Política de Certificado da Entidade Certificadora de Documentos

Políticas

PJ.CNICV_24.1.2_0004_pt_IAC

Versão: V3.0

Data: 06/2021

Dono: SNIAC

Classificação: Público

Identificador do documento: PJ.CNICV_24.1.2_0004_pt_IAC

Nível de acesso: Público

Data: 08/06/2021

Versão atual: 3.0

Histórico de Versões

N.º de Versão	Data	Detalhes	Autor(es)
1.0	05/07/2010	Versão inicial	MULTICERT
2.0	19/09/2019	Revisão (sem alterações egistadas)	MULTICERT
3.0	06/2021	Revisão (sem alterações egistadas)	MULTICERT

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
PJ.CNICV_24.1.1_0001_pt_IAC	Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil	MULTICERT

Resumo Executivo

Decorrente da implementação de vários programas públicos para a promoção das tecnologias de informação e comunicação e a introdução de novos processos de relacionamento em sociedade, entre cidadãos, empresas, organizações não-governamentais e o Estado, com vista ao fortalecimento da sociedade de informação e do governo eletrónico (*eGovernment*), o Cartão Nacional de Identificação fornece os mecanismos necessários para a autenticação digital forte da identidade do Cartão Nacional de Identificação perante os serviços da Administração Pública, assim como as assinaturas eletrónicas indispensáveis aos processos de desmaterialização que estão a ser disponibilizados pelo Estado.

A infraestrutura de chaves públicas do Cartão Nacional de Identificação fornece uma hierarquia de confiança, que promoverá a segurança eletrónica do Cartão Nacional de Identificação no seu relacionamento com o Estado. A infraestrutura de chaves públicas do Cartão Nacional de Identificação estabelece uma estrutura de confiança eletrónica que proporciona a realização de transações eletrónicas seguras, a autenticação forte, um meio de assinar eletronicamente transações ou informações e documentos eletrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transações ou informação.

A hierarquia de confiança da EC de Identificação e Autenticação Civil encontra-se englobada na hierarquia da ICP-CV - Infraestrutura de Chaves Públicas de Cabo Verde.

Este documento define a Política de certificados utilizada na emissão do certificado de Entidade Certificadora de Documentos, que complementa e está de acordo com a Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil.[1]

[1] *cf.* PJ.CNICV_24.1.1_0001_pt_IAC, Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil.

Conteúdo

1. POLÍTICA DE CERTIFICADO DA ENTIDADE CERTIFICADORA DE DOCUMENTOS

1.1. Objetivo e Âmbito

O objetivo deste documento é definir as políticas utilizadas na emissão do certificado de Entidade Certificadora de Documentos, pela Entidade de Certificação de Identificação e Autenticação Civil (EC IAC).

1.2. Público-Alvo

Este documento deve ser lido por:

- Recursos humanos ao serviço da PKI do CNICV.
- Terceiras partes encarregues de auditar as Entidades Certificadoras,
- Todo o público, em geral.

1.3. Estrutura do Documento

Assume-se que o leitor é conhecedor dos conceitos de criptografia, infraestruturas de chave pública e assinatura eletrónica. Caso esta situação não se verifique recomenda-se o aprofundar de conceitos e conhecimento nos tópicos anteriormente focado antes de proceder com a leitura do documento.

Este documento complementa a Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil[1], presumindo-se que o leitor leu integralmente o seu conteúdo antes de iniciar a leitura deste documento.

2. CONTEXTO GERAL

O presente documento é um documento de Política de Certificados, ou PC, cujo objetivo se prende com a definição de um conjunto de políticas e dados para a emissão e validação de Certificados e para a garantia de fiabilidade desses mesmos certificados. Não se pretende nomear regras legais ou obrigações, mas antes informar. Pretende-se assim que este documento seja simples, direto e entendido por um público alargado, incluindo pessoas sem conhecimentos técnicos ou legais.

Este documento descreve a política de certificados para a emissão e gestão do certificado de Entidade Certificadora de Documentos, emitido pela EC de Identificação e Autenticação do Civil adiante denominada de EC IAC.

Os Certificados emitidos pela EC IAC contêm uma referência ao PC de modo a permitir que Partes confiantes e outras pessoas interessadas possam encontrar informação sobre o certificado e sobre as políticas seguidas pela entidade que o emitiu.

