Política de Certificado Multicert Biz Certification Authority

Políticas

MULTICERT_PJ.ECRAIZ_816_pt

Identificação da EC: 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
Telefone: +351 217 123 010

Identificação de Documento: MULTICERT_PJ.ECRAIZ_816_pt

Palavras-chave:

Tipo de Documento: Políticas

Título: Política de Certificado Multicert Biz Certification Authority

Língua Original: Português

Língua de Publicação: Português

Nivel de Acesso: Público

Data: 01/07/2023

Versão Atual: 3.0

Identificação da EC: 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

ID Documento	Detalhes	Autor(es)
MULTICERT_PJ.ECRAIZ_815_pt	Declaração de Práticas de Certificação da Multicert Biz Certification Authority	Multicert S.A

Sumário

1 Introdução

1.1 Visão Geral

Este documento tem como objetivo definir um conjunto de requisitos que definem como os titulares devem gerir os certificados digitais que adquirem à Multicert Biz Certification Authority. Não tem como objetivo nomear regras ou obrigações, mas sim informar. Portanto, este documento pretende ser simples, direto e compreendido por um grande público.

1.2 Nome e Identificação do Documento

Este documento é uma Política de Certificado. A PC é representada no certificado por um número único intitulado “identificador de objeto” (OID). O valor do OID associado a este documento é descrito na tabela abaixo.

Este documento é identificado pelos dados incluídos na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 3.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.25070.3.2.1.1
Data de Emissão	01/07/2023
Validade	2 anos
Localização	https://pki.multicert.com/

A Multicert Biz Certification Authority 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 da PKI

1.3.1 Entidades de Certificação

A Multicert detém e gere a sua própria infraestrutura. A Multicert Biz Root Certification Authority, bem como as EC`s Subordinadas /Intermédias são operadas por Grupos de Trabalho com diferentes funções.

O Grupo de Trabalho de Autenticação é responsável por definir todas as Políticas de segurança, incluindo a gestão deste documento, bem como a Declaração de Práticas de Certificação, e o Grupo de Trabalho de Gestão é responsável pela sua aprovação.

1.3.2 Entidades de Registo

As Entidades de Registo (ER) são responsáveis pela identificação dos subscritores dentro de uma organização ou associação.

As ER`s da Multicert devem assinar um acordo com a EC Multicert, com a finalidade de cumprir todos os requisitos de identificação.

1.3.3 Subscritores

No contexto deste documento, o termo Subscritor aplica-se a todos os utilizadores finais para os quais foram atribuídos certificados pela Multicert Biz Certification Authority.

São considerados Subscritores de certificados emitidos pela Multicert Biz Certification Authority aqueles cujo nome está inscrito no campo “Assunto” do certificado e utilizam o certificado e chave privada correspondente de acordo com o estabelecido na DPC e PC; certificados emitidos para as seguintes categorias:

- Entidade individual ou legal;
- Entidade Coletiva (Organizações); ou
- Serviços (como computadores, firewall, routers, servidores, etc).

Em alguns casos, os certificados são diretamente emitidos para entidades individuais ou coletivas para uso pessoal.

No entanto, existem casos em que a pessoa que solicita o certificado é diferente do seu Subscritor, por exemplo, uma organização pode solicitar certificados para os seus empregados, para que estes possam representar a organização em transações/comércio eletrónico. Nestas situações a entidade que solicita a emissão do certificado é diferente do seu subscritor.

1.3.4 *Relying Parties*

As *Relying parties* são pessoas naturais, entidades ou equipamento que atuam com base num certificado e/ou assinatura digital emitido pela EC Emissora.

As *Relying Parties* têm que verificar a CRL ou resposta OCSP adequada antes de confiar na informação constate no certificado.

1.4 Utilização do Certificado

Os certificados emitidos no domínio da Multicert Biz Certification Authority são utilizados por diferentes subscritores, sistemas, aplicações, mecanismos e protocolos com o propósito de assegurar os seguintes serviços de segurança:

a) Controlo de Acessos;
b) Confidencialidade;
c) Integridade;
d) Autenticidade; e
e) Não-repúdio.

Estes serviços são obtidos recorrendo à utilização de criptografia de chave pública, através da sua utilização na estrutura disponibilizada pela Multicert Biz Certification Authority.

1.4.1 Utilizações Apropriadas de Certificado

Os certificados emitidos para serviços são destinados ao uso em serviços de autenticação e no estabelecimento de canais cifrados.

Os certificados emitidos para pessoas ou entidades destinam-se à utilização em Assinaturas Digitais, autenticação ou encriptação.

