Política de Certificado da EC do Cartão Nacional de Identificação

Políticas

PJ.CNICV_24.1.2_0002_pt_eID

Versão: 3.0

Data: 06/2021

Classificação: Público

Identificador do documento: PJ.CNICV_24.1.2_0002_pt_eID

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	15/07/2010	Versão inicial	MULTICERT
2.0	25/10/2019	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_0002_pt_eID.pdf	Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação	MULTICERT
PJ.CNICV_24.1.1_0001_pt_IAC	Declaração de Práticas de Certificação da EC 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 da Entidade de Certificação 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 Entidade de Certificação 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 Raiz de Cabo Verde Cartão 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 do Cartão Nacional de Identificação, 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

Resumo Executivo 3

Conteúdo 4

1. POLÍTICA DE CERTIFICADO DA EC DO CARTÃO NACIONAL DE IDENTIFICAÇÃO 10

1.1. Objetivo e Âmbito 10

1.2. Público-Alvo 10

1.3. Estrutura do Documento 10

2. CONTEXTO GERAL 10

2.1. Visão Geral 11

2.2. Designação e Identificação do Documento 11

2.3. Participantes 11

2.4. Dados de Contacto 11

3. DISPOSIÇÕES LEGAIS 12

3.1. Obrigações e Direitos 12

3.1.1. Obrigações da EC 12

3.1.2. Obrigações das Unidades de Registo 12

3.1.3. Obrigações dos Titulares de Certificados 12

3.1.4. Direito das partes confiantes 12

3.1.5. Obrigações de Repositório 12

3.2. Responsabilidades 12

3.2.1. Responsabilidades da EC 12

3.2.2. Responsabilidades das Unidades de Registo 13

3.3. Responsabilidade Financeira 13

3.3.1. Indemnização devida pela terceira parte 13

3.3.2. Relações fiduciárias 13

3.4. Interpretação e execução 13

3.4.1. Legislação 13

3.4.2. Forma de interpretação e notificação 13

3.4.3. Procedimentos para a resolução de disputas 13

3.5. Taxas de serviço 13

3.5.1. Taxas de emissão e renovação de certificados 13

3.5.2. Taxas de revogação ou de acesso à informação de status 13

3.5.3. Taxas para outros serviços 14

3.5.4. Política de reembolso 14

3.6. Publicação e repositório 14
3.6.1. Frequência da publicação 14
3.6.2. Controlo de acesso 14
3.6.3. Repositórios 14
3.7. Auditoria de Conformidade 14
3.7.1. Frequência ou motivo da auditoria 14
3.7.2. Identidade e qualificações do auditor 15
3.7.3. Relação entre o auditor e a Entidade Certificadora 15
3.7.4. Âmbito da auditoria 15
3.7.5. Procedimentos após uma auditoria com resultado deficiente 15
3.7.6. Comunicação de resultados 15
3.8. Sigilo 15
3.8.1. Divulgação de Informação de Revogação e de Suspensão de Certificado 15
3.8.2. Quebra de sigilo por motivos legais 15
3.8.3. Informações a terceiros 16
3.8.4. Divulgação por solicitação do titular 16
3.8.5. Direitos de propriedade intelectual 16
4. IDENTIFICAÇÃO E AUTENTICAÇÃO 16
4.1. Registo Inicial 16
4.1.1. Disposições Legais 16
4.1.2. Tipos de nomes 16
4.1.3. Necessidade de nomes significativos 17
4.1.4. Necessidade de nomes significativos 17
4.1.5. Unicidade de nomes 17
4.1.6. Procedimento para resolver disputa de nomes 17
4.1.7. Método de comprovação da posse de chave privada 17
4.1.8. Autenticação da identidade de uma pessoa singular 18
4.1.9. Autenticação da identidade de uma pessoa coletiva 18
4.1.9.1. Documentos para efeitos de identificação de pessoa coletiva 18
4.1.9.2. Informações Certificado de equipamento tecnológico 18
4.1.9.3. Validação de Autoridade 18
4.1.10. Critérios para interoperabilidade 18
4.2. Identificação e Autenticação para pedidos de renovação de chaves 18
4.3. Identificação e autenticação para pedido de revogação 18

5. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO 19
5.1. Pedido de Certificado 19
5.1.1. Requisitos 19
5.1.2. Quem pode subscrever um pedido de certificado? 19
5.1.3. Processo de registo e responsabilidades 19
5.2. Processamento do pedido de certificado 19
5.2.1. Requisitos 19
5.2.2. Processos para a identificação e funções de autenticação 19
5.2.3. Aprovação ou recusa de pedidos de certificado 19
5.2.4. Prazo para processar o pedido de certificado 19
5.3. Emissão de Certificado 20
5.3.1. Procedimentos para a emissão de certificado 20
5.3.2. Notificação da emissão do certificado ao titular 20
5.4. Aceitação do Certificado 20
5.4.1. Procedimentos para a aceitação de certificado 20
5.4.2. Publicação do certificado 20
5.4.3. Notificação da emissão de certificado a outras entidades 20
5.5. Uso do certificado e par de chaves 20
5.5.1. Uso do certificado e da chave privada pelo titular 20
5.5.2. Uso do certificado e da chave pública pelas partes confiantes 21
5.6. Renovação de Certificados 21
5.6.1. Renovação de Certificados 21
5.6.2. Motivos para renovação de certificado 21
5.6.3. Quem pode submeter o pedido de renovação de certificado 21
5.6.4. Processamento do pedido de renovação de certificado 21
5.6.5. Notificação de emissão de novo certificado ao titular 21
5.6.6. Procedimentos para aceitação de certificado 21
5.6.7. Publicação de certificado após renovação 21
5.6.8. Notificação da emissão do certificado a outras entidades 21
5.7. Modificação de Certificados 22
5.8. Suspensão e revogação de certificado 22
5.8.1. Circunstâncias para revogação 22
5.8.2. Quem pode submeter o pedido de revogação 22
5.8.3. Procedimento para o pedido de revogação 22

5.8.4. Prazo para processar o pedido de revogação 22
5.8.5. Motivos para suspensão 23
5.8.6. Quem pode pedir o pedido de suspensão 23
5.8.7. Procedimentos para pedido de suspensão 23
5.8.8. Limite do período de suspensão 23
5.8.9. Frequência de emissão de LCR 23
5.8.10. Requisitos de verificação on-line de revogação 23
5.8.11. Outras formas disponíveis para divulgação de revogação 23
5.8.12. Disponibilidade de verificação on-line do estado / revogação de certificado 23
5.8.13. Requisitos especiais em caso de comprometimento de chave privada 23
5.9. Serviços sobre o estado certificado 24
5.9.1. Características operacionais 24
5.9.2. Disponibilidade do serviço 24
5.9.3. Características opcionais 24
5.10. Fim de subscrição 24
5.11. Retenção e recuperação de chaves (Key escrow) 24
5.11.1. Políticas e práticas de recuperação de chaves 24
5.11.2. Políticas e práticas de encapsulamento e recuperação de chaves de sessão 24
6. MEDIDAS DE SEGURANÇA FÍSICA, DE GESTÃO E OPERACIONAIS 25
6.1. Medidas de segurança física 25
6.1.1. Construção e Localização Física das Instalações da EC 25
6.1.2. Acesso físico ao local 25
6.1.3. Energia e ar condicionado 25
6.1.4. Exposição à água 25
6.1.5. Prevenção e proteção contra incêndio 25
6.1.6. Salvaguarda de suportes de armazenamento 25
6.1.7. Eliminação de resíduos 26
6.1.8. Instalações externas (alternativa) para recuperação de segurança 26
6.2. Medida de segurança dos processos 26
6.2.1. Funções de Confiança 26
6.2.2. Número de pessoas exigidas por tarefa 26
6.2.3. Identificação e Autenticação para cada função 26
6.3. Medidas de Segurança de Pessoal 26
6.3.1. Requisitos relativos às qualificações, experiência, antecedentes e credenciação 26