2.1. Visão Geral

Este documento satisfaz e complementa os requisitos impostos pela Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil.

2.2. Designação e Identificação do Documento

Este documento é a Política de Certificados do certificado de Entidade Certificadora de Documentos. A PC é representada num certificado através de um número único designado de "identificador de objecto" (OID), sendo o valor do OID apresentado abaixo.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 3.000
Estado do Documento	Versão Final
OID	2.16.132.1.2.2.1.2.1
Data de Emissão	Junho 2021
Validade	Não aplicável
Localização	http://pki.cni.gov.cv/pub/pol/pc_ecd.html.pdf

2.3. Participantes

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

2.4. Dados de Contacto

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3. DISPOSIÇÕES GERAIS

3.1. Obrigações e Direitos

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.1.1. Obrigações da EC

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.1.2. Obrigações das Unidades de Registo

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.1.3. Obrigações dos Titulares de Certificados

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.1.4. Direito das partes confiantes

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.1.5. Obrigações de Repositório

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.2. Responsabilidades

3.2.1. Responsabilidades da EC

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.2.2. Responsabilidades das Unidades de Registo

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.3. Responsabilidade Financeira

3.3.1. Indemnização devida pela terceira parte

Nada a assinalar.

3.3.2. Relações fiduciárias

Nada a assinalar.

3.4. Interpretação e execução

3.4.1. Legislação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.4.2. Forma de interpretação e notificação

Nada a assinalar.

3.4.3. Procedimentos para a resolução de disputas

Nada a assinalar.

3.5. Taxas de serviço

3.5.1. Taxas de emissão e renovação de certificados

Nada a assinalar.

3.5.2. Taxas de revogação ou de acesso à informação de status

O acesso a informação sobre o estado ou revogação dos certificados é livre e gratuita.

3.5.3. Taxas para outros serviços

Nada a assinalar.

3.5.4. Política de reembolso

Nada a assinalar.

3.6. Publicação e repositório

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.6.1. Frequência da publicação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.6.2. Controlo de acesso

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.6.3. Repositórios

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.7. Auditoria de Conformidade

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.7.1. Frequência ou motivo da auditoria

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.7.2. Identidade e qualificações do auditor

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.7.3. Relação entre o auditor e a Entidade Certificadora

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.7.4. Âmbito da auditoria

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.7.5. Procedimentos após uma auditoria com resultado deficiente

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.7.6. Comunicação de resultados

Os resultados de auditorias são apenas comunicados à Entidade Auditada e à ANAC em relatório em formato eletrónico com aposição de assinatura digital qualificada.

3.8. Sigilo

3.8.1. Divulgação de Informação de Revogação e de Suspensão de Certificado

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.8.2. Quebra de sigilo por motivos legais

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.8.3. Informações a terceiros

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.8.4. Divulgação por solicitação do titular

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

3.8.5. Direitos de propriedade intelectual

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

4. IDENTIFICAÇÃO E AUTENTICAÇÃO

4.1. Registo Inicial

4.1.1. Disposições Legais

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

4.1.2. Tipos de nomes

O certificado de Entidade Certificadora de Documentos é identificado por um nome único (DN – *Distinguished Name*) de acordo com *standard* X.500.

O nome único deste certificado emitido pela EC de Identificação e Autenticação Civil é identificado pelos seguintes componentes:

Atributo	Código	Valor
Country	C	CV
Organization	O	Sistema Nacional de Identificação e Autenticação Civil de Cabo Verde
Organization Unit	OU	Serviços de Identificação e Autenticação Civil
Organization Unit	OU	Entidades Certificadoras de Documentos
Serial Number	serialnumber	<nnnnn>[2]
Common Name	CN	Entidade Certificadora de Documentos do Cartão Nacional de Identificação

4.1.3. Necessidade de nomes significativos

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

4.1.4. Unicidade de nomes

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

[2] <nnnnn> é um valor sequencial iniciado em "00001" na emissão do primeiro certificado deste tipo.

4.1.5. Procedimento para resolver disputa de nomes

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

4.1.6. Reconhecimento, autenticação, e função das marcas registadas

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

4.1.7. Método de comprovação da posse de chave privada

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

4.1.8. Autenticação da identidade de uma pessoa singular

Nada a assinalar.