Os certificados emitidos pela Multicert Biz Certification Authority também são usados pelas Partes de Confiança para a verificação da cadeia de confiança do certificado emitido pela EC, bem como para garantir a autenticidade e identidade do emissor de uma assinatura digital criada pela chave privada correspondente à chave pública contida no certificado emitido pela 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.

1.5 Gestão da Política

1.5.1 Entidade Responsável pela Gestão do Documento

Esta PC e todos os documentos públicos pertencentes à Multicert Biz Certification Authority são geridos pelo Grupo de Trabalho de Autenticação, cujos contactos se encontram descritos na secção 1.5.2.

1.5.2 Contacto

NOME	Grupo de Trabalho de Autenticação
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 PC

O Grupo de Trabalho de Gestão é responsável pela aprovação desta política.

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.
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.

Infraestrutura de Chaves Públicas (ICP ou PKI)	Conjunto de hardware, software, pessoas, procedimentos, regras, políticas e obrigações utilizadas para facilitar de forma confiável a criação, emissão, gestão, e utilização de certificados e chaves baseadas em criptografia de chave pública.
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

Acrónimos	Definição
CA	Certification Authority
CLMS	Certificates Lifecycle Management System
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DL	Decree-law
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

As EC`s abrangidas por esta política devem assegurar que os dados de revogação de certificados emitidos estão disponíveis publicamente através de um repositório.

2.2 Publicação de Informação de Certificado

A informação pública da Multicert Biz Certification Authority está disponível na internet. Inclui:

- Certificados das EC`s;
- CRL`s;
- PC e DPC.

2.3 Periodicidade de Publicação

As atualizações a esta PC e DPC correspondente, efetuadas com a periodicidade indicada na secção 1.2, devem ser publicadas imediatamente após a sua aprovação pelo Grupo de Trabalho de Gestão.

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.
A CRL da Multicert Biz Certification Authority deve ser publicada pelo menos semanalmente. As Delta CRL`s devem ser publicadas diariamente.

2.4 Controlo de Acesso aos Repositórios

A informação publicada pela Multicert Biz Certification Authority deve estar 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

3.1.1 Tipos de Nomes

Os certificados da Multicert Biz Certification Authority são emitidos de acordo com o standard ITU X.500 e os seus Nomes Distintos (DN – *Distinguished Name*) são construídos de acordo com o standard X.500.

3.1.2 Necessidade de Nomes Significativos

Os tipos de certificados descritos neste documento são emitidos utilizando Nomes Únicos de forma a clarificar um nome único e identificável. Alguns atributos podem ser usados para tornar os nomes significativos. Um exemplo desses atributos é o *serial number* e o *organization identifier*.

3.1.3 Regras para Interpretação de Formato de Nomes

Os nomes distintos (*Distinguished Names*) são definidos de acordo com o RFC 5280.

3.2 Validação de Identidade Inicial

Os certificados emitidos segundo esta política são sempre sujeitos a uma verificação do indivíduo e/ou organização para a qual o certificado vai ser emitido.

3.2.1 Método de Prova de Posse da Chave Privada

No caso de o Subscritor emitir a chave privada, a Multicert Biz Certification Authority que vai emitir o certificado deve confirmar a posse da chave privada no pedido de certificado (*Certificate Signing Request* – CSR).

3.2.1.1 Método de Prova de Controlo de Endereço de Email

Quando o endereço de email é incluído nos atributos do *Distinguished Name* ou *Subject Alternative Name* do certificado, o Subscritor deve fazer prova de controlo do endereço de email a ser incluído no certificado. Para tal, a Multicert Biz Certification Authority desempenha um procedimento de *challenge-response*, que se encontra detalhado na DPC.

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 autenticidade do pedido.

4 Requisitos Operacionais do Ciclo de Vida do Certificado

4.1 Pedido de Certificado

4.1.1 Quem Pode Submeter um Pedido de Certificado

Tanto o Subscritor/Titular 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. Fornecimentos de informação/documentação e/ou desempenho das 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 identifica e verifica todos os pedidos de certificado de acordo com as práticas definidas no Capítulo 3 “Identificação e Autenticação” desta DPC.

4.2.2 Aprovação ou Rejeição de Pedidos de Certificado

Todos os pedidos que sejam identificados e verificados com sucesso, são aprovados para emissão pela Multicert Biz Certification Authority.

Caso não seja possível verificar o pedido, a Multicert Biz Certification Authority deve rejeitar a emissão do certificado.

4.2.3 Prazo de Processamento de Pedidos de Certificado

Uma vez verificado com sucesso o pedido a Multicert Biz Certification Authority emite o certificado de acordo com o SLA acordado, cuja informação está disponível na loja online.

4.3 Emissão de Certificado

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

As EC`s emissoras verificam todas as fontes de informação que utilizam para verificar os pedidos.

