Declaração de Práticas de Certificação

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 01/07/2023

Versão atual: 3.0

Identificação de projeto: MULTICERT PKI

Histórico de Versões

Versão	Data	Detalhes	Autor(es)
1.0	13/01/2020	Documento inicial	Multicert S.A.
2.0	03/12/2021	Versão Aprovada	Multicert S.A.
2.1	01/07/2023	Revisão contactos, revisão geral	Multicert S.A.
3.0	01/07/2023	Aprovação	Multicert S.A.

Documentos Relacionados

Identificador de documento	Detalhes	Autor(es)
MULTICERT_PJ.ECRAIZ_816_pt	Política de Certificado Multicert Biz Certification Authority	Multicert S.A.

Anexos

Identificador de documento	Detalhes	Autor(es)

Sumário

1 Introdução

1.1 Visão Geral

O presente documento é uma Declaração de Práticas de Certificação, ou DPC, cujo objetivo é a definição de um conjunto de práticas para a emissão e validação de certificados e para a garantia de fiabilidade desses mesmos certificados. Pretende-se que este documento seja simples, direto e entendido por um público alargado, incluindo pessoas sem conhecimentos técnicos ou legais.

Este documento descreve as práticas gerais de emissão e gestão de certificados seguida pela Multicert – Serviços de Certificação Eletrónica S.A., aplicável às Multicert Biz Certification Authorities, e de acordo com a Política de Certificados (PC) da Multicert Biz Certification Authority definida por esta entidade, explicando o significado e função de um certificado, assim como os procedimentos que deverão ser seguidos pelas *Relying Parties* e por qualquer outra parte interessada em confiar nos certificados emitidos pelas Multicert Biz Certification Authoritities. Este documento pode sofrer atualizações regulares.

Os certificados emitidos na Multicert Biz Certification Authority contêm uma referência à DPC de modo a permitir que as *Relying Parties* e outras partes interessadas possam encontrar informação sobre o certificado e sobre a entidade que o emitiu.

Este documento segue a estrutura definida e apresentada pelo grupo de trabalho PKIX (*Public-Key Infrastructure* X.509) do IETF (*Internet Engineering Task Force*) no documento RFC 3647[1].

1.2 Designação e Identificação do Documento

Este documento representa a Declaração de Práticas de Certificação da Multicert Biz Certification Authority. A DPC é representada num certificado através de um número único designado como “identificador de objecto” (OID). O OID de Política de Certificado é usado conforme explicado na secção 3.1.1.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 3.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.25070.3.2.1.2.1
Data de Emissão	01/07/2023
Validade	2 anos
Localização	https://pki.multicert.com/index.html

[1] *cf.* RFC 3647. 2003, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*.

A Multicert emite certificados com os seguintes OID`s:

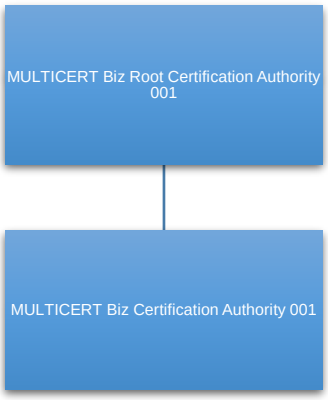
Tipo de Certificado	OID Multicert
Aplicação	1.3.6.1.4.1.25070.3.2.1.1.1
Assinatura Digital – IGCP	1.3.6.1.4.1.25070.3.2.1.1.3
Assinatura Digital	1.3.6.1.4.1.25070.3.2.1.1.7

1.3 Participantes PKI

1.3.1 Entidades de Certificação

Esquematicamente, fazem parte da hierarquia da Multicert Biz Root Certification Authority 001 as seguintes EC`s:

EC`s a emitir certificados:



Multicert Biz Root Certification Authority 001

INFORMAÇÃO DE CERTIFICADO	
Nome distinto	CN = MULTICERT Biz Root Certification Authority 001 OU = Certification Authority O = MULTICERT - Serviços de Certificação Electrónica S.A. C = PT
Validade	08/05/2045
Thumbprint	19 ce 5a 79 6c 33 6c 1a e6 25 7f 37 ca 11 36 74 fc ff 12 9b
Emissor	CN = MULTICERT Biz Root Certification Authority 001 OU = Certification Authority O = MULTICERT - Serviços de Certificação Electrónica S.A. C = PT

Multicert Biz Certification Authority 001

INFORMAÇÃO DE CERTIFICADO	
Nome distinto	CN = MULTICERT Biz Certification Authority 001 OU = Certification Authority O = MULTICERT - Serviços de Certificação Electrónica S.A. C = PT
Validade	06/04/2032
Thumbprint	7c 18 b1 ea 18 b3 38 83 fd 54 7d 55 07 55 e8 88 79 e7 91 9e
Emissor	CN = MULTICERT Biz Root Certification Authority 001 OU = Certification Authority O = MULTICERT - Serviços de Certificação Electrónica S.A. C = PT

1.3.1.1 Entidades de Certificação Externas

Sem Estipulação.

1.3.2 Entidades de Registo

A Entidade de Registo (ER) é a entidade que aprova os nomes distintos (DN) dos titulares dos certificados e mediante avaliação do pedido, aceita ou rejeita a solicitação do certificado. Para além disso, a ER também tem autoridade para aprovar a revogação ou suspensão de certificados.

1.3.2.1 Entidade de Registo Interna

No âmbito da Multicert Biz Certification Authority, a entidade de registo materializa-se pelos serviços internos da mesma que procedem ao registo e validação dos dados necessários, conforme explicitado na Política de Certificado da Multicert Biz Certification Authority para cada tipo de certificado emitido.

1.3.2.2 Entidades de Registo Externas

A Multicert descentraliza esta função através das ER`s externas, que efetuam as seguintes atividades:

- Validação da identidade e atributos a constar no certificado digital;
- Entrega do certificado digital ao Subscritor ou a quem o represente;
- Processamento de pedidos de suspensão e revogação, quando se verifique um dos motivos de suspensão/revogação constantes na secção 4.9.

1.3.3 Subscritores / Titulares

No contexto deste documento o termo Subscritor / Titular aplica-se a todos os utilizadores finais que tenham adquirido certificados à Multicert Biz Certification Authority.

São considerados Subscritores / Titulares de certificados emitidos pela Multicert Biz Certification Authority, aqueles cujo nome está inscrito no campo “Assunto” (*Subject*) do certificado e utilizam o certificado e respetiva chave privada de acordo com o estabelecido na política de certificado descritas neste documento, sendo emitidos certificados para as seguintes categorias de subscritores / titulares:

- Pessoa física ou jurídica;
- Pessoa coletiva (organizações);
- Serviços (tais como computadores, firewalls, routers, servidores, etc).

Em alguns casos, os certificados são emitidos diretamente a pessoas físicas ou jurídicas para uso pessoal, no entanto, existem situações em que quem solicita o certificado é diferente do titular do mesmo, por exemplo, uma organização pode solicitar certificados para os seus colaboradores para que estes representem a organização em transações/comércio eletrónico. Nestas situações a entidade/organização que solicita a emissão do certificado é diferente do titular do mesmo.

1.3.3.1 Patrocinador

A emissão de certificados para equipamentos tecnológicos é efetuada sempre sob responsabilidade humana, sendo esta entidade designada por patrocinador. Neste caso, a ER valida a autoridade do patrocinador para representar a entidade/organização.

O patrocinador tem que aceitar o certificado e é responsável pela sua correta utilização, bem como pela proteção e salvaguarda da sua chave privada.

1.3.4 Relying Parties

As *relying parties* ou destinatários são pessoas singulares, entidades ou equipamentos que confiam na validade dos mecanismos e procedimentos utilizados no processo de associação do nome do titular com a sua chave pública, ou seja, confiam que o certificado corresponde na realidade a quem diz pertencer.

Neste documento, considera-se uma *relying partie*, aquela que confia no conteúdo, validade e aplicabilidade do certificado emitido pela Multicert Biz Certification Authority.

As *Relying Parties* têm que verificar a CRL ou resposta OCSP adequada antes de confiar na informação constante no certificado. A localização do ponto de distribuição da CRL e OCSP está detalhada no certificado.

1.3.5 Outros Participantes

1.3.5.1 Entidade de Registo

Detalhado na secção 1.3.2.

1.3.5.2 Entidades Externas de Prestação de Serviços

As Entidades que prestam serviços de suporte à Multicert Biz Certification Authority têm as suas responsabilidades deviamente definidas através de contratos estabelecidos com as mesmas.

1.3.5.3 Entidade de Validação OCSP

A Entidade de Validação OCSP, tem como função comprovar o estado dos certificados emitidos, através da utilização do protocolo *Online Certificate Status Protocol*[2] (OCSP), de forma a determinar o estado atual do certificado, a pedido de uma entidade, sem necessidade de recorrer à verificação do estado através da consulta das Listas de Certificados Revogados (CRL).

O serviço de Entidade de Validação OCSP é disponibilizado pela Multicert Biz Certification Authority.

1.4 Utilização do Certificado

Os certificados emitidos no âmbito da Multicert Biz Certification Authority são utilizados pelos vários subscritores/titulares, sistemas, aplicações, mecanismos e protocolos de forma a garantir os seguintes serviços de segurança, dependendo do constante nos campos de utilização da chave e utilização estentida da chave do certificado:

a) Controlo de Acessos;

b) Confidencialidade;

c) Integridade;

d) Autenticidade e;

e) Não-repúdio.

Estes serviços são obtidos com recurso à utilização de criptografia de chave pública, através do seu uso na estrutura de confiança que a Multicert Biz Certification Authority fornece.

1.4.1 Utilizações Apropriadas de Certificado

Os requisitos e regras definidos neste documento aplicam-se a todos os certificados emitidos pela Multicert Biz Certification Authority.

Os certificados emitidos de acordo com esta DPC podem ser usados para controlo de acessos, confidencialidade, integridade, autenticidade ou não-repúdio, dependendo da utilização de chave e utilização estentidade de chave existentes no certificado.

