Política de Certificados de Validação Cronológica

Políticas

PJ.CNICV_24.1.2_0005_pt

Versão: 1.0

Data: 14.07.2022

Responsável: SNIAC

Classificação: Público

Identificador do documento: PJ.CNICV_24.1.2_0005_pt

Tipologia documental: Políticas

Título: Política de Certificados de Validação Cronológica

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 14.07.2022

Versão actual: 1.0

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 S.A.

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 electrónico (*eGovernment*), o Cartão Nacional de Identificação fornece os mecanismos necessários para a autenticação digital forte da identidade do Cidadão perante os serviços da Administração Pública, assim como as assinaturas eletrónicas indispensáveis aos processos de desmaterialização que estão a ser disponibilizados pelo Estado.

A infra-estrutura da Entidade de Certificação do Cartão Nacional de Identificação (ou Entidade de Certificação do Cidadão) fornece uma hierarquia de confiança, que promoverá a segurança eletrónica do Cidadão no seu relacionamento com o Estado. A Entidade de Certificação do Cidadão estabelece uma estrutura de confiança eletrónica que proporciona a realização de transacções eletrónicas seguras, a autenticação forte, um meio de assinar electronicamente transacções ou informações e documentos electrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transacções ou informação.

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

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

[1] *cf.* PJ.CNICV_24.1.1_0001_pt_IAC.doc. 2010, Declaração de Práticas de Certificação da EC Identificação e Autenticação Civil.

CONTROLO DA DOCUMENTAÇÃO

Responsável	**Equipa de Implementação do SNIAC**

I - Informações do Cliente

Nome	**Endereço**	**Email**
Juvenal Pereira (*MJT / **SNIAC** / Presidente CI*)	Rua Cidade do Funchal – Meio de Achada St António Praia, Cabo Verde, CP 286/A T. 3337266 M. (00238) 5160283 | 9180233	juvenal.pereira@mj.gov.cv

II - Histórico de versões e Aprovação

Versão	**Implementado**	**Revisto**	**Aprovação**	**Homologação**
1.0	Nome	Nome	Juvenal Pereira – Presidente da Equipa do SNIAC	Ministério da Justiça e Trabalho
Data__/__/___	Data__/__/___	Data__/__/___	Data__/__/___	Data__/__/___

III - Informações de Contacto

Nome	**Endereço**	**Email**

IV - Histórico de Alterações

Versão	**Data**	**Autor**	**Descrição das alterações**

Sumário

Introdução

Objetivos

O objetivo deste documento é definir as políticas utilizadas na emissão do certificado de Validação Cronológica, pela Entidade de Certificação do Cartão Nacional de Identificação (EC Identificação e Autenticação Civil).

Público-Alvo

Este documento deve ser lido por:

- Recursos humanos atribuídos aos grupos de trabalho da EC Identificação e Autenticação Civil,
- Terceiras partes encarregues de auditar a EC Identificação e Autenticação Civil,
- Todo o público, em geral.

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 Identificação e Autenticação Civil[1], presumindo-se que o leitor leu integralmente o seu conteúdo antes de iniciar a leitura deste documento.

1 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 pelo que se pretende 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 Validação Cronológica, emitido pela EC Identificação e Autenticação Civil.

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.

1.1 Visão Geral

Esta PC satisfaz e complementa os requisitos impostos pela Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil[1].

1.2 Designação e Identificação do Documento

Este documento é a Política de Certificados do certificado de Validação Cronológica. A PC é representada num certificado através de um número único designado de "identificador de objecto" (OID), indicado na tabela abaixo.

Este documento é identificado pelos seguintes dados:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 1.0
Estado do Documento	Aprovado
OID	2.16.132.1.2.6
Data de Emissão	14.07.2022
Validade	2 anos
Localização	http://pki.cni.gov.cv/pub/pol/pc_tsa.html.pdf

1.3 Participantes

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 4.2 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

1.4 Dados de Contacto

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 4.3.2 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2 Disposições Gerais

2.1 Obrigações e Direitos

Toda a informação inerente a esta secção consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 5.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2.1.1 Obrigações da EC

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 5.1.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2.1.2 Obrigações das Unidades de Registo

Nada a assinalar.