Todos os sistemas pertencentes ao processo de emissão de certificado são protegidos contra modificação, através de políticas de controlo de acesso, proteção das bases de dados e autenticação entre sistemas.

Quando a emissão do certificado envolve a EC Raiz, são necessários elementos autorizados pertencentes aos grupos de trabalho a fim de emitir manualmente o certificado na EC Raiz.

4.3.2 Notificação ao Subscritor/Titular pela EC Emissora do Certificado

As EC`s emissoras devem notificar o Subscritor por email quando o seu certificado é 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 publica todos os certificados de EC`s emitidos no seu repositório em https://pki.multicert.com.

4.4.3 Notificação da Emissão do Certificado pela EC a Outras Entidades

Nos casos em que o pedido foi submetido através da ER a EC deve notificar a ER relativamente à emissão do certificado.

4.5 Utilização do Certificado e Par de Chaves

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

O Subscritor deve usar as suas chaves privadas de acordo com os termos aceites no acordo.

As chaves privadas são pessoais de tal forma que o Subscritor não pode torná-las disponíveis para terceiras partes.

As chaves privadas apenas devem ser usadas para a finalidade exclusiva a que se destinam.

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

As *Relying Parties* devem verificar sempre a validade do certificado e o seu estado através dos métodos disponibilizados pela EC emissora, tais como as CRL`s e OCSP.

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 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 finalidades 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 uma 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 funções 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 que corresponde 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 funções 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

A EC Emissora ou ER devem aceitar pedidos de revogação provenientes de partes autenticadas e autorizadas, tais como o Subscritor ou a Entidade/Organização associada, quando aplicável.

4.9.3 Procedimento para o Pedido de Revogação

A EC Emissora deve fornecer um processo para os Subscritores solicitarem a revogação dos seus próprios certificados. O processo deve ser descrito na DPC da EC Emissora.

A EC Emissora revogará sempre o certificado se o pedido for autenticado como originário pelo Subscritor ou Entidade/Organização associada, quando aplicável.

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 dentro de 24 horas após a sua deteção.

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

Uma EC Emissora deve revogar o certificado dentro de 24 horas quando o pedido é feito através de formulário de pedido revogação escrito. Quando o pedido de revogação é feito de forma autenticada, a revogação é processada imediatamente.

4.9.6 Requisito de Verificação da Revogação pelas *Relying Parties*

As *Relying Parties* devem confirmar a validade do certificado através dos serviços que a EC Emissora tenha disponibilizado, tais como o OCSP e CRL.

4.9.7 Frequência de Emissão de CRL

As EC`s a funcionarem de acordo com esta política devem emitir as suas CRL`s com a seguinte frequência:

- EC`s Intermédias/Subordinadas – semanalmente;
- EC Raiz – no mínimo a cada 12 (doze) meses ou dentro de 24 (vinte e quatro) horas se for revogado o certificado de 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 uma 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*

Todas as EC`s abrangidas por esta política fornecem serviço OCSP.

As respostas OCSP devem ser conformes com o RFC 6960 ou RFC 5019. As respostas OCSP devem sempre ser 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 seção 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 a Suspensão

É permitida a suspensão de certificado.

4.9.14 Quem Pode Solicitar Suspensão

A EC Emissora e a ER devem aceitar pedidos de suspensão autenticados. A autorização para a suspensão deve ser aceite se o pedido de suspensão for efetuado pelo Subscritor ou Entidade/Organização associada, quando aplicável. A EC Emissora também pode suspender o certificado por sua iniciativa.

4.9.15 Procedimento para o Pedido de Suspensão

Considerando a natureza dos pedidos de suspensão e a necessidade de eficiência, a EC Emissora e a ER providenciam mecanismos automáticos para a solicitação e autenticação de pedidos de suspensão.

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

A EC Emissora deve disponibilizar informação sobre o estado do certificado via CRL e OCSP. A EC Emissora deve listar os certificados revogados na CRL apropriada, e devem ser mantidos após a data de expiração.

4.10.2 Disponibilidade de Serviço

Os serviços de estado do certificado devem estar disponíveis 24 horas por dia, 7 dias por semana.

4.10.3 Funcionalidades Opcionais

Sem Estipulação.

4.11 Fim de Subscrição

A EC Emissora deve permitir aos Subscritores terminarem a sua subscrição dos serviços de certificado tendo o seu certificado revogado, permitindo que o certificado expire sem renovação, ou permitindo que o contrato do subscritor expire sem renovação.

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

As EC`s devem implementar várias regras e políticas incidindo sobre controlos físicos, procedimentais e humanos, que suportam os requisitos de segurança constantes desta PC. 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, revogação de certificados, e arquivo. Todos estes controlos não técnicos de segurança são críticos para garantir a confiança nos certificados, pois qualquer falha de segurança pode comprometer as operações da EC.