[2] cf.RFC 2560. 1999, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol–OCSP.

Certificado	Utilização Apropriada
Aplicação	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 entidades legais / organizações. Garante a autenticidade da entidade / organização.
Assinatura Digital Avançada	Utilização para transações que suportam a assinatura digital de formulários eletrónicos, documentos eletrónicos, ou correio eletrónico. Emitido para um indivíduo, com ou sem associação de uma entidade/organização. Garante o não-repúdio de assinaturas e integridade do conteúdo assinado pelos indivíduos. 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 os 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. Garante a confidencialidade do conteúdo.

Os certificados das Multicert Biz Certification Authorities são também utilizados pelas *Relying Parties* para verificação da cadeia de confiança de um certificado emitido pelas mesmas, assim como para garantir a autenticidade e identidade do emissor de uma assinatura digital gerada pela chave privada correspondente à chave pública incluída num certificado emitido pelas Multicert Biz Certification Authority.

1.4.2 Utilizações Proibidas de Certificado

Os certificados emitidos pelas Multicert Biz Certification Authorities não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente.

Os serviços de certificação oferecidos pela Multicert Biz Certification Authority não foram desenhados nem estão autorizados a ser utilizados em atividades de alto risco ou que requeiram uma atividade isenta de falhas, como as relacionadas com o funcionamento de instalações hospitalares, nucleares, controlo de tráfego aéreo, controlo de tráfego ferroviário, ou qualquer outra atividade onde uma falha possa levar à morte, lesões pessoais ou danos graves para o meio ambiente.

Adicionalmente, os certificados emitidos no âmbito desta DPC não podem ser usados para a finalidade de gestão de tráfego ou *man-in-middle*.

Os certificados não garantem que o Sujeito seja confiável, honesto, respeitável nas suas transações comerciais, seguro para fazer negócios, ou em conformidade com quaisquer leis. O certificado apenas estabelece que a informação do certificado foi verificada de acordo com esta DPC quando o certificado foi emitido.

1.5 Gestão da Política

1.5.1 Entidade Responsável pela Gestão do Documento

A gestão desta DPC é da responsabilidade do Grupo de Trabalho de Autenticação da PKI Multicert, que pode ser contactado pelos meios indicados na secção 1.5.2.

1.5.2 Contacto

NOME	Grupo de Trabalho de Autenticação da PKI Multicert
Morada:	A/C: Grupo de Trabalho de Autenticação Multicert – Serviços de Certificação Electrónica, S.A. Rua Carlos Pinto Coelho, 13 2720-092 Amadora, Portugal
Correio Eletrónico:	ca.forum@multicert.com
Página Web	https://www.multicert.com
Telefone:	+351 217 123 010

Os Subscritores, *Relying Parties*, Fornecedores de Aplicações de Software, e outras terceiras partes podem reportar a suspeita de comprometimento da chave privada, uso indevido do certificado, ou outros tipos de fraude, comprometimento, uso indevido, conduta inadequada, ou qualquer outro assunto relacionado com os certificados através do envio de email para os contactos acima.

1.5.3 Procedimentos para Aprovação da DPC

A validação desta DPC (e/ou respetiva PC) e subsequentes correções (ou atualizações) deverão ser desempenhadas pelo Grupo de Trabalho de Autenticação. Correções (ou atualizações) deverão ser publicadas sob a forma de novas versões desta DPC (e/ou respetiva PC), substituíndo qualquer DPC (e/ou respetiva PC) anteriormente definida. O Grupo de Trabalho de Autenticação deverá ainda determinar quando é que as alterações na DPC (e/ou respetiva PC) levam a uma alteração nos identificadores dos objetos (OID) da DPC (e/ou respetiva PC).

Após validação, a DPC (e/ou respetiva PC) é submetida ao Grupo de Trabalho de Gestão, que é responsável pela aprovação e autorização de modificações neste tipo de documento.

1.6 Definições e Acrónimos

1.6.1 Definições

Item	Definição
Entidade de Certificação (EC)	Entidade em que um ou mais usuários confia para criar e atribuir certificados.
Política de Certificado (PC)	Conjunto denominado de regras que indica a aplicabilidade de um certificado a uma determinada comunidade e/ou classe de aplicativo com requisitos de segurança comuns.
Declaração de Práticas de Certificação (DPC)	Declaração de práticas que uma Entidade de Certificação aplica para a emissão, gestão, revogação, e renovação ou *re-key* de certificados.
Lista de Revogação de Certificados (CRL)	Lista assinada que indica os certificados que foram revogados por um emissor de certificado.
Certificado Digital	Documento eletrónico que associa os dados de verificação de uma assinatura com o seu titular/subscritor e confirma a identidade de tal titular/subscritor.
Assinatura Digital	Modalidade de assinatura eletrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento eletrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento eletrónico foi alterado depois de aposta a assinatura.
Endereço Eletrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos.
Documento Eletrónico	Documento elaborado mediante processamento eletrónico de dados.

OCSP *Responder*	Servidor *online* operado sob a autoridade da EC e conectado ao seu repositório para processar pedidos de estado de certificado.
Online Certificate Status Protocol (OCSP)	Um protocolo *online* de verificação de certificado que permite a aplicações de software de *relying parties* determinar o estado de um certificado identificado.
Chave Privada	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a correspondente chave pública.
Chave Pública	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves.
Relying Party	Qualquer pessoa singular ou entidade legal que confia num certificado válido.
Entidade de Registo (ER)	Entidade principalmente responsável pela identificação e autenticação de sujeitos de certificados. A ER pode apoiar no processo de solicitação de certificado, processo de revogação, ou em ambos.
EC Raiz	Entidade Certificadora de raiz, cujo certificado de raiz é distribuído por fornecedores de aplicações de software, e que emite certificados de Entidade Certificadora intermédia.
Dados de Criação de Assinatura	Conjunto único de dados, como chaves privadas, utilizado pelo titular para a criação de uma assinatura eletrónica.
Dispositivo de Criação de Assinatura	Suporte lógico ou dispositivo de equipamento utilizado para possibilitar o tratamento dos dados de criação de assinatura.
Assunto	Pessoa singular, dispositivo, sistema, unidade ou entidade legal identificada num certificado como Assunto. O Assunto pode ser o subscritor/titular ou um dispositivo sob o controlo e operação de um subscritor.

EC Intermédia / Subordinada	Entidade Certificadora cujo certificado é assinado pela Entidade Certificadora Raiz, ou outra Entidade Certificadora Subordinada. Uma EC Subordinada normalmente emite certificados para utilizadores ou certificados para outras EC`s Subordinadas.
Subscritor	Pessoa singular ou entidade legal para a qual um certificado é emitido e que está legalmente vinculada por um contrato ou termos e condições.

1.6.2 Acrónimos

Acrónimo	Definição
CA	Certification Authority
CLMS	Certificates Lifecycle Management System
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
OCSP	Online Certificate Status Protocol
OID	Object identifier
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
SSCD	Secure Signature-Creation Device

2 Responsabilidade de Publicação e Repositório

2.1 Repositórios

A Multicert S.A. é responsável pelas funções de repositório da Multicert Biz Certification Authority, publicando, entre outras, informação relativa às práticas adotadas e o estado dos certificados emitidos (CRL).

O acesso à informação disponibilizada pelo repositório é efetuado através do protocolo HTTPS e HTTP, estando implementado os seguintes mecanismos de segurança:

- CRL e DPC só podem ser alterados através de processos e procedimentos bem definidos;
- Plataforma tecnológica do repositório encontra-se devidamente protegida pelos mecanismos mais atuais de segurança física e lógica;
- Os recursos humanos que gerem a plataforma têm formação e treino adequado para o serviço em questão.

2.2 Publicação de Informação de Certificação

A Multicert S.A. mantém um repositório em ambiente web, permitindo que as *Relying Parties* efetuem pesquisa on-line relativas à DPC, PC, certificados de EC`s, revogação (CRL) e outra informação referente aos certificados, disponível em https://pki.multicert.com/index.html (e via URI`s incluídos nos próprios certificados).

2.3 Periodicidade de Publicação

As atualizações a esta DPC e respetiva PC, efetuadas com a periodicidade indicada na secção 1.2, serão publicadas imediatamente após a sua aprovação pelo Grupo de Trabalho de Gestão, de acordo com a secção 8.10.

Os certificados das Multicert Biz Certification Authorities são publicados logo que possível após a sua emissão.

A CRL emitida pela Multicert Biz Root Certification Authority é publicada pelo menos uma vez a cada 12 meses ou dentro de 24 horas após a revogação do certificado de uma EC Intermédia.

As CRL`s emitidas pelas Multicert Biz Certification Authorities intermédias serão publicadas pelo menos semanalmente. As Delta-CRL`s relevantes serão publicadas diariamente.

2.4 Controlo de Acesso aos Repositórios

A informação publicada pela Multicert Biz Certification Authority está disponível na Internet, sendo sujeita a mecanismos de controlo de acesso (acesso apenas de leitura). A Multicert S.A. implementou medidas de segurança lógica e física para impedir que pessoas não autorizadas possam adicionar, apagar ou modificar registos do repositório.

3 Identificação e Autenticação

3.1 Atribuição de Nomes

A atribuição de nomes segue a seguinte convenção:

- Aos certificados de pessoa singular é atribuído o nome real do titular (ou pseudónimo);
- Aos certificados de pessoa singular com associação de pessoa coletiva é atribuído o nome da pessoa singular no campo Common Name, e o nome da pessoa coletiva no campo Organization;
- Aos certificados de pessoa coletiva é atribuído o nome da entidade;
- Aos certificados de serviços é atribuído o nome qualificado do domínio e/ou o âmbito da sua utilização.

3.1.1 Tipos de Nomes

Os certificados das Multicert Biz Certification Authorities, assim como os certificados emitidos por estas, são identificados por um nome único (DN – Distinguished Name) de acordo com o standard X.500.