2.1.3 Obrigações dos Titulares de Certificados

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 5.1.3 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2.1.4 Obrigações das partes confiantes

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 5.1.4 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2.1.5 Obrigações do Repositório

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 5.1.5 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2.2 Responsabilidades

2.2.1 Responsabilidades da EC

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 5.2.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2.2.2 Responsabilidades das Unidades de Registo

Nada a assinalar.

2.3 Responsabilidade Financeira

2.3.1 Indemnização devida pela terceira parte

Nada a assinalar.

2.3.2 Relações fiduciárias

Nada a assinalar.

2.4 Interpretação e execução

2.4.1 Legislação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 12.11 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2.4.2 Forma de interpretação e notificação

Nada a assinalar.

2.4.3 Procedimentos para a resolução de disputas

Nada a assinalar.

2.5 Taxas de serviço

2.5.1 Taxas de emissão e renovação de certificados

Nada a assinalar.

2.5.2 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.

2.5.3 Taxas para outros serviços

Nada a assinalar.

2.5.4 Política de reembolso

Nada a assinalar.

2.6 Publicação e repositório

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 5.3 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2.6.1 Frequência da publicação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 5.3.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2.6.2 Controlo de acesso

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 5.3.2 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2.6.3 Repositórios

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 5.3 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2.7 Auditoria de Conformidade

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 5.4 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2.7.1 Frequência ou motivo da auditoria

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 5.4.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2.7.2 Identidade e qualificações do auditor

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 5.4.2 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2.7.3 Relação entre o auditor e a Entidade Certificadora

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 5.4.3 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2.7.4 Âmbito da auditoria

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 5.4.4 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2.7.5 Procedimentos após uma auditoria com resultado deficiente

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 5.4.5 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2.7.6 Comunicação de resultados

2.8 Sigilo

2.8.1 Divulgação de Informação de Revogação e de Suspensão de Certificado

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 5.5.2 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2.8.2 Quebra de sigilo por motivos legais

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 5.5.3 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2.8.3 Informações a terceiros

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 5.5.4 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

2.8.4 Divulgação por solicitação do titular

Não aplicável.

2.8.5 Direitos de propriedade intelectual

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 5.5.6 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

3 Identificação e Autenticação

3.1 Registo Inicial

3.1.1 Disposições Legais

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 6.1.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

3.1.2 Tipos de nomes

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

O nome único do certificado do Serviço de Validação Cronológica do Cartão Nacional de Identificação 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	Serviço de Validação Cronológica
Serial number	serialNumber	<nnnnnn>[2]
Common Name	CN	Serviço de Validação Cronológica do Cartão Nacional de Identificação

[2] <nnnnnn> é um valor sequencial iniciado em "000001" na emissão do primeiro certificado deste tipo.

3.1.3 Necessidade de nomes significativos

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 6.1.3 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

3.1.4 Unicidade de nomes

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 6.1.5 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

3.1.5 Procedimento para resolver disputa de nomes

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 6.1.6 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

3.1.6 Reconhecimento, autenticação, e função das marcas registadas

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 6.1.7 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

3.1.7 Método de comprovação da posse de chave privada

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 6.1.8 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

3.1.8 Autenticação da identidade de uma pessoa singular

Nada a assinalar.

3.1.9 Autenticação da identidade de uma pessoa coletiva

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 6.1.10 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

3.1.9.1 Disposições Gerais

3.1.9.2 Documentos para efeitos de identificação de Certificado de equipamento tecnológico

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 6.1.12 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