4.1.9. Autenticação da identidade de uma pessoa coletiva

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

4.1.9.1. Documentos para efeitos de identificação de pessoa coletiva

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

4.1.9.2. Informações Certificado de equipamento tecnológico

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

4.1.9.3. Validação de Autoridade

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

4.1.10. Critérios para interoperabilidade

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

4.2. Identificação e Autenticação para pedidos de renovação de chaves

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

4.3. Identificação e autenticação para pedido de revogação

Qualquer entidade integrada no domínio da ICP-CV, pode solicitar a revogação de um certificado de ECD, havendo conhecimento ou suspeita de compromisso da chave privada do titular ou qualquer outro acto que recomende esta acção[3].

A EC IAC guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efetua o pedido de revogação, que podem ser, entre outros:

- Patrocinador nomeado pela entidade;
- Representante legal do MJT, com poderes de representação para o pedido de revogação de certificados;
- Parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos.

Um formulário próprio[3] serve de base ao pedido de revogação de certificado e contém, entre outros, os seguintes elementos de identificação da entidade que inicia o pedido de revogação:

a) Denominação legal;

b) Número de pessoa coletiva, sede, objeto social, nome dos titulares dos corpos sociais e de outras pessoas com poderes para a obrigarem e número de matrícula na conservatória do registo comercial;

[3] cf. PJ.CNICV_53.2.2_0001_pt_IAC, Formulário de revogação de certificado emitido pela EC Identificação e Autenticação Civil.

5. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

5.1. Pedido de Certificado

5.1.1. Requisitos

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

5.1.2. Quem pode subscrever um pedido de certificado?

O patrocinador é a única entidade que pode subscrever pedidos de certificados para equipamento tecnológico que seja utilizado no âmbito do Cartão Nacional de Identificação.

5.1.3. Processo de registo e responsabilidades

O processo de registo de certificado de equipamento tecnológico é constituído pelos seguintes passos, a serem efetuados pela entidade de certificação subordinada requerente:

- Geração do par de chaves (chave pública e privada) pelo patrocinador;
- Geração do PKCS#10 correspondente pelo patrocinador;
- Geração do *hash* (SHA-256[4]) do PKCS#10, em formato PEM, pelo patrocinador;
- Arquivo do PKCS#10 e *hash* num CD/DVD, pelo patrocinador;
- Preenchimento pelo patrocinador de documento de validação da identidade da entidade, de acordo com secção 4.1.9.2;
- Envio do CD/DVD e do documento corretamente preenchido ao contacto da EC IAC.

5.2. Processamento do pedido de certificado

5.2.1. Requisitos

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

[4] cf. NIST FIPS PUB 180-1. 1995, The Secure Hash Algorithm (SHA-256). National Institute of Standards and Technology, "Secure Hash Standard,", U.S. Department of Commerce.

5.2.2. Processos para a identificação e funções de autenticação

O Conselho Executivo da EC IAC aprova a candidatura para um certificado de equipamento tecnológico quando os seguintes critérios são preenchidos:

- Identificação e autenticação bem-sucedida de toda a informação necessária nos termos da secção 4.1.9.2 – toda a documentação utilizada para verificação da identidade e de poderes de representação é guardada;
- Formulário de pedido de emissão corretamente preenchido;
- PKCS#10 válido.

Em qualquer outra situação, será rejeitada a candidatura para emissão de certificado.

Após a emissão do certificado, o Conselho Executivo da EC IAC é responsável por entregar o certificado e restantes dados necessários de forma presencial – tal ato é registado através do preenchimento e assinatura de formulário[5].

5.2.3. Aprovação ou recusa de pedidos de certificado

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

5.2.4. Prazo para processar o pedido de certificado

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

5.3. Emissão de Certificado

5.3.1. Procedimentos para a emissão de certificado

A emissão do certificado é efetuada por meio de uma intervenção que decorre na zona de alta segurança da EC IAC e, em que se encontram presentes:

- Os representantes legais do patrocinador requerente ou o(s) representante(s) nomeado(s) para esta intervenção;

[5] PJ.CNICV_53.2.4_0001_pt_IAC, Formulário de receção de certificado de EC subordinada da EC de Identificação e Autenticação Civil.