3.1.2 Necessidade de Nomes Significativos

A Multicert irá assegurar, dentro das Multicert Biz Certification Authorities:

- A não existência de certificados que, tendo o mesmo nome único, identificam entidades distintas;
- A relação entre o titular e a organização a que pertence é a mesma que consta no certificado e é facilmente percetível e identificável pelos Humanos (com exceção dos certificados com pseudónimos).

3.1.3 Regras para Interpretação de Formato de Nomes

As regras utilizadas pela Multicert para interpretar o formato dos nomes seguem o estabelecido no RFC 5280[3], assegurando que todos os atributos DirectoryString dos campos "*issuer*" e "*subject*" do certificado são codificados no formato UTF8String, com exceção dos atributos "*country*" e "*serialnumber*" que são codificados no formato PrintableString.

3.2 Validação de Identidade Inicial

Os certificados emitidos ao abrigo desta política estão sempre sujeitos a uma verificação do indivíduo e / ou da organização para a qual o certificado será emitido.

[3] cf. RFC 5280. 2008, InternetX.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile.

3.2.1 Método de Prova de Posse da Chave Privada

3.2.1.1 Assinatura (eSign)

O par de chaves e certificado é fornecido em token criptográfico (SmartCard ou token USB) com chip criptográfico, personalizado fisicamente para o titular. A posse da chave privada é garantida pelo processo de emissão e personalização do token criptográfico, garantindo que:

1. O par de chaves é gerado no HSM criptográfico e inserido no token criptográfico, por comunicação direta segura e sem ficar registado em qualquer dispositivo;
2. O token criptográfico é personalizado para o titular;
3. A chave pública é enviada à Multicert Biz Certification Authority para emissão do correspondente certificado digital, sendo este também inserido no token criptográfico;
4. O token criptográfico é entregue presencialmente ou via correio.

3.2.1.2 Certificados de Aplicação

Deve ser garantido que o pedido de certificado inclui a chave privada correspondente à chave pública listada no certificado. O método para provar a posse da chave privada deve seguir o standard PKCS#10.

3.2.1.3 Método de Prova de Controlo de Endereço de Email

Quando é incluído um endereço de email nos atributos *Distinguished Name* ou *Subject Alternative Name* de um certificado digital, o subscritor deve provar que controla o endereço de email.

Para isso, a Multicert Biz Certification Authority realiza um procedimento de desafio-resposta, que consiste em gerar um token e enviá-lo por email para o endereço de email a ser incluído no certificado. Para comprovar o controlo do endereço de email, o subscritor clica no link que contém o token, que consta no email. A Multicert Biz Certification Authority recebe a resposta e a prova de controlo de endereço de email é concluída com sucesso.

Este procedimento também é realizado para confirmar o endereço de email do subscritor incluído no formulário de pedido de certificado (contacto de email do subscritor).

3.3 Identificação e Autenticação para Pedidos de Renovação de Chaves

3.3.1 Identificação e Autenticação para Pedidos de Rotina de Renovação de Chaves

A Multicert Biz Certification Authority requer ao subscritor que use os mesmos detalhes de autenticação usados no pedido original de pedido de certificado.

3.3.2 Identificação e Autenticação para Renovação de Chaves após Revogação

Todos os pedidos após revogação são tratados como novas emissões de certificados emitidos de acordo com esta política, sujeitos ao mesmo procedimento de validação inicial.

3.4 Identificação e Autenticação para Pedido de Revogação

São consideradas formas de pedido de revogação autenticadas as seguintes:

- Pedido de revogação através da área de cliente – inserindo username e password;
- Pedido de revogação através da área de parceiro – apresentando certificado digital, username e password;
- Pedido de revogação através do Formulário Web de Pedido de Revogação – recebendo um token de revogação através de um meio de comunicação confiável;
- Pedido de revogação através do Formulário de Pedido de Revogação – assinado digitalmente, ou autenticado por uma entidade legal com poderes para tal ato (advogado, notário ou solicitador), ou através de presença física nas instalações da ER pela pessoa que solicita a revogação;
- Pedido de revogação feito por elementos dos Grupo de Trabalho de Operação de Registo – apresentando certificado digital, username e password;
- Pela EC emissora – apresentando certificado digital, username e password;

Se o pedido for feito de outra forma, o processo de revogação de certificados emitidos pela Multicert Biz Certification Authority inicia-se com a suspensão, permitindo a validação adequada da autenticação do pedido.

4 Requisitos Operacionais do Ciclo de Vida do Certificado

4.1 Pedido de Certificado

O pedido de emissão de qualquer certificado à Multicert Biz Certification Authority inicia-se com o preenchimento de um formulário apropriado ao certificado pretendido.

4.1.1 Quem Pode Submeter um Pedido de Certificado

Tanto o titular/subscritor como um indivíduo autorizado pelo subscritor podem submeter um pedido de certificado. Os subscritores são responsáveis pelos dados que o subscritor ou um indivíduo autorizado pelo subscritor submeta à Multicert Biz Certification Authority.

4.1.2 Processo de Registo e Responsabilidades

O processo de registo inclui os seguintes passos:

1. Certificados de Aplicação: geração do par de chaves e envio do CSR;
   1.1. Outros tipos de certificados: o par de chaves é gerado em QSCD/SSCD pela Multicert Biz Certification Authority no momento de emissão do certificado, após serem realizadas todas as atividades seguintes.
2. Preenchimento do formulário de pedido de certificado;
3. Aceitação dos termos e condições de emissão do certificado;
4. Submissão do formulário de pedido de certificado;
5. Pagamento de custos aplicáveis;
6. Fornecedimento de informação/documentação e/ou desempenhando as ações solicitadas pela ER de forma a permitir o processo de validação.

4.2 Processamento do Pedido de Certificado

4.2.1 Identificação e Autenticação

A Multicert Biz Certification Authority, assim que rececione o formulário de pedido de emissão de certificado, bem como a informação necessária à emissão do pedido, procederá à validação de toda a informação disponibilizada a fim de verificar a autenticidade dos dados (ver secção 3.2).

4.2.2 Aprovação ou Rejeição de Pedidos de Certificado

A Multicert Biz Certification Authority apenas aceita o pedido de certificado para emissão se todos os dados constantes no pedido forem autênticos, neste caso o pedido é aprovado.

No caso das informações constantes não forem verdadeiras ou inexistentes, a Multicert rejeita o pedido de emissão de certificado sendo o responsável pelo pedido devidamente informado.

4.2.3 Prazo de Processamento de Pedidos de Certificado

A Multicert Biz Certification Authority dispõe de Service Level Agreements (SLAs), cuja informação se encontra disponível na Loja Online, para emissão de certificados. Contudo, a emissão dos certificados e o tempo que ocorre entre o pedido de certificado e a entrega do mesmo depende sobretudo da submissão completa da informação solicitada e da veracidade da mesma.

4.3 Emissão de Certificado

4.3.1 Ações da Multicert Biz Certification Authority durante a Emissão do Certificado

Para qualquer certificado emitido pela Multicert Biz Certification Authority, o pedido é sujeito a aprovação. Esta aprovação depende do tipo de certificado.

Para aprovação de certificado de utilizador final, o Grupo de Trabalho de Operação de Registo é responsável pela gestão e aprovação dos pedidos de certificados.

4.3.2 Notificação ao Subscritor/Titular pela EC Emissora do Certificado

O subscritor ou o responsável pelo pedido de certificado será automaticamente notificado por email quando o certificado for emitido.

4.4 Aceitação do Certificado

4.4.1 Conduta que Constitui a Aceitação do Certificado

Os certificados são considerados aceites 7 (sete) dias após a sua emissão, ou antes se o certificado for usado quando exista evidência de que o subscritor usou o certificado.

4.4.2 Publicação do Certificado pela EC

A Multicert Biz Certification Authority publicada todos os certificados de EC`s no seu repositório disponível em https://pki.multicert.com. A publicação de certificados de utilizador final é feita através da entrega do certificado ao subscritor.

4.4.3 Notificação da Emissão do Certificado pela EC a Outras Entidades

Podem ser informados da emissão de certificado as ER`s Multicert ou parceiros/revendedores caso estejam envolvidos na solicitação inicial do certificado.

4.5 Utilização do Certificado e Par de Chaves

4.5.1 Utilização do Certificado e Par de Chaves pelo Subscritor/Titular

Os Subscritores dos certificados apenas podem usar a chave privada dos seus certificados para a finalidade exclusiva a que a chave se destina (definida nos campos "*KeyUsage*" e "*Extended Key Usage*" do certificado). A utilização da chave é da exclusiva responsabilidade do subscritor. Os termos e condições para emissão do certificado identificam as obrigações do subscritor relativamente à proteção da chave privada e utilização aceitável.

4.5.2 Utilização do Certificado e Chave Pública pela *Relying Party*

As *Relying Parties* devem usar software em conformidade com os *standards* X.509 e devem apenas confiar no certificado se este não estiver expirado, suspendido ou revogado.

A Multicert Biz Certification Authority fornece nesta DPC informação sobre os serviços apropriados disponíveis para verificar o estado de validade do certificado, tais como o OCSP e CRL.

4.6 Renovação de Certificado

4.6.1 Circunstâncias para a Renovação do Certificado

A Multicert Biz Certification Authority não procede à renovação de certificados digitais, o processo é assumido como uma nova emissão.

4.6.2 Quem Pode Solicitar a Renovação

Sem Estipulação.

4.6.3 Processamento de Pedidos de Renovação de Certificado

Sem Estipulação.

4.6.4 Notificação de Nova Emissão de Certificado ao Subscritor/Titular

Sem Estipulação.

4.6.5 Conduta que Constitui a Aceitação do Certificado Renovado

Sem Estipulação.

4.6.6 Publicação do Certificado Renovado pela EC

Sem Estipulação.

4.6.7 Notificação do Certificado Emitido pela EC a Outras Entidades

Sem Estipulação.