3.1.9.3 Informações Certificado de equipamento tecnológico

A EC IAC guarda toda a documentação utilizada para verificação da identidade do patrocinador, garantindo que o mesmo tem os poderes bastantes de representante nomeado pela entidade para a emissão do certificado digital. O documento que serve de base ao registo do pedido do certificado de equipamento tecnológico contém, entre outros, os seguintes elementos:

a) Denominação legal da pessoal coletiva (i.e., organismo da dependência do MJT);
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;
c) Nome completo, número do bilhete de identidade ou qualquer outro elemento que permita a identificação inequívoca das pessoas singulares que estatutária ou legalmente a representam;
d) Endereço e outras formas de contacto;
e) Indicação de que o certificado digital de equipamento tecnológico é emitido para a entidade, na hierarquia de confiança da ICP-CV, de acordo com a presente DPC;
f) Nome único (DN) a ser atribuído ao certificado;
g) Informação relativas à identificação e aos poderes do(s) patrocinador(es) nomeados pela entidade para efetuar presencialmente o pedido do certificado digital de equipamento tecnológico (apresentado mediante o preenchimento de formulário próprio[3] e do fornecimento do pedido de certificado no formato PKCS#10);
h) Outras informações relativas ao formato do pedido de certificado, assim como ao conteúdo do DN do certificado.

O certificado e restantes dados necessários serão entregues ao patrocinador pelo método "cara-a-cara", sendo tal ato registado através do preenchimento e assinatura de formulário[4] que é arquivado pela EC IAC.

3.1.9.4 Validação de Autoridade

Nada a assinalar.

3.1.10 Critérios para interoperabilidade

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 6.2 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

[3] cf. PJ.CNICV_53.2.1_0002_pt_IAC.doc, Formulário de emissão de certificado de equipamento tecnológico emitido pela EC de Identificação e Autenticação Civil.
[4] cf. PJ.CNICV_53.2.4_0002_pt_IAC.doc, Formulário de receção de certificado de equipamento tecnológico emitido pela EC de Identificação e Autenticação Civil.

3.2 Identificação e Autenticação para pedidos de renovação de chaves

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 6.3 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

3.3 Identificação e autenticação para pedido de revogação

Qualquer entidade integrada no domínio da ICP-CV, pode solicitar a revogação de um determinado certificado, havendo conhecimento ou suspeita de comprometimento da chave privada do titular ou qualquer outro ato que recomende esta acção[5].

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[5] 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;

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

4 Requisitos operacionais do ciclo de vida do certificado

4.1 Pedido de Certificado

4.1.1 Requisitos

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 7.1.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

4.1.2 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.

4.1.3 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[6]) do PKCS#10, em formato PEM, pelo patrocinador;
- Arquivo do PKCS#10 e *hash* num CD/DVD, pelo patrocinador;
- Preenchimento, pelo patrocinador, do documento de validação da identidade da entidade, de acordo com secção 3.1.9.3;
- Envio do CD/DVD e do documento corretamente preenchido ao contacto da EC IAC.

4.2 Processamento do pedido de certificado

4.2.1 Requisitos

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 7.2.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

[6] 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.

4.2.2 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 3.1.9.3 – 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[7].

4.2.3 Aprovação ou recusa de pedidos de certificado

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 7.2.3 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

4.2.4 Prazo para processar o pedido de certificado

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 7.2.4 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

4.3 Emissão de Certificado

4.3.1 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;
- Três (3) membros dos Grupos 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.

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

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

- Identificação e autenticação de todas as pessoas presentes na intervenção, garantindo que o patrocinador e os membros dos Grupos de Trabalho têm os poderes necessários para os atos a praticar;
- O patrocinador entrega, em mão, o CD/DVD e o formulário de emissão[8] 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 em formato PEM;
- Os membros do Grupo de Trabalho da EC IAC arquivam o certificado em formato PEM num CD/DVD e preenchem o formulário de receção e aceitação de certificado[9], 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 CD/DVD com o certificado em formato PEM 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.

4.3.2 Notificação da emissão do certificado ao titular

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

4.4 Aceitação do Certificado

4.4.1 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 4.3.1).

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.

[8] cf. PJ.CNICV_53.2.1_0002_pt_IAC, Formulário de emissão de certificado de Equipamento Tecnológico
[9] cf. PJ.CNICV_53.2.4_0002_pt_IAC.doc, Formulário de receção de certificado de Equipamento Tecnológico

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.