6.3.2. Procedimento de verificação de antecedentes 27
6.3.3. Requisitos de formação e treino 27
6.3.4. Frequência e requisitos para ações de reciclagem 27
6.3.5. Frequência e sequência da rotação de funções 27
6.3.6. Sanções para ações não autorizadas 27
6.3.7. Requisitos para prestadores de serviços 27
6.3.8. Documentação fornecida ao pessoal 27
7. CONTROLOS TÉCNICOS DE SEGURANÇA 27
7.1. Geração e instalação do par de chaves 28
7.1.1. Geração do par de chaves 28
7.1.2. Chaves para efeitos de Assinatura Digital e Autenticação 28
7.1.3. Chaves para efeitos de Confidencialidade 28
7.1.4. Entrega da chave privada ao titular 28
7.1.5. Entrega da chave pública ao emissor do certificado 28
7.1.6. Disponibilização de chave pública da EC às partes confiantes 28
7.1.7. Tamanho de chave 28
7.1.8. Parâmetros de chave pública e verificação de qualidade 29
7.1.9. Utilização das Chaves (campo “key usage” X.509 v3) 29
7.2. Proteção da chave privada e características do módulo criptográfico 29
7.2.1. Normas e medidas de segurança do módulo criptográfico 29
7.2.2. Controlo multi-pessoal (n de m) para a chave privada 29
7.2.3. Retenção da chave privada (key escrow) 29
7.2.4. Cópia de segurança (backup) de chave privada 29
7.2.5. Arquivo da chave privada 29
7.2.6. Transferência da chave privada para/módulo criptográfico 30
7.2.7. Armazenamento da chave privada no módulo criptográfico 30
7.2.8. Método para ativação da chave privada 30
7.2.9. Método para desativação da chave privada 30
7.2.10. Padrões de referência do módulo criptográfico 30
7.3. Outros aspetos da manipulação do par de chaves 30
7.3.1. Arquivo da chave pública 30
7.3.2. Períodos de validade do certificado e das chaves 30
7.4. Dados de ativação 31
7.4.1. Geração e instalação dos dados de ativação 31

7.4.2. Proteção dos dados de ativação 31
7.4.3. Outros aspetos dos dados de ativação 31
7.5. Medidas de segurança informática 31
7.5.1. Requisitos técnicos específicos 31
7.5.2. Avaliação/nível de segurança 31
7.6. Ciclo de vida das medidas técnicas de segurança 31
7.6.1. Medidas de desenvolvimento do sistema 31
7.6.2. Medidas de gestão de segurança 31
7.6.3. Ciclo de vida das medidas de segurança 32
7.7. Medidas de Segurança da Rede 32
7.8. Validação cronológica (Time-stamping) 32
8. PERFIL DE CERTIFICADO 32
8.1. Perfil de Certificado 32
8.1.1. Número da Versão 33
8.1.2. Extensões do Certificado 33
8.1.3. OID do Algoritmo 41
8.1.4. Formato dos Nomes 41
8.1.5. Condicionamento nos Nomes 41
8.1.6. OID da Política de Certificados 41
8.1.7. Utilização da extensão Policy Constraints 41
8.1.8. Sintaxe e semântica do qualificador de política 41
8.1.9. Semântica de processamento para a extensão crítica Certificate Policies 42
8.2. Perfil da lista de revogação de certificados 42
8.2.1. Número da Versão 42
8.2.2. Extensões da LRC da EC eID 43
9. ADMINISTRAÇÃO DE ESPECIFICAÇÃO 47
9.1. Procedimentos de mudança de especificação 47
9.2. Políticas de publicação e notificação 47
9.3. Procedimentos para aprovação 47
Referências Bibliográficas 48
Aprovação do Conselho Executivo ..... **Erro! Marcador não definido.**

1. POLÍTICA DE CERTIFICADO DA EC DO CARTÃO NACIONAL DE IDENTIFICAÇÃO

1.1. Objetivo e Âmbito

O objetivo deste documento é definir as políticas utilizadas na emissão do certificado de Entidade de Certificação do Cartão Nacional de Identificação, 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 CNI.
- Terceiras partes encarregues de auditar as Entidades Certificadoras,
- Todo o público, em geral.

1.3. Estrutura 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.

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 da Entidade Certificação do Cartão Nacional de Identificação.

Os Certificados emitidos pela EC eID contêm uma referência à 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.

2.2. Designação e Identificação do Documento

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

Este documento é identificado pelos dados seguintes:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão v3.000
Estado do Documento	Versão Final
OID	2.16.132.1.2.2.1.1.1
Data de Emissão	Junho 2021
Validade	1 ano
Localização	http://pki.cni.gov.cv/pub/pol/pc_eceid.html

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 LEGAIS

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

Nada a assinalar.