4.7 *Re-Key* de Certificado

4.7.1 Circunstâncias para *Re-Key* de Certificado

A Multicert Biz Certification Authority não procede ao re-key de certificados digitais, sendo o processo é assumido como uma nova emissão.

4.7.2 Quem Pode Solicitar a Certificação de uma Nova Chave Pública

Sem Estipulação.

4.7.3 Processamento de Pedidos de *Re-Key* de Certificado

Sem Estipulação.

4.7.4 Notificação de Nova Emissão de Certificado ao Subscritor/Titular

Sem Estipulação.

4.7.5 Conduta que Constitui a Aceitação do Certificado para o qual foi feito *Re-Key*

Sem Estipulação.

4.7.6 Publicação do Certificado pela EC para o qual foi feito Re-Key

Sem Estipulação.

4.7.7 Notificação de Emissão de Certificado pela EC a Outras Entidades

Sem Estipulação.

4.8 Modificação de Certificado

A modificação de certificado é um processo através do qual o certificado é emitido para um Subscritor (ou *Sponsor*) mantendo as mesmas chaves, com alterações apenas na informação do certificado.

Esta prática não é suportada pela Multicert Biz Certification Authority.

4.8.1 Circunstâncias para a Modificação de Certificado

Sem Estipulação.

4.8.2 Quem Pode Solicitar a Modificação de Certificado

Sem Estipulação.

4.8.3 Processamento de Pedidos de Modificação de Certificado

Sem Estipulação.

4.8.4 Notificação de Nova Emissão de Certificado ao Subscritor/Titular

Sem Estipulação.

4.8.5 Conduta que Constitui Aceitação de Certificado Modificado

Sem Estipulação.

4.8.6 Publicação do Certificado Modificado pela EC

Sem Estipulação.

4.8.7 Notificação de Emissão de Certificado pela EC a Outras Entidades

Sem Estipulação.

4.9 Revogação e Suspensão de Certificado

4.9.1 Motivos para Revogação

A revogação ou suspensão de certificados são ações através das quais o certificado perde a sua validade antes do término do período de validade, perdendo a sua operacionalidade.

Certificados no estado SUSPENSO podem ser revertidos para o estado ATIVO. Certificados no estado REVOGADO não podem ser revertidos para o estado ATIVO.

Se uma das seguintes razões ocorrer, o certificado é revogado dentro de 24 horas:

- O Subscritor solicita à Multicert Biz Certification Authority a revogação do certificado, através da submissão do pedido de revogação;
- O Subscritor notifica a Multicert Biz Certification Authority de que o pedido original de certificado não foi autorizado e não concede autorização com efeitos retroativos;
- A chave privada e/ou a password de acesso à chave privada (i.e. PIN) foi comprometido ou existe suspeita de comprometimento;
- A chave privada foi perdida;
- A Multicert Biz Certification Authority tem conhecimento de um método demonstrado ou comprovado que pode facilmente computar a chave privada do Subscritor com base na chave pública do certificado.

Se uma das seguintes razões ocorrer, o certificado é revogado dentro de 5 dias:

- O certificado foi usado para finalidade não autorizadas;
- A Multicert Biz Certification Authority é informada de uma alteração significativa na informação contida no certificado;
- A Multicert Biz Certification Authority determina ou tem conhecimento de que qualquer informação do certificado é imprecisa;
- A Multicert Biz Certification Authority tem conhecimento de que o Subscritor violou um ou mais obrigações estipuladas nos termos e condições de emissão do certificado digital;
- A Multicert Biz Certification Authority tem conhecimento de que o certificado não foi emitido de acordo com os requisitos da EC previstos na DPC ou PC;
- O algoritmo e tamanho de chave do certificado, ou a geração e verificação da qualidade dos parâmetros da chave pública já não estão em conformidade com a norma ETSI TS 119 312;
- Quando aplicável, se o token/smartcard criptográfico onde a chave privada está armazenada tenha sido perdido, destruído ou deteriorado.

Se uma das seguintes razões ocorrer, o certificado pode ser revogado pela Multicert Biz Certification Authority:

- A Multicert Biz Certification Authority tem conhecimento de que o certificado foi usado para atividades ilícitas;
- A Multicert Biz Certification Authority cessa operações e não encontra outra EC que forneça suporte à revogação dos certificados.

Se uma das seguintes razões ocorrer, a Multicert Biz Certification Authority Subordinada é revogada dentro de 7 dias:

- A Multicert Biz Certification Authority Subordinada solicita a revogação por escrito;
- A Multicert Biz Certification Authority Subordinada notifica a EC Emissora de que o pedido de certificado original não foi autorizado e não concede autorização com efeitos retroativos;
- A Multicert Biz Certification Authority Emissora obtém evidência de que a chave privada da EC Subordinada correspondente à chave pública no certificado sofreu um comprometimento ou já não está em conformidade com a norma ETSI TS 119 312;

- A Multicert Biz Certification Authority Emissora obtém evidência de que o certificado foi usado para finalidades não autorizadas;
- A Multicert Biz Certification Authority Emissora determina que qualquer informação constante no certificado é imprecisa ou enganadora;
- A Multicert Biz Root Certification Authority Emissora ou a Multicert Biz Certification Authority Subordinada cessa operações por qualquer razão e não tem acordos com outra EC para o fornecimento de suporte à revogação do certificado.

4.9.2 Quem Pode Solicitar Revogação

O pedido de revogação pode ser feito por um dos seguintes elementos:

- Pelo cliente/subscritor ou um representante;
- Pela entidade/organização que solicitou o certificado;
- Por um elemento do Grupo de Trabalho de Operação de Registo da Multicert Biz Certification Authority, quando tenha conhecimento de que os dados incluídos no certificado não correspondem à verdade ou não são detidos pelo Subscritor ou quando ocorra uma das razões de revogação definidas na secção 4.9.1.

4.9.3 Procedimento para o Pedido de Revogação

O pedido de revogação pode ser apresentado de uma das seguintes formas:

- On-line, usando o Formulário Web de Pedido de Revogação, em que o estado do certificado será alterado para REVOGADO:
  - https://www.multicert.com/3ws/certRevocationForm?lang=pt_PT
- Através do envio direto do Formulário de Pedido de Revogação, disponível pela Multicert no seu *site*, devidamente preenchido e acompanhado da documentação solicitada para esta finalidade;
- Utilizando os serviços online da Área de Cliente ou Área de Parceiro, não sendo necessário submeter qualquer documentação.

4.9.4 Período de Carência do Pedido de Revogação

O período de carência do pedido de revogação é o tempo disponível para o Subscritor tomar as ações necessárias para pedir a revogação de um certificado sobre o qual exista suspeita de comprometimento da chave, utilização de uma chave fraca ou descoberta de informação imprecisa contida no certificado.

Nesta situação, o Subscritor deve pedir a revogação no prazo de 24 horas após a sua deteção.

4.9.5 Tempo de Processamento do Pedido de Revogação pela Multicert Biz Certification Authority

Quando o pedido de revogação é feito pelo Subscritor ou pessoa responsável pela Entidade/Organização, através de formulário de pedido de revogação escrito, o Grupo de Trabalho de Operação de Registo tem 24 horas, após receber o formulário de pedido de revogação, para o processar e revogar o certificado. Se o pedido de revogação é feito através de um meio autenticado, o processamento da revogação é imediato. A Multicert Biz Certification Authority garante a publicação do novo estado do certificado dentro dos seguintes prazos:

- 12 horas através de Delta CRL;
- 24 horas através de CRL;
- Imediatamente através de OCSP.

4.9.6 Requisito de Verificação da Revogação pelas Relying Parties

Antes de confiar na informação listada num certificado, a Relying Party deve validar a adequação do certificado para a finalidade pretendida e garantir que o certificado é válido. Para verificar o estado do certificado, as Relying Parties necessitam consultar as respostas OCSP ou CRL identificadas em cada certificado.

4.9.7 Frequência de Emissão de CRL

As Multicert Biz Certification Authority Subordinadas emitem CRL`s semanalmente, sendo emitidas Delta CRL`s diariamente.

No caso da Multicert Biz Root Certification Authority, a CRL é publicada a cada 12 meses ou dentro de 24 horas se for revogada uma EC Subordinada.

4.9.8 Latência Máxima para CRLs

As CRL`s de certificados emitidos para utilizadores finais são publicadas automaticamente no repositório online, dentro de um prazo comercialmente razoável após a sua geração, tipicamente dentro de minutos após a sua geração.

Quando são emitidas CRL`s da Multicert Biz Root Certification Authority devido à revogação de EC Subordinada, a CRL é publicada dentro de 24 horas após a sua emissão. As CRL`s regularmente agendadas são publicadas antes do campo nextUpdate da CRL anteriormente emitida para o mesmo âmbito.

4.9.9 Disponibilidade de Verificação de Estado/Revogação *On-Line*

A Multicert Biz Certification Authority dispõe de um serviço de resposta para validação *online* do estado de certificado, com uma disponibilidade correspondente a 99,9%.

O serviço OCSP fornece uma validação em tempo real do estado do certificado.

As respostas OCSP estão em conformidade com o RFC 6960 ou RFC 5019. As respostas OCSP são assinadas por um *responder* OCSP cujo certificado é assinado pela EC que emitiu o certificado sobre o qual se está a verificar o estado de revogação.

4.9.10 Requisitos de Verificação de Revogação *On-Line*

A *Relying Party* deve confirmar a validade do certificado de acordo com a secção 4.9.6 antes de confiar no certificado.

Os OCSP *responders* que recebam um pedido de estado de um certificado que ainda não foi emitido, não devem responder com o estado "*good*" para tal certificado.

4.9.11 Outras Formas Disponíveis de Anunciar Revogação

Sem Estipulação.

4.9.12 Requisitos Especiais Relacionados com o Comprometimento de Chave

A Multicert Biz Certification Authority e Entidade de Registo devem usar métodos comercialmente razoáveis para informar os Subscritores de que a sua chave privada pode ter sido comprometida.