4.4.2 Publicação do certificado

Os certificados TSA emitidos são publicados no repositório da PKI disponível em http://pki.cni.gov.cv/.

4.4.3 Notificação da emissão de certificado a outras entidades

Nada a assinalar.

4.5 Uso do certificado e par de chaves pelo titular

A EC de Identificação e Autenticação Civil é a titular do certificado de Validação cronológica, sendo o mesmo emitido para o servidor de validação cronológica da EC Identificação e Autenticação Civil. A chave privada associada a este tipo de certificados é utilizada para assinar as respostas a pedidos de validações cronológicas[10], garantindo e permitindo verificar a integridade e não-repúdio dessas mesmas respostas.

4.5.1 Uso do certificado e da chave pública pelas partes confiantes

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 7.5.2 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

4.6 Renovação de Certificados

4.6.1 Renovação de Certificados

Esta prática não é suportada na ICP-CV.

4.7 Modificação de Certificados

Esta prática não é suportada na ICP-CV

[10] *cf.* RFC 3161. 2001, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

4.8 Suspensão e revogação de certificado

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 7.9 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

4.8.1 Circunstâncias para revogação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 7.9.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

4.8.2 Quem pode submeter o pedido de revogação

Está legitimado para submeter o pedido de revogação, sempre que se verifiquem alguma das condições descritas na secção 4.8.1, 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 equipamento tecnológico.

4.8.3 Procedimento para o pedido de revogação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 7.9.3 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

4.8.4 Prazo para processar o pedido de revogação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 7.9.5 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

4.8.5 Motivos para suspensão

Nada a assinalar.

4.8.6 Quem pode pedir o pedido de suspensão

Nada a assinalar.

4.8.7 Procedimentos para pedido de suspensão

Nada a assinalar.

4.8.8 Limite do período de suspensão

Nada a assinalar.

4.8.9 Frequência de emissão de LCR

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 7.9.8 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

4.8.10 Requisitos de verificação on-line de revogação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 7.9.11 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

4.8.11 Outras formas disponíveis para divulgação de revogação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 7.9.12 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

4.8.12 Disponibilidade de verificação on-line do estado / revogação de certificado

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 7.9.10 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

4.8.13 Requisitos especiais em caso de comprometimento de chave privada

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 7.9.13 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

4.9 Serviços sobre o estado certificado

4.9.1 Características operacionais

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 7.10.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

4.9.2 Disponibilidade do serviço

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 7.10.2 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

4.9.3 Características opcionais

Nada a assinalar.

4.10 Fim de subscrição

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 7.11 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

4.11 Retenção e recuperação de chaves (*Key escrow*)

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 7.18 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

4.11.1 Políticas e práticas de recuperação de chaves

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 7.18.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

4.11.2 Políticas e práticas de encapsulamento e recuperação de chaves de sessão

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 7.18.2 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

5 Medidas de segurança física, de gestão e operacionais

5.1 Medidas de segurança física

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 8.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

5.1.1 Construção e Localização Física das Instalações da EC

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 8.1.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

5.1.2 Acesso físico ao local

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 8.1.2 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

5.1.3 Energia e ar condicionado

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 8.1.3 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

5.1.4 Exposição à água

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 8.1.4 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

5.1.5 Prevenção e proteção contra incêndio

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 8.1.5 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

5.1.6 Salvaguarda de suportes de armazenamento

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 8.1.6 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

5.1.7 Eliminação de resíduos

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 8.1.7 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

5.1.8 Instalações externas (alternativa) para recuperação de segurança

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 8.1.8 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

5.2 Medida de segurança dos processos

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 8.2 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

5.2.1 Funções de Confiança

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 8.2.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

5.2.2 Número de pessoas exigidas por tarefa

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 8.2.2 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

5.2.3 Identificação e Autenticação para cada função

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 8.2.3 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

5.3 Medidas de Segurança de Pessoal

5.3.1 Requisitos relativos às qualificações, experiência, antecedentes e credenciação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 8.3.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

5.3.2 Procedimento de verificação de antecedentes

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 8.3.2 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

5.3.3 Requisitos de formação e treino

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 8.3.3 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

5.3.4 Frequência e requisitos para ações de reciclagem

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 8.3.4 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

5.3.5 Frequência e sequência da rotação de funções

Nada a assinalar.