- Três (3) membros do Grupo de Trabalho – a segregação de funções não possibilita a presença de um número inferior de elementos,
- Quaisquer observadores aceites simultaneamente pelos membros do Grupo de Trabalho e pelo patrocinador.

A intervenção de emissão de certificado ECD é constituída pelos seguintes passos:

- Identificação e autenticação de todas as pessoas presentes na intervenção, garantindo que o patrocinador e os membros do Grupo de Trabalho têm os poderes necessários para os atos a praticar;
- O patrocinador entrega, em mão, o CD/DVD e o formulário de emissão[6] do certificado aos membros do Grupo de Trabalho da EC IAC. O formulário é datado e assinado pelos membros do Grupo de Trabalho que o devolvem ao patrocinador;
- Os membros do Grupo de Trabalho da EC IAC efetuam o procedimento de arranque de processamento da EC IAC e emitem o certificado (correspondente ao PKCS#10) fornecido no CD/DVD;
- Os membros do Grupo de Trabalho da EC IAC arquivam o certificado num suporte tecnológico não regravável) e preenchem o formulário de receção e aceitação de certificado[7], em duplicado;
- Após a assinatura de ambas as cópias do formulário de receção e aceitação de certificado pelo patrocinador e pelos membros do Grupo de Trabalho, os membros do Grupo de Trabalho entregam o certificado, num suporte tecnológico não regravável, ao patrocinador.
- A intervenção de emissão fica terminada com a execução do procedimento de finalização de processamento da EC IAC, pelos membros do Grupo de Trabalho da EC IAC;

O certificado emitido inicia a sua vigência no momento da sua emissão.

5.3.2. Notificação da emissão do certificado ao titular

A emissão do certificado é efetuada de forma presencial, de acordo com secção anterior.

[6] cf. PJ.CNICV_53.2.1_0002_pt_IAC, Formulário de emissão de certificado de Equipamento Tecnológico
[7] cf. PJ.CNICV_53.2.4_0002_pt_IAC, Formulário de receção de certificado de Equipamento Tecnológico

5.4. Aceitação do Certificado

5.4.1. Procedimentos para a aceitação de certificado

O certificado considera-se aceite após a assinatura do formulário de emissão e aceitação de certificado pelo patrocinador, de acordo com intervenção de emissão (conforme secção 5.3.1).

Note-se que antes de ser disponibilizado o certificado ao patrocinador, e consequentemente lhe serem disponibilizadas todas as funcionalidades na utilização da chave privada e certificado, é garantido que,

a) O titular toma conhecimento dos seus direitos e responsabilidades;

b) O titular toma conhecimento das funcionalidades e conteúdo do certificado;

c) O titular aceita formalmente o certificado e as suas condições de utilização assinando para o efeito o Termo de Responsabilidade do Titular.

No termo de responsabilidade do titular constam os procedimentos necessários em caso de expiração, revogação e renovação do certificado, bem como os termos, condições e âmbito de utilização do mesmo. Deve ser assinado pela pessoa física responsável por esses certificados.

5.4.2. Publicação do certificado

Os certificados ECD emitidos não são publicados, são disponibilizados integralmente ao patrocinador, com os constrangimentos definidos no ponto 5.4.1.

5.4.3. Notificação da emissão de certificado a outras entidades

Nada a assinalar.

5.5. Uso do certificado e par de chaves

5.5.1. Uso do certificado e da chave privada pelo titular

A EC de Identificação e Autenticação Civil é a titular do certificado de Entidade Certificadora de Documentos, utilizando a sua chave privada para a assinatura de dados a colocar no *chip* do Cartão Nacional de Identificação, garantindo e permitindo verificar a integridade dos mesmos.

5.5.2. Uso do certificado e da chave pública pelas partes confiantes

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

5.6. Renovação de Certificados

5.6.1. Renovação de Certificados

Esta prática não é suportada na ICP-CV.

5.7. Modificação de Certificados

Esta prática não é suportada na ICP-CV.