4.9.13 Motivos para Suspensão

É permitida a suspensão de certificado.

A suspensão do certificado pode ser usada quando o Subscritor, o Responsável pela Entidade/Organização (quando aplicável), ou a Entidade de Registo pretendem desabilitar o certificado temporariamente. Pode levar a isso situações como a perda temporária do certificado, saída temporária do Subscritor da Entidade/Organização, etc. Contrariamente à revogação do certificado, a suspensão permite que o estado do certificado seja alterado para ativo ou revogado.

4.9.14 Quem Pode Solicitar Suspensão

O pedido de suspensão pode ser efetuado por um dos seguintes elementos:

- Pelo cliente/subscritor ou um representante;
- Pela Entidade/Organização que solicitou o certificado;
- Por um elementos do Grupo de Trabalho de Operação de Registo da Multicert Biz Certification Authority ou pela EC Emissora.

4.9.15 Procedimento para o Pedido de Suspensão

O pedido de suspensão pode ser apresentado de uma das seguintes formas:

- On-line, utilizando o Formulário Web de Pedido de Suspensão, em que o estado do certificado é alterado para SUSPENSO: https://www.multicert.com/3ws/certSuspensionForm.
- Utilizando os serviços online da Área de Cliente ou Área de Parceiro, não sendo necessário submeter documentação.

4.9.16 Limites do Período de Suspensão

O Subscritor deve submeter o pedido à ER para ativar ou revogar o certificado. Se o Subscritor não submeter o pedido de revogação, o certificado poderá ficar suspenso até ao final da sua validade.

4.10 Serviços de Estado de Certificado

4.10.1 Características Operacionais

O estado de certificados emitidos está disponível publicamente utilizando CRL`s, Delta CRL´s e o serviço OCSP.

Se um certificado for revogado, este mantém-se na CRL após a sua data de expiração.

4.10.2 Disponibilidade de Serviço

O serviço de estado de certificado está disponível 24 horas por dia, 7 dias por semana.

4.10.3 Funcionalidades Opcionais

Sem Estipulação.

4.11 Fim de Subscrição

A operacionalidade do certificado terminará quando ocorra uma das seguintes circunstâncias:

- Revogação do certificado;
- Expiração do período de validade do certificado;
- O contrato do Subscritor aplicável expira sem que seja renovado.

4.12 Custódia e Recuperação de Chaves

4.12.1 Política e Práticas de Custódia e Recuperação de Chaves

A Multicert Biz Certification Authority não faz custódia de chaves de certificados para utilizador final.

4.12.2 Política e Práticas de Encapsulamento e Recuperação de Chave de Sessão

Sem Estipulação.

5 Controlos de Segurança Física, Gestão e Operacionais

A Multicert Biz Certification Authority implementou várias regras e políticas incidindo sobre controlos físicos, procedimentais e humanos, que suportam os requisitos de segurança constantes desta DPC. Esta secção descreve sucintamente os aspetos não técnicos de segurança que possibilitam, de modo seguro, realizar as funções de geração de chaves, autenticação dos titulares, emissão de certificados e revogação de certificados.

5.1 Controlos de Segurança Física

5.1.1 Localização Física e Tipo de Construção

As instalações da Multicert Biz Certification Authority são desenhadas de forma a proporcionar um ambiente capaz de controlar o acesso aos sistemas de certificação, estando fisicamente protegidas de acesso não autorizado, dano, ou interferência. A arquitetura utiliza o conceito de defesa em profundidade, ou seja, por níveis de segurança, garantindo-se que o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado o nível imediatamente anterior, nunca sendo possível, em qualquer local das instalações, aceder ao nível de segurança (n) a partir de outro que não seja o nível (n-1).

As operações da Multicert Biz Certification Authority são realizadas numa sala em zona de alta segurança, inserida noutra zona também de alta segurança e, dentro de um edifício que reúne diversas condições de segurança, nomeadamente o controlo total de acessos que previne, deteta e impede acessos não autorizados, baseado em múltiplos níveis de segurança física.

As duas zonas de alta segurança são áreas que obedecem às seguintes características:

a) Paredes em alvenaria, betão ou tijolo;

b) Tecto e pavimento com construção similar à das paredes;

c) Inexistência de janelas;

d) Porta de segurança, com chapa em aço, com as dobradiças fixas e ombreira igualmente em aço, com fechadura de segurança acionável eletronicamente, características corta-fogo e funcionalidade antipânico.

Adicionalmente, as seguintes condições de segurança são garantidas no ambiente Multicert Biz Certification Authority:

- Perímetros de segurança claramente definidos;
- Paredes, chão e teto em alvenaria, sem janelas, que impedem acessos não autorizados;
- Trancas e fechaduras antiroubo de alta segurança, nas portas de acesso ao ambiente de segurança;
- O perímetro do edifício é estanque na medida em que não existem portas, janelas ou outras brechas não controladas, que possibilitem acessos não autorizados;
- O acesso ao ambiente passa obrigatoriamente por áreas de controlo humano, e por outros meios de controlo que restringem o acesso físico apenas a pessoal devidamente autorizado.

5.1.2 Acesso Físico

Os sistemas da Multicert Biz Certification Authority estão protegidos por um mínimo de 4 níveis de segurança física hierárquicos (edifício em si, bloco de alta segurança, área de alta segurança, sala de alta segurança), garantindo-se que o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado os privilégios necessários ao nível imediatamente anterior.

As atividades operacionais sensíveis da Multicert Biz Certification Authority, criação e armazenamento de material criptográfico, quaisquer atividades no âmbito do ciclo de vida do processo de certificação como autenticação, verificação e emissão ocorrem dentro da zona mais restrita de alta segurança. O acesso a cada nível de segurança requer o uso de um cartão magnético de autenticação.

O acesso à zona mais restrita de alta segurança requer duplo controlo, cada um deles utilizando dois fatores de autenticação, incluindo autenticação biométrica.

5.1.3 Energia e Ar Condicionado

O ambiente seguro da Multicert Biz Certification Authority possui equipamento redundante, que garante condições de funcionamento 24 horas por dia / 7 dias por semana, de:

- Fornecimento de energia elétrica ininterrupta com a potência suficiente para manter autonomamente a disponibilidade do serviço durante períodos de falta de abastecimento da rede pública. O sistema garante a proteção dos equipamentos face a flutuações elétricas que os possam danificar (a alternativa à rede pública é garantida por unidades de alimentação ininterrupta e baterias, bem como geradores de eletricidade a diesel); e
- Refrigeração/ventilação/ar condicionado que controlam os níveis de temperatura e humidade, garantindo condições adequadas para o correto funcionamento de todos os equipamentos eletrónicos e mecânicos presentes dentro do ambiente. A desconformidade dos parâmetros de temperatura/humidade despoleta o envio de alarmes para as equipas de manutenção e para a Central de Segurança.

5.1.4 Exposição à Água

As zonas de alta segurança têm instalados os mecanismos devidos (detetores de inundação) para minimizar o impacto de inundações nos sistemas da Multicert Biz Certification Authority.

5.1.5 Prevenção e Proteção contra Incêndio

O ambiente seguro da Multicert Biz Certification Authority tem instalado os mecanismos necessários para evitar e apagar fogos ou outros incidentes derivados de chamas ou fumos. Estes mecanismos estão em conformidade com os regulamentos existentes:

- Estão instalados nos vários níveis físicos de segurança, sistemas de deteção e alarme de incêndio;
- Estão disponíveis equipamentos fixos e móveis de extinção de incêndios, colocados em sítios estratégicos e de fácil acesso de modo a poderem ser rapidamente usados no início de um incêndio e extingui-lo com sucesso;
- Existem procedimentos de emergência bem definidos, em caso de incêndio.

5.1.6 Armazenamento de *Media*

Todos os suportes de informação sensível, contendo software e dados de produção, arquivo ou cópias de segurança são guardados em cofres e armários de segurança dentro da zona de alta segurança, assim como num ambiente distinto externo ao edifício, com controlos de acessos físicos e lógicos apropriados para restringir o acesso apenas a elementos autorizados dos Grupos de Trabalho.

5.1.7 Eliminação de Resíduos

Documentos e materiais em papel que contenham informação sensível deverão ser triturados antes da sua eliminação.

5.1.8 *Backup* em Instalações Externas

Todas as cópias de segurança são guardadas em ambiente seguro em instalações externas, ficando alojadas em cofres e armários seguros situados em zonas com controlos de acesso físicos e lógicos, de modo a restringir o acesso apenas a pessoal autorizado.

5.2 Controlos Procedimentais

A atividade da Multicert Biz Certification Authority depende da intervenção coordenada e complementar de um extenso elenco de recursos humanos, nomeadamente:

- Segregação de responsabilidades, que minimize a importância individual de cada um dos intervenientes;
- Garantir que a Multicert Biz Certification Authority apenas poderá ser sujeita a ataques do tipo denial-of-service mediante o conluio de um número significativo de intervenientes.

5.3 Controlos de Segurança Pessoal

A admissão de pessoal com funções de confiança nos Grupos de Trabalho é apenas possível se forem cumpridas as seguintes condições:

- Ser formalmente nomeado para a função;
- Ter recebido treino adequado para a função;
- Fazer prova da sua identidade, usando documentação emitida por fontes fiáveis;
- Fazer prova de não possuir antecedentes criminais;
- Fazer prova de que possui as qualificações e experiência exigidas pela entidade ou grupo que efetuou a sua nomeação formal;
- Comprometer-se (formalmente) a não revelar (salvo com autorização expressa dos representantes legais da entidade que detém a Multicert Biz Certification Authority) qualquer informação sobre a Multicert Biz Certification Authority, seu funcionamento, sobre os ambientes e recursos humanos ao seu serviço e sobre os titulares dos certificados digitais por esta emitidos;
- Comprometer-se (formalmente) a desempenhar as funções para as quais foi nomeado e a não assumir responsabilidades que possam colocar problemas éticos ou

deontológicos à sua execução. Nesse sentido, é necessário que declare não só conhecer os termos e condições para o desempenho das respetivas funções, como também a sua capacidade e disponibilidade para o fazer.