5.3.6 Sanções para ações não autorizadas

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 8.3.6 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

5.3.7 Requisitos para prestadores de serviços

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 8.3.7 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

5.3.8 Documentação fornecida ao pessoal

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 8.3.8 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

6 Controlos Técnicos de Segurança

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 9 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

6.1 Geração e instalação do par de chaves

6.1.1 Geração do par de chaves

O par de chaves utilizado para a emissão do certificado da TSA é gerado no Sistema de Validação Cronológica, a EC IAC certifica esse par de chaves através da emissão do certificado, certificado esse a ser utilizado no Sistema de Validação Cronológica para assinar as respostas a pedidos de validações cronológicas, garantindo e permitindo verificar a integridade e não-repúdio dessas mesmas respostas e garantindo a data e hora da ocorrência.

6.1.2 Chaves para efeitos de Assinatura Digital e Autenticação

Não aplicável

6.1.3 Chaves para efeitos de Confidencialidade

Não aplicável

6.1.4 Entrega da chave privada ao titular

Não aplicável

6.1.5 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.

6.1.6 Disponibilização de chave pública da EC às partes confiantes

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

6.1.7 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 equipamento tecnológico é a seguinte de 2048 bits RSA.

6.1.8 Parâmetros de chave pública e verificação de qualidade

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 9.1.6 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

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

De acordo com a secção 7.1.2

6.2 Proteção da chave privada e características do módulo criptográfico

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 9.2 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

6.2.1 Normas e medidas de segurança do módulo criptográfico

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 9.2.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

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

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 9.2.2 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

6.2.3 Retenção da chave privada (*key escrow*)

Não é permitida a retenção de chaves privadas.

6.2.4 Cópia de segurança (backup) de chave privada

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 9.2.4 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

6.2.5 Arquivo da chave privada

Conforme especificado na Política de Segurança da ICP-CV.

6.2.6 Transferência da chave privada para/módulo criptográfico

Não aplicável.

6.2.7 Armazenamento da chave privada no módulo criptográfico

De acordo com a secção 6.2.1.

6.2.8 Método para ativação da chave privada

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 9.2.8 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

6.2.9 Método para desativação da chave privada

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 9.2.9 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

6.2.10 Padrões de referência do módulo criptográfico

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 9.2.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

6.3 Outros aspetos da manipulação do par de chaves

6.3.1 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.

6.3.2 Períodos de validade do certificado e das chaves

O certificado de equipamento tecnológico, neste caso o certificado TSA, tem um período de validade de 6 anos, sendo que a sua renovação ocorre anualmente.

O período de utilização da chave privada do certificado TSA é de 1 ano e 2 meses, findo esse período é utilizada a chave privada de um novo certificado TSA para aposição dos selos temporais.

6.4 Dados de ativação

6.4.1 Geração e instalação dos dados de ativação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 9.4.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

6.4.2 Proteção dos dados de ativação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 9.4.2 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

6.4.3 Outros aspetos dos dados de ativação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 9.4.3 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

6.5 Medidas de segurança informática

6.5.1 Requisitos técnicos específicos

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 9.5.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

6.5.2 Avaliação/nível de segurança

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 9.5.2 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

6.6 Ciclo de vida das medidas técnicas de segurança

6.6.1 Medidas de desenvolvimento do sistema

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 9.6.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

6.6.2 Medidas de gestão de segurança

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 9.6.2 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

6.6.3 Ciclo de vida das medidas de segurança

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 9.6.3 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

6.7 Medidas de Segurança da Rede

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 9.7 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

6.8 Validação cronológica (*Time-stamping*)

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 9.8 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

7 Perfil de Certificado

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 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.