5.8. Suspensão e revogação de certificado

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

5.8.1. Circunstâncias para revogação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

5.8.2. Quem pode submeter o pedido de revogação

Está legitimado para submeter o pedido de revogação, sempre que se verifiquem alguma das condições descritas no ponto 5.8.1, os seguintes:

a) O patrocinador titular do certificado;

b) A EC IAC;

c) A Entidade Credenciadora;

d) Uma parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos.

A EC IAC guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efetua o pedido de revogação, garantindo a verificação da identidade dos seus

representantes legais, por meio legalmente reconhecido, não aceitando poderes de representação para o pedido de revogação do certificado de ECD.

5.8.3. Procedimento para o pedido de revogação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

5.8.4. Prazo para processar o pedido de revogação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

5.8.5. Motivos para suspensão

Nada a assinalar.

5.8.6. Quem pode pedir o pedido de suspensão

Nada a assinalar.

5.8.7. Procedimentos para pedido de suspensão

Nada a assinalar.

5.8.8. Limite do período de suspensão

Nada a assinalar.

5.8.9. Frequência de emissão de LCR

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

5.8.10. Requisitos de verificação on-line de revogação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

5.8.11. Outras formas disponíveis para divulgação de revogação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

5.8.12. Disponibilidade de verificação on-line do estado / revogação de certificado

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

5.8.13. Requisitos especiais em caso de comprometimento de chave privada

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

5.9. Serviços sobre o estado certificado

5.9.1. Características operacionais

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

5.9.2. Disponibilidade do serviço

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

5.9.3. Características opcionais

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

5.10. Fim de subscrição

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

5.11. Retenção e recuperação de chaves (*Key escrow*)

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

5.11.1. Políticas e práticas de recuperação de chaves

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

5.11.2. Políticas e práticas de encapsulamento e recuperação de chaves de sessão

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

6. MEDIDAS DE SEGURANÇA FÍSICA, DE GESTÃO E OPERACIONAIS

6.1. Medidas de segurança física

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

6.1.1. Construção e Localização Física das Instalações da EC

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

6.1.2. Acesso físico ao local

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

6.1.3. Energia e ar condicionado

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

6.1.4. Exposição à água

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

6.1.5. Prevenção e proteção contra incêndio

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

6.1.6. Salvaguarda de suportes de armazenamento

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

6.1.7. Eliminação de resíduos

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

6.1.8. Instalações externas (alternativa) para recuperação de segurança

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

6.2. Medida de segurança dos processos

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

6.2.1. Funções de Confiança

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

6.2.2. Número de pessoas exigidas por tarefa

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

6.2.3. Identificação e Autenticação para cada função

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

6.3. Medidas de Segurança de Pessoal

6.3.1. Requisitos relativos às qualificações, experiência, antecedentes e credenciação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

6.3.2. Procedimento de verificação de antecedentes

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

6.3.3. Requisitos de formação e treino

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

6.3.4. Frequência e requisitos para ações de reciclagem

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

6.3.5. Frequência e sequência da rotação de funções

Nada a assinalar.

6.3.6. Sanções para ações não autorizadas

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

6.3.7. Requisitos para prestadores de serviços

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

6.3.8. Documentação fornecida ao pessoal

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

7. CONTROLOS TÉCNICOS DE SEGURANÇA

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

7.1. Geração e instalação do par de chaves

7.1.1. Geração do par de chaves

O par de chaves utilizado para a emissão do certificado ECD é gerado no Sistema da Entidade Certificadora de Documentos, a EC IAC certifica esse par de chaves através da emissão do certificado, certificado esse a ser utilizado no Sistema da Entidade Certificadora de Documentos para assinar os dados constantes no chip do Cartão Nacional de Identificação.

7.1.2. Chaves para efeitos de Assinatura Digital e Autenticação

Não aplicável

7.1.3. Chaves para efeitos de Confidencialidade

Não aplicável

7.1.4. Entrega da chave privada ao titular

Não aplicável

7.1.5. Entrega da chave pública ao emissor do certificado

A chave pública é entregue à EC IAC, em formato pkcs#10 (formato que contem a chave pública, assinada pela chave privada) para que esta a certifique assinando-a com a sua chave privada, dando origem ao certificado.

7.1.6. Disponibilização de chave pública da EC às partes confiantes

A chave pública da ECD é disponibilizada através do certificado emitido pela EC IAC.