5.4 Procedimentos de Registo de Auditoria

5.4.1 Tipos de Eventos Registados

Eventos significativos geram registos auditáveis. Estes incluem, pelo menos os seguintes:

- Pedido, emissão, renovação, reemissão e revogação de certificados;
- Publicação de CRL;
- Eventos relacionados com segurança, incluindo:
    - Tentativas de acesso (com e sem sucesso) a recursos sensíveis da Multicert Biz Certification Authority;
    - Operações realizadas por membros dos Grupos de Trabalho;
    - Dispositivos físicos de segurança de entrada / saída dos vários níveis de segurança.

As entradas nos registos incluem a seguinte informação:

- Número de série do evento;
- Data e hora do evento;
- Identidade do sujeito que causou o evento;
- Categoria do evento;
- Descrição do evento.

5.5 Arquivo de Registos

5.5.1 Tipos de Registos Arquivados

Todos os dados auditáveis são arquivados (conforme indicado na secção 5.4.1), assim como informação de pedidos de certificados e documentação de suporte ao ciclo de vida das várias operações.

5.5.2 Período de Retenção em Arquivo

Os dados sujeitos a arquivo são retidos por um período de tempo de 7 anos após a data de expiração do certificado a quem digam respeito.

5.6 Renovação de Chaves

Sem Estipulação.

5.7 Recuperação em Caso de Desastre ou Comprometimento

Esta seção descreve os requisitos relacionados com os procedimentos de notificação e de recuperação no caso de desastre ou de comprometimento.

5.7.1 Procedimentos em Caso de Incidente ou Desastre

Cópias de segurança das chaves privadas da Multicert Biz Certification Authority e dos registos arquivados (secção 5.5.1) são guardados em ambientes seguros externos e disponíveis em caso de desastre ou de comprometimento.

5.7.2 Recursos Computacionais, Software e/ou Dados Corrompidos

No caso dos recursos informáticos, software e/ou dados estarem corrompidos ou existir suspeita de corrupção, podem ser obtidas as cópias de segurança das chaves privadas da Multicert Biz Certification Authority e os registos arquivados, para verificação da integridade, dos dados originais.

Se for confirmado que os recursos informáticos, software e/ou dados estão corrompidos, devem ser tomadas medidas apropriadas de resposta ao incidente. A resposta ao incidente pode incluir o restabelecimento do equipamento/dados corrompidos, utilizando equipamento similar e/ou recuperando cópias de segurança e registos arquivados. Até que sejam repostas as condições seguras, a Multicert suspenderá os serviços das Multicert Biz Certification Authorities afetadas.

5.7.3 Procedimentos em caso de Comprometimento de Chave Privada da Entidade

No caso da chave privada de uma das Multicert Biz Certification Authorities ser comprometida ou haver suspeita do seu comprometimento, devem ser tomadas medidas apropriadas de resposta ao incidente. As respostas a esse incidente podem incluir:

- Revogação do certificado da Multicert Biz Certification Authority afetada e de todos os certificados emitidos no “ramo” da respetiva hierarquia;
- Geração de novo par de chaves para a Multicert Biz Certification Authority afetada;
- Renovação de todos os certificados emitidos no “ramo” da hierarquia da Multicert Biz Certification Authority afetada.

5.7.4 Capacidades de Continuidade de Negócio em caso de Desastre

A Multicert dispõe dos recursos de computação, software, cópias de segurança e registos arquivados nas suas instalações secundárias de segurança, necessários para restabelecer ou recuperar operações essenciais (emissão e revogação de certificados, com a publicação de informação de revogação) após um desastre natural ou outro.

5.8 Cessação da EC ou ER

Em caso de cessação de atividade da Multicert Biz Certification Authority, a Multicert deve, atempadamente, com uma antecedência mínima de três meses, proceder às seguintes ações:

a) Informar os Subscritores de certificados;

b) Revogar todos os certificados emitidos;

c) Efetuar uma notificação final aos Subscritores 2 (dois) dias antes da cessação formal da atividade;

d) Destruir ou prevenir a utilização, de forma definitiva, das chaves privadas.

6 Controlos de Segurança Técnica

Esta seção define as medidas de segurança implementadas para a Multicert Biz Certification Authority de forma a proteger as chaves criptográficas geradas por esta, e respetivos dados de ativação. O nível de segurança atribuído à manutenção das chaves deve ser máximo para que chaves privadas e chaves seguras, assim como dados de ativação, estejam sempre protegidos e sejam apenas acedidos por pessoas devidamente autorizadas.

6.1 Geração e Instalação do Par de Chaves

A geração dos pares de chaves das Multicert Biz Certification Authorities são processados de acordo com os requisitos e algoritmos definidos nesta política.

6.1.1 Geração do Par de Chaves

O hardware criptográfico, usado para a geração de chaves das Multicert Biz Certification Authorities, cumpre os requisitos FIPS 140-1 nível 3 e/ou Common Criteria EAL 4+, e efetua a manutenção de chaves, armazenamento e todas as operações que envolvem chaves criptográficas utilizando exclusivamente o hardware. O acesso a chaves críticas é protegido por políticas de segurança, divisão de papéis entre os Grupos de Trabalho, assim como através de regras de acesso limitado de utilizadores. As cópias de segurança de chaves criptográficas são efetuadas apenas usando hardware, permitindo que estas cópias sejam devidamente auditadas e que na eventualidade de uma perda de dados, possa haver uma recuperação total e segura das chaves.

6.1.2 Entrega da Chave Privada ao Subscritor/Titular

A entrega da chave privada associada aos certificados de Assinatura Avançada é efetuada em dispositivo criptográfico QSCD.

No caso dos certificados de Aplicação, a chave privada é gerada e fornecida pelo Subscritor.

6.1.3 Entrega da Chave Pública ao Emissor do Certificado

A chave pública é entregue à Multicert Biz Certification Authority, de acordo com os procedimentos indicados na secção 4.1.

6.1.4 Entrega da Chave Pública da Multicert Biz Certification Authority às Relying Parties

As chaves públicas das Multicert Biz Certification Authorities são disponibilizadas através dos respetivos certificados, conforme secção 2.2.

6.1.5 Tamanhos de Chave

Os pares de chaves devem ter tamanho suficiente de forma a prevenir possíveis ataques de criptoanálise que descubram a chave privada correspondente ao par de chaves no seu período de utilização. A dimensão das chaves é a seguinte:

- 4096 *bits* RSA para chaves das Multicert Biz Certification Authorities;
- 2048 *bits* RSA para as chaves associadas aos restantes certificados emitidos pelas Multicert Biz Certification Authorities com algoritmo de assinatura sha256RSA.

6.1.6 Finalidades de Utilização da Chave (de acordo com o campo *key usage* X.509 v3)

De acordo com a secção 1.4.

6.2 Proteção de Chave Privada e Controlos de Engenharia de Módulo Criptográfico

Para a geração dos pares de chaves das Multicert Biz Certification Authorities, assim como para o armazenamento das chaves privadas, a Multicert utiliza um módulo criptográfico em hardware, avaliado de acordo com FIPS 140-2 Nível 3 OU de acordo com a Common Criteria (de acordo com o Perfil de Proteção EN 419 211-5).

6.3 Outros Aspectos da Gestão do Par de Chaves

6.3.1 Arquivo da Chave Pública

É efetuada uma cópia de segurança de todas as chaves públicas das Multicert Biz Certification Authorities pelos membros dos Grupos de Trabalho.

6.3.2 Períodos Operacionais do Certificado e Períodos de Utilização do Par de Chaves

O período de utilização das chaves pode ser o mesmo que o período de validade do certificado.

Os certificados assinados por uma EC específica têm que expirar antes do período de validade do par de chaves da EC.

Neste sentido a validade dos diversos tipos de certificados é a seguinte:

Tipo de Certificado	Utilização de Chave Privada	Validade Máxima do Certificado
Multicert Biz Root Certification Authority	12 anos	25 anos
Multicert Biz Certification Authority	Sem Estipulação	12 anos e 6 meses
Validação *on-line* OCSP	4 meses	1 ano
Aplicação	Sem Estipulação	3 anos
Assinatura Digital Avançada	Sem Estipulação	3 anos

6.4 Dados de Ativação

6.4.1 Geração e Instalação de Dados de Ativação

Os dados de ativação necessários para a utilização das chaves privadas das Multicert Biz Certification Authorities são divididos em várias partes (guardadas em chaves PED – pequenos tokens de identificação digital, com o formato de caneta USB – que identificam diferentes papéis no acesso ao HSM), ficando à responsabilidade de diferentes membros dos Grupos de Trabalho. As diferentes partes são geradas de acordo com o definido no processo/cerimónia de geração de chaves, e obedecem aos requisitos definidos pelo *standard* FIPS 140-2 nível 3.

6.5 Controlos de Segurança Computacional

6.5.1 Requisitos Técnicos Específicos de Segurança Computacional

O acesso aos servidores da Multicert Biz Certification Authority é restrito aos membros dos Grupos de Trabalho com um motivo válido para esse acesso.

6.5.2 Avaliação/Nível de Segurança Computacional

Os vários sistemas e produtos utilizados pela Multicert Biz Certification Authority são fiáveis e protegidos contra modificações.

O módulo criptográfico em Hardware das Multicert Biz Certification Authorities está em conformidade com o *standard* EAL 4+ *Common Criteria for Information Technology Security Evaluation* e/ou FIPS 140-2 nível 3.

6.6 Controlos Técnicos do Ciclo de Vida

6.6.1 Controlos de Desenvolvimento de Sistema

É fornecida metodologia auditável que permite verificar que o software das Multicert Biz Certification Authorities não foi alterado antes da sua primeira utilização. Todas as configurações e alterações do software são executadas e auditadas por membros dos Grupos de Trabalho.