O perfil do certificado de Validação Cronológica está de acordo com:

- Recomendação ITU.T X.509[11],
- RFC 5280,
- Política de Certificados da ICP-CV.

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

7.1.1 Número da Versão

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

7.1.2 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.

Cerificate Component		Section in RFC 5280	Value	Field Type	Comments
tbsCertificate	**Version**	4.1.2.1	2	m	O valor 2 identifica a utilização de certificados 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>		
	Not After		<data de emissão + 6 anos>		Utilizado para assinar objetos de tempo, com período de utilização da chave privada, período de validade do certificado e prazo de renovação de acordo com o indicado na secção 6.3.2.
	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 de Identificação e Autenticação Civil"		
	Organization Unit (OU)		"Serviço de Validação Cronológica"		
	Serial Number (serialNumber)		<nnnnnn>		nnnnnn – nº sequêncial, a iniciar 000001
	Common Name (CN)		"Serviço de Validação Cronológica 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 (*cf.* RFC 3279. 2002, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile)
	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 obrigatória e CRÍTICA.
	Digital Signature		"1" selecionado		
	Non Repudiation		"1" selecionado		
	Key Encipherment		"0" selecionado		
	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	m	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		2.16.132.1.2.6	m	Identificador da Política de Certificados de Validação Cronológica.
	policyQualifiers		policyQualiflierID: 1.3.6.1.5.5.7.2.2 cPSuri: "http://pki.cni.gov.cv/pub/pol/pc_tsa.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 como obrigatória e CRÍTICA.
	CA		FALSE		
	PathLenConstraint		0		
	Extended Key Usage	4.2.1.13		c	
	TimeStamping		id-kp-timeStamping		Descrição do OID: indica que o certificado é utilizado para ligar um objeto a uma hora e data obtida de uma fonte fiável de tempo. Esta extensão TEM de ser crítica[10].
	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(11)
	Signature Value	4.1.1.3	<contains digital signature issued by the EC>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (subject) do certificado.

7.1.3 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]).

7.1.4 Formato dos Nomes

Tal como definido na secção 3.1.2

7.1.5 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 Grupo de Trabalho de Gestão da EC.

7.1.6 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 ("*policyQualifierID*: 2.16.132.1.3.2.1.1" 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 ("*policyQualifierID*: 2.16.132.1.2.6" 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).

7.1.7 Utilização da extensão *Policy Constraints*

Nada a assinalar.

7.1.8 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 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.

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

7.1.9 Semântica de processamento para a extensão crítica *Certificate Policies*

Nada a assinalar.

8 Administração de Especificação

8.1.1 Procedimentos de mudança de especificação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 11.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

8.1.2 Políticas de publicação e notificação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 11.1.1 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

8.1.3 Procedimentos para aprovação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil, na secção 11.1.2 (http://pki.cni.gov.cv/pub/pol/dpc_eciac.html).

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.*

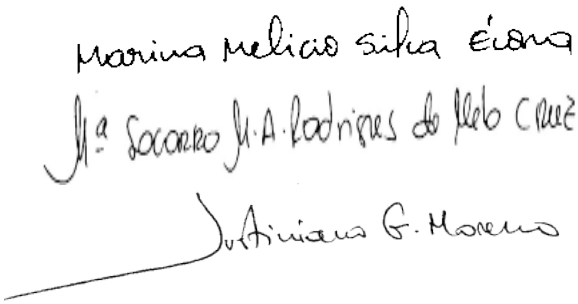
RFC 5280. 2008, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*

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).*

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

Aprovação do Conselho Executivo



João Cruz

Assinado de forma digital por João Cruz
DN: email=jcruz@gov.cv, cn=João Cruz, serialNumber=CV-19850505M017Y, givenName=João, sn=Cruz, title=Diretor Nacional da Modernização do Estado, ou=DNME, ou=Certificado para pessoa singular - Assinatura Qualificada, o=Direção Nacional da Modernização do Estado, l=Praia, st=Santiago, c=CV
Dados: 2022.08.04 10:22:37 -01'00'