7.1.7. Tamanho de chave

O comprimento dos pares de chaves deve ter o tamanho suficiente, de forma a prevenir possíveis ataques de criptanálise que descubram a chave privada correspondente ao par de chaves no seu período de utilização. A dimensão da chave para certificados emitidos para o serviço ECD é 2048 bits RSA.

7.1.8. Parâmetros de chave pública e verificação de qualidade

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

7.1.9. Utilização das Chaves (campo "key usage" X.509 v3)

De acordo com a secção 8.1.2

7.2. Proteção da chave privada e características do módulo criptográfico

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

7.2.1. Normas e medidas de segurança do módulo criptográfico

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

7.2.2. Controlo multi-pessoal (n de m) para a chave privada

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

7.2.3. Retenção da chave privada (key escrow)

Não é permitida a retenção de chaves privadas.

7.2.4. Cópia de segurança (backup) de chave privada

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

7.2.5. Arquivo da chave privada

Conforme especificado na Política de Segurança da ICP-CV.

7.2.6. Transferência da chave privada para/módulo criptográfico

Não aplicável.

7.2.7. Armazenamento da chave privada no módulo criptográfico

De acordo com a secção 6.2.1.

7.2.8. Método para ativação da chave privada

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

7.2.9. Método para desativação da chave privada

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

7.2.10. Padrões de referência do módulo criptográfico

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

7.3. Outros aspetos da manipulação do par de chaves

7.3.1. Arquivo da chave pública

O sistema de emissão de certificados utilizado pela EC IAC, guarda os certificados por ela emitidos, ficando assim armazenadas as chaves públicas.

7.3.2. Períodos de validade do certificado e das chaves

O período de utilização das chaves é determinado pelo período de validade do certificado, pelo que após expiração do certificado as chaves deixam de poder ser utilizadas, dando origem à cessação permanente da sua operacionalidade e da utilização que lhes foi destinada.

Neste sentido a validade dos certificados de equipamento tecnológico é de 6 anos, sendo utilizados durante o seu primeiro mês de validade, e reemitido após o primeiro mês de validade.

7.4. Dados de ativação

7.4.1. Geração e instalação dos dados de ativação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

7.4.2. Proteção dos dados de ativação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

7.4.3. Outros aspetos dos dados de ativação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

7.5. Medidas de segurança informática

7.5.1. Requisitos técnicos específicos

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

7.5.2. Avaliação/nível de segurança

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

7.6. Ciclo de vida das medidas técnicas de segurança

7.6.1. Medidas de desenvolvimento do sistema

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

7.6.2. Medidas de gestão de segurança

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

7.6.3. Ciclo de vida das medidas de segurança

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

7.7. Medidas de Segurança da Rede

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

7.8. Validação cronológica (Time-stamping)

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

8. PERFIL DE CERTIFICADO

8.1. 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 do uso de certificados digitais X.509 v3, que são estrutura de dados que fazem a ligação entre a chave pública e o seu titular. Esta ligação é afirmada através da assinatura digital de cada certificado por uma EC de confiança. A EC 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 limitado de validade, 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 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 ECs assinados por outras ECs[8].

O perfil do certificado de Entidade Certificadora de Documentos está de acordo com:

- Recomendação ITU.T X.509[9],
- RFC 5280[8],
- Política de Certificados da ICP-CV

8.1.1. Número da Versão

O campo "*version*" do certificado descreve a versão utilizada na codificação do certificado. Neste perfil, a versão utilizada é 3 (três).

[8] cf. RFC 5280. 2008, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.
[9] cf. ITU-T *Recommendation X.509. 1997, (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.*

8.1.2. Extensões do Certificado

As componentes e as extensões definidas para os certificados X.509 v3 fornecem métodos para associar atributos a utilizadores ou chaves públicas, assim como para gerir a hierarquia de certificação.