6.6.2 Controlos de Gestão da Segurança

A Multicert Biz Certification Authority tem mecanismos e/ou Grupos de Trabalho para controlar e monitorizar a configuração dos sistemas da PKI.

6.6.3 Controlos de Segurança do Ciclo de Vida

As operações de atualização e manutenção dos produtos e sistemas da Multicert Biz Certification Authority, seguem o mesmo controlo que o equipamento original e são instalados pelos membros dos Grupos de Trabalho com formação adequada para o efeito, seguindo os procedimentos definidos.

6.7 Controlos de Segurança da Rede

A Multicert Biz Certification Authority dispõe de dispositivos de proteção de fronteira, nomeadamente sistema firewall, e cumpre com os requisitos necessários para identificação, autenticação, controlo de acessos, administração, auditoria, reutilização, responsabilidade e recuperação de serviços e troca de informação.

6.8 Validação Cronológica

Certificados, CRL`s e outras entradas na base de dados contêm sempre informação sobre a data e hora dessa entrada. Todas estas entradas são assinadas digitalmente por um certificado emitido para o efeito.

7 Perfis de Certificado, CRL e OCSP

7.1 Perfil de Certificado

Os utilizadores de uma chave pública têm que ter confiança que a chave privada associada é detida pelo titular remoto correto (pessoa ou sistema) com o qual irão utilizar mecanismos de cifra ou assinatura digital. A confiança é obtida através da utilização de certificados digitais X.509 v3, que são a estrutura de dados que faz a ligação entre a chave pública e o seu titular. Esta ligação é afirmada através da assinatura digital de cada certificado por uma EC. A Multicert Biz Certification Authority pode basear esta afirmação em meios técnicos (por exemplo, prova de posse da chave privada através de um protocolo desafio-resposta), na apresentação da chave privada, ou no registo efetuado pelo titular.

Um certificado tem um período de validade limitado, indicado no seu conteúdo e assinado pela EC. Como a assinatura do certificado e a sua validade podem ser verificadas independentemente por qualquer software que utilize certificados, os certificados podem ser distribuídos através de linhas de comunicação e sistemas públicos, assim como podem ser guardados em qualquer tipo de unidades de armazenamento.

O utilizador de um serviço de segurança que requeira o conhecimento da chave pública do utilizador necessita, normalmente, de obter e validar o certificado que contém essa chave. Se o serviço não dispuser de uma cópia fidedigna da chave pública da EC que assinou o certificado, assim como do nome da EC e informação relacionada (tal como o período de validade), então poderá necessitar de um certificado adicional para obter a chave pública da EC e validar a chave pública do utilizador. Em geral, para validar a chave pública de um utilizador, pode ser necessária uma cadeia de múltiplos certificados, incluindo o certificado da chave pública do utilizador assinado por uma EC, e zero ou mais certificados adicionais de EC`s assinados por outras EC`s.

7.1.1 Número(s) de Versão

Todos os certificados emitidos pela Multicert Biz Certification Authority estão em conformidade com a versão 3 do X.509.

7.1.2 Extensões do Certificado

As extensões dos certificados emitidos pela Multicert Biz Certification Authority estão em conformidade com o RFC 5280.

7.1.3 Identificadores de Objeto de Algoritmo

Os certificados emitidos pela Multicert Biz Certification Authority são assinados usando o algoritmo sha256WithRSAEncrypton (1.2.840.113549.1.1.11):

{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}

7.1.4 Formatos de Nome

De acordo com o definido na secção 3.1.

7.1.5 Identificador de Objeto de Política de Certificado

Todos os certificados emitidos pela Multicert Biz Certification Authority contêm os seguintes qualificadores:

"*policyQualiflierID*: 1.3.6.1.5.5.7.2.1" e "*cPSuri*", que aponta para o URI onde se encontra a Declaração de Práticas de Certificação com o OID identificado pelo "*policyIdentifier*". São incluídos outros identificadores de objetos de política de certificado, dependendo do tipo de certificado, de acordo com a secção 1.2 deste documento.

7.1.6 Utilização de Extensão de Restrições de Política

Sem Estipulação.

7.1.7 Sintaxe e Semânticas de Qualificadores de Política

A extensão "*certificate policies*" contém um tipo de qualificador de política a ser utilizado pelos emissores de certificados e autores da política de certificado. O tipo de qualificador é o "*CPSuri*", que contém um apontador, na forma de URI, para a Declaração de Práticas de Certificação publicada pela EC; e o "*userNotice explicitText*", que contém um apontador, na forma de URI, para a Política de Certificado.

7.1.8 Processamento de Semânticas para a Extensão de Políticas de Certificado Críticas

Sem Estipulação.

7.2 Perfil CRL

Quando um certificado é emitido, espera-se que seja utilizado durante todo o seu período de validade. Contudo, existem várias circunstâncias podem causar que um certificado se torne inválido antes da expiração do seu período de validade. Tais circunstâncias incluem a mudança de nome, mudança de associação entre o titular e os dados do certificado (por exemplo, um trabalhador que termina o emprego), o comprometimento ou suspeita de comprometimento da correspondente chave privada. Nestas circunstâncias, a EC tem que revogar o certificado.

O protocolo X.509 define um método de revogação do certificado, que envolve a emissão periódica, pela EC, de uma estrutura de dados assinada, a que se dá o nome de Lista de Revogação de Certificados (LRC ou CRL). A CRL é uma lista com identificação temporal dos certificados revogados, assinada pela EC e disponibilizada livremente num repositório público. Cada certificado revogado é identificado na CRL pelo seu número de série. Quando uma aplicação utiliza um certificado (por exemplo, para verificar a assinatura digital de um utilizador remoto), a aplicação verifica a assinatura e validade do certificado, assim como obtém a CRL mais recente e verifica se o número de série do certificado não faz parte da mesma. Note-se que uma EC emite uma nova CRL periódicamente.

7.2.1 Número(s) de Versão

As CRL`s emitidas pela Multicert Biz Certification Authority estão em conformidade com a versão 2 do RFC 5280, e incluem os seguintes campos:

Campo	Valor
Version	2
Signature Algorithm	sha-256WithRSAEncryption
Issuer Name	DN da EC emissora da CRL
This Update	Data de emissão da CRL
Next Update	Data da próxima emissão de CRL
Revoked Certificates List	Lista de certificados revogados Em cada entrada da lista é incluído o número de série e data de revogação
Signature	Assinatura produzida pela EC emissora da CRL

7.2.2 CRL e Extensões da CRL

As CRL`s emitidas pela Multicert Biz Certification Authority têm as seguintes extensões:

Extensão	Valor
Authority Key Identifier	Identificador da EC emissora da CRL
CRL Number	Número sequencial da CRL
CRL Reason Code	Razão da revogação (opcional)

7.3 Perfil OCSP

O perfil dos certificados OCSP emitidos pela Multicert Biz Certification Authority estão em conformidade com:

- ITU.T recommendation X.509[4];
- RFC 6960[4].

7.3.1 Número(s) de Versão

Os pedidos e respostas OCSP emitidos pela Multicert Biz Certification Authority estão em conformidade com a versão 1 do RFC 6960.

7.3.2 Extensões OCSP

Sem Estipulação.

[4] cf. RFC 69602013,X.509 Internet Public Key Infrastructure Online Certificate Status Protocol -OCSP.

8 Outras Matérias Legais e de Negócio

8.1 Taxas

8.1.1 Taxas de Emissão ou Renovação de Certificado

As taxas cobradas pela Multicert estão identificadas na sua loja online ou numa proposta formal realizada pela Multicert.

8.1.2 Taxas de Acesso a Certificado

Sem Estipulação.

8.1.3 Taxas de Acesso a Informação de Estado ou Revogação

O acesso a informação sobre o estado de certificado ou revogação (CRL e Delta CRL) é gratuita e livre.

8.2 Confidencialidade de Informação de Negócio

8.2.1 Âmbito de Informação Confidencial

Declara-se expressamente como informação confidencial, aquela que não poderá ser divulgada a terceiros, nomeadamente:

- As chaves privadas das EC`s da Multicert Biz Certification Authority;
- Toda a informação relativa aos parâmetros de segurança, controlo e procedimentos;
- Toda a informação de carácter pessoal fornecida à Multicert Biz Certification Authority durante o processo de registo dos subscritores de certificados, salvo se houver autorização explícita para a sua divulgação e/ou se a mesma não for incluída no conteúdo do certificado emitido;
- Planos de continuidade de negócio e recuperação;
- Registos de transações, incluindo os registos completos e os registos de auditoria das transações;
- Informação de todos os documentos relacionados com a Multicert Biz Certification Authority (regras, políticas, cerimónias, formulários e processos), incluindo conceitos organizacionais, informação financeira/comercial secreta, confidencial e/ou privilegiada, sendo propriedade da Multicert.
- Todas as palavras-chave, PIN`s e outros elementos de segurança relacionados com as Multicert Biz Certification Authorities;
- A identificação dos membros dos Grupos de Trabalho da Multicert Biz Certification Authority;

- A localização dos ambientes da Multicert Biz Certification Authority e seu conteúdo.

8.2.2 Informação fora do Âmbito de Informação Confidencial

É considera informação de acesso público:

- Política de Certificado;
- Declaração de Práticas de Certificação;
- CRL;
- Delta CRL;
- Toda a informação classificada como “Público” (a informação que não esteja expressamenta considerada “pública” deve ser considerada confidencial).

A Multicert Biz Certification Authority permite o acesso a informação não confidencial sem prejuízo dos controlos de segurança necessários para proteger a autenticidade e integridade da informação.

8.2.3 Responsabilidade de Proteção de Informação Confidencial

Os elementos dos Grupos de Trabalho ou outras entidades que recebam informação confidencial são responsáveis por assegurar que esta não é copiada, reproduzida, armazenada, traduzida ou transmitida a terceiras partes por quaisquer meios sem antes terem o consentimento escrito da Multicert.