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 EC.

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 que digam respeito.

5.6 Renovação de Chaves

Sem Estipulação.

5.7 Recuperação em Caso de Desastre ou Comprometimento

Esta secção 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 Authority 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 EC às *Relying Parties*

A chave privada da Multicert Biz Certification Authority deve ser disponibilizada através do respetivo certificado, conforme a secção 2.2.

6.1.5 Tamanhos de Chave

O tamanho dos pares de chaves deve ser suficiente de forma a prevenir possíveis ataques de criptoanálise que descubram a chave privada correspondente ao par de chaves durante o seu período de utilização. Os tamanhos de chave estão definidos na secção 6.1.5 da DPC.

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 da DPC.

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 das chaves públicas da Multicert Biz Certification Authority 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.

A validade dos vários tipos de certificados está descrita na secção 6.3.2 da DPC.

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 EC Multicert 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 EC são fiáveis e protegidos contra modificações.

O módulo criptográfico em Hardware da EC 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 da Multicert Biz Certification Authority 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 cumprem 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

Os 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

O campo “*version*” do certificado descreve a versão utilizada na codificação do certificado. Neste perfil, a versão utilizada é a versão 3 do X.509.

7.1.2 Extensões dos Certificados

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 sha256WithRSAEncryption (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:

"*policyQualifIierID*: 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 de 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

A Multicert Biz Certification Authority emite CRL`s em conformidade com a versão 2 do RFC 5280.

7.2.2 CRL e Extensões da CRL

A Multicert Biz Certification Authority emite extensões da CRL de acordo com o RFC 5280.

7.3 Perfil OCSP

O perfil de certificados OCSP está em conformidade com:

- ITU.T recommendation X.509**Erro! Marcador não definido.**;
- RFC 6960[1].

7.3.1 Número(s) de Versão

A Multicert Biz Certification Authority suporta a versão 1 do RFC 6960.

7.3.2 Extensões OCSP

Sem Estipulação.

[1] cf. RFC 6960. 2013, 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 considerada 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 expressamente 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 autenticidades 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

A EC é responsável por implementar as medidas que assegurem a privacidade dos 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 do certificado que não seja disponibilizada no certificado digital do subscritor ou CRL.

8.3.3 Informação Não Considerada Privada

É considerada informação não protegida pela privacidade, toda a informação fornecida pelo subscritor do certificado que seja disponibilizada no certificado digital do subscritor 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, Delta CRL emitidos, OID, DPC e PC, bem como qualquer outro documento relativo à PKI Multicert, pertencem à Multicert S.A..

As chaves privadas e as chaves públicas são propriedade do subscritor, 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 **Erro! A origem da referência não foi encontrada.** deste documento, e publicar os certificados revogados no repositório da CRL das Multicert Biz Certification Authorities, com a frequência estabelecida na secção **Erro! A origem da referência não foi encontrada.**;

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

l) Garantir a disponibilidade da CRL de acordo com o disposto na secção **Erro! A origem da referência não foi encontrada.**;

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 da 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; e

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 das *Relying Party*

É obrigação das partes que confiem nos certificados emitidos pela EC:

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 revogação do mesmo, utilizando os meios que a Multicert indique na sua DPC.

8.5.5 Representações e Garantias de outros Participantes

Sem Estipulação.

8.6 Renúncia de Garantias

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

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 PC) tornam-se efetivos logo que sejam aprovados pelo Grupo de Trabalho de Gestão.

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

Esta PC 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 nova versão maior.

8.9 Notificações Individuais e Comunicações aos Participantes

Qualquer notificação relacionada com esta PC 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 PC 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 PC. Quando se encontra pronta para aprovação uma nova versão da PC, o Grupo de Trabalho de Autenticação submete o documento para aprovação pelo Grupo de Trabalho de Gestão, sendo que uma versão maior é incrementada à PC.

8.10.2 Mecanismo e Período de Notificação

As alterações à PC 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 PC 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 Disposição 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 PC.

8.12.2 Atribuição

As partes que operam sob esta PC 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 PC, incluindo cláusulas de limitação de responsabilidade, for considerada ineficaz ou não executável, o restante desta PC deve ser interpretado no sentido da intenção original das partes.
Qualquer disposição desta PC 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 de advogados de uma parte por danos, perdas e despesas relacionadas à conduto dessa parte. A falha da Multicert em aplicar uma cláusula desta PC não renuncia ao direito da Multicert de aplicar a mesma cláusula posteriormente ou ao direito de aplicar quaisquer outras cláusulas desta PC. 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 17:19:04 +01'00'