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[10]	Comentários
tbsCertificate	**Version**	4.1.2.1	2	m	O valor 2 identifica a utilização de certificado ITU-T X.509 versão 3
	Serial Number	4.1.2.2	<atribuído pela EC a cada certificado>	m	
	Signature	4.1.2.3	1.2.840.113549.1.1.11	m	Valor TEM que ser igual ao OID no *signatureAlgorithm* (abaixo)
	Issuer	4.1.2.4		m	
	Country (C)		"CV"		
	Organization (O)		"ICP-CV"		
	Organization Unit (OU)		"EC"		
	Common Name (CN)		"Entidade Certificadora de Identificação e Autenticação Civil" <nnnn>		
	Validity	4.1.2.5		m	TEM que utilizar tempo UTC até 2049, passando a partir daí a utilizar GeneralisedTime
	Not Before		<data de emissão>		

[10] O perfil utilize a terminologia seguinte para cada um dos tipos de campo no certificado X.509:
m – obrigatório (o campo TEM que estar presente)
o – opcional (o campo PODE estar presente)
c – crítico (a extensão é marcada crítica o que significa que as aplicações que utilizem os certificados TÊM que processar esta extensão).

	Not After		<data de emissão + 6 anos>		Utilizado para assinar objetos de segurança de Documentos durante o primeiro mês de validade e renovado (com geração de novo par de chaves) após o primeiro mês de validade.
	Subject	4.1.2.6		m	
	Country (C)		"CV"		
	Organization (O)		"Sistema Nacional de Identificação e Autenticação Civil de Cabo Verde"		
	Organization Unit (OU)		"Serviços Identificação e Autenticação Civil"		
	Organization Unit (OU)		"Entidades Certificadoras de Documentos"		
	Serial Number (serialNumber)		<nnnnnn>		nnnnnn – nº sequêncial, a iniciar 000001
	Common Name (CN)		"Entidade Certificadora de Documentos do Cartão Nacional de Identificação"		
	Subject Public Key Info	4.1.2.7		m	Utilizado para conter a chave pública e identificar o algoritmo com o qual a chave é utilizada (e.g., RSA, DSA ou Diffie-Hellman) .
	algorithm		1.2.840.113549.1.1.1		O OID rsaEncryption identifica chaves públicas RSA. pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 } rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1}

					O OID rsaEncryption deve ser utilizado no campo algorithm com um valor do tipo AlgorithmIdentifier. Os parâmetros do campo TÊM que ter o tipo ASN.1 a NULL para o identificador deste algoritmo.[11]
	subjectPublicKey		<Chave Pública com modulus n de 2048 bits>		
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		m	
	keyIdentifier		<O key Identifier é composto pela hash de 160-bit SHA-256 do valor da BIT STRING do subject key identifier do certificado do emissor (excluindo a tag, length, e número de bits não usado)>	m	
	Subject Key Identifier	4.2.1.2	<O key Identifier é composto pela hash de 160-bit SHA-256 do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>	m	
	Key Usage	4.2.1.3		mc	Esta extensão é marcada CRÍTICA.
	Digital Signature		"1" selecionado		
	Non Repudiation		"0" selecionado		
	Key Encipherment		"0" selecionado		

[11] *cf.* RFC 3279. 2002, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

	Data Encipherment		“0” selecionado		
	Key Agreement		“0” selecionado		
	Key Certificate Signature		“0” selecionado		
	CRL Signature		“0” selecionado		
	Encipher Only		“0” selecionado		
	Decipher Only		“0” selecionado		
	Certificate Policies	4.2.1.5		m	
	policyIdentifier		2.16.132.1.3.2.1.1	m	Identificador da Declaração de Práticas de Certificação da EC IAC.
	policyQualifiers		policyQualiflierID: 1.3.6.1.5.5.7.2.1 *cPSuri*: http://pki.cni.gov.cv/pub/pol/dpc_eciac.html	o	Valor do OID: 1.3.6.1.5.5.7.2.1 (id-qt-cps PKIX CPS Pointer Qualifier) Descrição do OID: "O atributo cPSuri contém um apontador para a Declaração de Práticas de Certificação publicada pela EC. O apontador está na forma de um URI." (http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.1.html)
	policyIdentifier		2.16.132.1.2.2.1.2.1	m	Identificador da Política de Certificados de Entidade Certificadora de Documentos.