8.3 Privacidade de Informação Pessoal

8.3.1 Plano de Privacidade

O Sistema de Gestão do Ciclo de Vida do Certificado (SGCVC) é responsável por implementar medidas que assegurem a privacidade de dados pessoais, de acordo com a legislação Portuguesa e Europeia aplicável.

8.3.2 Informação Tratada como Privada

É considerada informação privada toda a informação fornecida pelo subscritor/titular do certificado que não seja disponibilizada no certificado digital do subscritor/titular ou CRL.

8.3.3 Informação Não Considerada Privada

É considerada informação não protegida pela privacidade, toda a informação fornecida pelo subscritor/titular do certificado que seja disponibilizada no certificado digital do subscritor/titular ou CRL.

8.3.4 Responsabilidade pela Proteção de Informação Privada

De acordo com a legislação Portuguesa e Europeia aplicável.

8.3.5 Notificação e Consentimento para Utilização de Informação Privada

De acordo com a legislação Portuguesa e Europeia aplicável.

8.4 Direitos de Propriedade Intelectual

Todos os direitos de propriedade intelectual, incluindo os que se referem a certificados, CRL e Delta CRL emitidos, OID, DPC e PC, bem como qualquer outro documento relativo à Multicert Biz Certification Authority, pertencem à Multicert S.A..

As chaves privadas e as chaves públicas são propriedade do subscritor/titular, independentemente do meio físico que se utilize para o seu armazenamento.

8.5 Representações e Garantias

8.5.1 Representações e Garantias da EC

A Multicert S.A. obriga-se a:

a) Desempenhar as suas operações de acordo com esta política;

b) Proteger as suas chaves privadas;

c) Emitir certificados de acordo com o *standard* X.509;

d) Emitir certificados que estejam conformes com a informação conhecida no momento da sua emissão e livres de erros de entrada de dados;

e) Garantir a confidencialidade no processo de geração dos dados de criação da assinatura e na sua entrega ao subscritor/titular através de um procedimento seguro;

f) Utilizar sistemas e produtos confiáveis que estejam protegidos contra todas as modificações e que garantam a segurança técnica e criptográfica dos processos de certificação;

g) Utilizar sistemas confiáveis para armazenar certificados reconhecidos, que permitam comprovar a sua autenticidade e impedir a modificação de dados por pessoas não autorizadas;

h) Arquivar os certificados emitidos sem quaisquer alterações;

i) Garantir que podem determinar com precisão a data e hora em que um certificado foi emitido, revogado ou suspenso;

j) Revogar os certificados nos termos da secção 4.9 deste documento, e publicar os certificados revogados no repositório da CRL das Multicert Biz Certification Authorities, com a frequência estabelecida na secção 2.3;

k) Proteger eventuais chaves existentes que estejam sob a sua custódia;

l) Garantir a disponibilidade da CRL de acordo com o disposto na secção 2;

m) Cumprir com as especificações contidas no regulamento Europeu sobre Proteção de Dados Pessoais;

n) Disponibilizar os certificados das EC`s Multicert Biz Certification Authority.

8.5.2 Representações e Garantias da ER

As Entidades de Registo obrigam-se a:

a) Desempenhar as suas operações de acordo com esta política;

b) Permitir a emissão de certificados livres de erros de entrada de dados;

c) Garantir a confidencialidade no processo de geração dos dados de criação da assinatura e na sua entrega ao subscritor/titular através de um procedimento seguro;

d) Utilizar sistemas e produtos confiáveis que estejam protegidos contra todas as modificações e que garantam a segurança técnica e criptográfica dos processos de certificação;

e) Arquivar os certificados emitidos sem quaisquer alterações;

f) Proteger eventuais chaves existentes que estejam sob a sua custódia;

g) Cumprir com as especificações contidas no regulamento Europeu sobre Proteção de Dados Pessoais.

8.5.3 Representações e Garantias do Subscritor/Titular

É obrigação do subscritor/titular do certificado emitido:

a) 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 secção 1.4 desta DPC;

b) Tomar todos os cuidados e medidas necessárias para garantir a posse da sua chave privada;

c) Solicitar de imediato a revogação de um certificado em caso de ter conhecimento ou suspeita do comprometimento da chave privada correspondente à chave pública contida no certificado, ou outra razão constante na secção 4.9;

d) Não utilizar o certificado digital que tenha perdido a sua eficácia, quer por ter sido revogado, suspenso ou expirado o seu período de validade;

e) Submeter à Entidade de Certificação (ou Entidade de Registo) a informação que considere exata e completa em relação aos dados que estas solicitem para realizar o processo de registo. Deve informar a EC de qualquer modificação desta informação;

f) Não monitorizar, manipular ou efetuar ações de “engenharia inversa” sobre a implementação técnica (hardware e software) dos serviços de certificação, sem a devida autorização prévia, por escrito, da Multicert S.A..

8.5.4 Representações e Garantias da *Relying Party*

É obrigação das partes que confiem nos certificados emitidos pelas Multicert Biz Certification Authorities:

a) 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 DPC;

b) Verificar a validade dos certificados no momento de realizar qualquer operação baseada nos mesmos;

c) Assumir a responsabilidade pela correta verificação das assinaturas digitais;

d) Assumir a responsabilidade na comprovação da validade, revogação ou suspensão dos certificados nos quais confia;

e) Ter pleno conhecimento das garantias e responsabilidades aplicáveis na aceitação e uso de certificados em que confia, e aceitar sujeitar-se às mesmas;

f) 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 S.A. indique nesta DPC.

8.5.5 Representações e Garantias de outros Participantes

Sem Estipulação.

8.6 Renúncia de Garantias

A Multicert S.A. recusa todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas nesta DPC.

8.7 Limitações de Responsabilidade

A Multicert S.A., enquanto Entidade de Certificação:

a) 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;

b) 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;

c) 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 Multicert Biz Certification Authorities.

8.8 Prazo e Terminação

8.8.1 Prazo

Os documentos relacionados com a Multicert Biz Certification Authority (incluindo esta DPC) tornam-se efetivos logo que sejam aprovados pelo Grupo de Trabalho de Gestão.

Esta DPC entra em vigor desde o momento de sua publicação no repositório da Multicert.

Esta DPC mantém-se em vigor enquanto não for revogada expressamente pela emissão de uma nova versão.

8.8.2 Terminação

As alterações são adequadamente registadas com indicação de uma versão menor.

As alterações tornam-se efetivas após a aprovação do Grupo de Trabalho de Gestão e a publicação no repositório de uma versão maior.

8.9 Notificações Individuais e Comunicações aos Participantes

Qualquer notificação relacionada com a DPC deve ser feita por correio eletrónico assinado digitalmente, formulários assinados enviados por correio, ou outros, dependendo da criticidade e assunto da comunicação. Estas notificações devem ser enviadas para os contactos indicados na secção 1.5.

8.10 Alterações

8.10.1 Procedimento para Alteração

As alterações a esta DPC são realizadas pelo Grupo de Trabalho de Autenticação. Podem ser submetidas ao Grupo de Trabalho de Autenticação sugestões de alterações para serem analisadas, através dos contactos fornecidos na secção 1.5.

O Grupo de Trabalho de Autenticação regista as alterações da revisão em versões menores na DPC. Quando se encontra pronta para aprovação uma nova versão da DPC, o Grupo de Trabalho de Autenticação submete o documento para aprovação do Grupo de Trabalho de Gestão, sendo que uma versão maior é incrementada à DPC.

8.10.2 Mecanismo e Período de Notificação

As alterações à DPC são registadas na tabela Histórico de Versões, contendo identificação da versão, data, e detalhes das alterações feitas.

Quando é aprovada uma nova versão maior da DPC pelo Grupo de Trabalho de Gestão, é publicada no repositório da Multicert uma versão atualizada deste documento.

8.10.3 Circunstâncias nas quais o OID deve ser Alterado

Se o Grupo de Trabalho de Autenticação determinar que é necessário alterar o OID correspondente à DPC ou PC, propõe essa alteração ao Grupo de Trabalho de Gestão. Neste caso, é criado um novo documento DPC ou PC com um OID diferente.

De outra forma, as alterações não devem requerer a alteração do OID da DPC ou PC.

8.11 Disposições de Resolução de Conflito

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 quanto a qualquer conflito decorrente da interpretação, aplicação ou execução do presente formulário de emissão, qualquer uma das partes poderá recorrer à via judicial, ficando desde já fixado como foro competente para o efeito a Comarca de Lisboa.

8.12 Outras Disposições

8.12.1 Acordo Completo

Todas as *relying parties* assumem na totalidade o conteúdo da última versão desta DPC.

8.12.2 Atribuição

As partes que operam sob esta DPC ou acordos aplicáveis não podem atribuir os seus direitos ou obrigações sem o prévio consentimento por escrito da Multicert.

8.12.3 Divisibilidade

Se uma disposição desta DPC, incluíndo cláusulas de limitação de responsabilidade, for considerada ineficaz ou não executável, o restante desta DPC deve ser interpretado no sentido da intenção original das partes.

Qualquer disposição desta DPC que estabeleça uma limitação de responsabilidade deve ser separável e independente de qualquer outra disposição e deve ser aplicada como tal.

8.12.4 Execução (Honorários de Advogados e Renúncia de Direitos)

A Multicert pode requerer a indemnização e honorários advocatícios de uma parte por danos, perdas e despesas relacionadas à conduta dessa parte. A falha da Multicert em aplicar uma cláusula desta DPC não renuncia ao direito da Multicert de aplicar a mesma cláusula posteriormente ou ao direito de aplicar quaisquer outras cláusulas desta DPC. Para ter efeito, qualquer renúncia deve ser feita por escrito e assinada pela Multicert.

8.12.5 Força Maior

As cláusulas de força maior estão incluídas nas Condições Gerais de Emissão de Certificado Digital.

8.13 Outras Provisões

Sem Estipulação.

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 17:35:26 +01'00'