	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.2 cPSuri: “http://pki.cni.gov.cv/pub/pol/pc_ecd.html”	o	Valor do OID: 1.3.6.1.5.5.7.2.2 (id-qt-unotice) Descrição do OID: "O atributo cPSuri contém um apontador para a Política de Certificado publicada pela EC. O apontador está na forma de um URI." (http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.2.html)
	Basic Constraints	4.2.1.10		mc	Esta extensão é marcada obrigatória e CRÍTICA.
	CA		FALSE		
	PathLenConstraint		0		
	CRLDistributionPoints	4.2.1.14		o	
	distributionPoint		http://pki.cni.gov.cv/pub/lrc/eciac0001.crl	o	
	Internet Certificate Extensions				
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha256WithRSAEncryption {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1)
	Signature Value	4.1.1.3	<contém a assinatura digital emitida pela EC>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (subject) do certificado.

8.1.3. OID do Algoritmo

O campo "*signatureAlgorithm*" do certificado contém o OID do algoritmo criptográfico utilizado pela EC para assinar o certificado: 1.2.840.113549.1.1.11 (sha-256WithRSAEncryption[12]).

8.1.4. Formato dos Nomes

Tal como definido na secção 4.1.2.

8.1.5. Condicionamento nos Nomes

Para garantir a total interoperabilidade entre as aplicações que utilizam certificados digitais, aconselha-se (mas não se obriga) a que apenas caracteres alfanuméricos não acentuados, espaço, traço de sublinhar, sinal negativo e ponto final ([a-z], [A-Z], [0-9], ' ', '_', '-', '.') sejam utilizados em entradas do Diretório X.500. A utilização de caracteres acentuados será da única responsabilidade do Comissão Executiva da EC.

8.1.6. OID da Política de Certificados

A extensão "*certificate policies*" contém a sequência de um ou mais termos informativos sobre a política, cada um dos quais consiste num identificador da política e qualificadores opcionais.

Os qualificadores opcionais ("*policyQualifIierID*: 1.3.6.1.5.5.7.2.1" e "*cPSuri*") apontam para o URI onde pode ser encontrada a Declaração de Práticas de Certificação com o OID identificado pelo "*policyIdentifier*". Os qualificadores opcionais ("*policyQualifIierID*: 1.3.6.1.5.5.7.2.2" e "*userNotice explicitText*") apontam para o URI onde pode ser encontrados a Politica de Certificados com o OID identificado pelo "*policyIdentifier*" (i.e., este documento).

8.1.7. Utilização da extensão Policy Constraints

Nada a assinalar.

8.1.8. Sintaxe e semântica do qualificador de política

A extensão "*certificate policies*" contém um tipo de qualificador de política a ser utilizado pelos emissores dos certificados e pelos escritores da política de certificados. O tipo de qualificador é o "*cPSuri*" que contém

[12] sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1)

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 Politica de Certificados.

8.1.9. Semântica de processamento para a extensão crítica Certificate Policies

Nada a assinalar.

9. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

9.1.1. Procedimentos de mudança de especificação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

9.1.2. Políticas de publicação e notificação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

9.1.3. Procedimentos para aprovação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC IAC (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html.pdf).

Referências Bibliográficas

ANAC, Estrutura da Declaração de Práticas de Certificação.

ANAC, Política de Certificados da ICP-CV e Requisitos mínimos de Segurança.

Portaria nº 2/2008, de 28 de Janeiro;

Decreto-Lei nº44/2009 de 9 de Novembro;

Decreto Regulamentar nº. 18/2007, de 24 de Dezembro;

Decreto-Lei nº 33 /2007, de 24 de Setembro;

Portaria nº 4/2008

FIPS 140-1. 1994, *Security Requirements for Cryptographic Modules.*

ISO/IEC 3166. 1997, *Codes for the representation of names and countries and their subdivisions.*

ITU-T Recommendation X.509. 1997, (1997 E): *Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.*

NIST FIPS PUB 180-1. 1995, *The Secure Hash Algorithm (SHA-1). National Institute of Standards and Technology, "Secure Hash Standard,", U.S. Department of Commerce.*

RFC 1421. 1993, *Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures.*

RFC 1422. 1993, *Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management.*

RFC 1423. 1993, *Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers.*

RFC 1424. 1993, *Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services.*

RFC 2252. 1997, *Lightweight Directory Access Protocol (v3).*

RFC 2986. 2000, PKCS #10: *Certification Request Syntax Specification, version 1.7.*

RFC 3279. 2002, *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*

RFC 5280. 2008, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*

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

RFC 4210. 2005, *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP).*