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

Nada a assinalar.

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

Não aplicável.

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 da EC eID é identificado por um nome único (DN – *Distinguished Name*) de acordo com *standard* X.500.

O nome único deste certificado emitido pela EC de eID 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	Entidades Certificadoras
Organization Unit	OU	Identificação e Autenticação Civil
Common Name	CN	Entidade Certificadora do Cartão Nacional de Identificação <nnnn>[2]

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. 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).

4.1.5. 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).

4.1.6. 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).

4.1.7. 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).

[2] <nnnn> é um valor sequencial iniciado em "0001" na emissão do primeiro certificado deste tipo.

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

Nada a assinalar.

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

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. 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?

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).

5.1.3. Processo de registo e responsabilidades

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. 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).

5.2.2. Processos para a identificação e funções de autenticação

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).

5.2.3. 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 Entidade de Certificação do Cartão Nacional de Identificação é uma entidade subordinada à EC IAC que partilha os mesmos recursos físicos e humanos. Desta forma a emissão do certificado da EC eID é feito de forma mais prática e na presença de pelo menos 1 elemento de cada grupo de trabalho.

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.

5.4. Aceitação do Certificado

5.4.1. Procedimentos para a aceitação de certificado

Conforme secção 5.3.1.

5.4.2. Publicação do 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).

5.4.3. 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 IAC é a titular do certificado da Entidade de Certificação do Cartão Nacional de Identificação (EC eID), utilizando a sua chave privada para a assinatura de certificados de EC subordinada, certificados de operação e serviços, assim como para a assinatura da respetiva Lista de Certificados Revogados (LRC), de acordo com a sua DPC.

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.

5.6.2. Motivos para renovação de certificado

Nada a assinalar.

5.6.3. Quem pode submeter o pedido de renovação de certificado

Nada a assinalar.

5.6.4. Processamento do pedido de renovação de certificado

Nada a assinalar.

5.6.5. Notificação de emissão de novo certificado ao titular

Nada a assinalar.

5.6.6. Procedimentos para aceitação de certificado

Nada a assinalar.

5.6.7. Publicação de certificado após renovação

Nada a assinalar.

5.6.8. Notificação da emissão do certificado a outras entidades

Nada a assinalar.

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) A EC IAC;

b) A Entidade Credenciadora;

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

A EC eID 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 seu certificado.

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

Nada a assinalar.

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

Nada a assinalar.

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

Nada a assinalar.

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

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).

7.1.1. Geração do par 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).

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

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).

7.1.6. Disponibilização de chave pública da EC às 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).

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 o certificado da EC eID é 4096 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

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).

7.2.6. Transferência da chave privada para/módulo criptográfico

Não aplicável.

7.2.7. Armazenamento da chave privada no 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).

7.2.8. 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

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).

7.3.2. 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 do certificado da EC eID é válido por um período de 10 anos e renovável de 2 em dois anos.

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 a 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 é assinado pela EC. Como a assinatura do certificado e a sua validade podem ser verificadas independentemente por qualquer *software* que utilize certificados, estes 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 Entidade Certificadora de Identificação Civil Eletrónica está de acordo com:

- Recomendação ITU.T X.509[3],
- RFC 5280[4]
- ETSI TS 101 862 e ETSI TS 102 280 e
- 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).

8.1.2. 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.

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

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[5]	Comentários
tbsCertificate	**Version**	4.1.2.1	2	m	O valor é 2 que 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>"		<nnnn> representa o número sequencial atribuído à EC
	Validity	4.1.2.5		m	TEM que utilizar tempo UTC até 2049, passando a partir daí a utilizar GeneralisedTime

[5] 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).

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[5]	Comentários
	Not Before		<data de emissão>		
	Not After		<data de emissão +10 anos>		Validade de 10 anos. Utilizado para assinar certificados durante os dois primeiros ano de validade e renovado (com geração de novo par de chaves) após os primeiros vinte meses 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)		"Entidades Certificadoras"		
	Organization Unit (OU)		"Identificação e Autenticação Civil"		
	Common Name (CN)		"Entidade Certificadora do Cartão Nacional de Identificação <nnnn>"		<nnnn> representa o número sequencial atribuído à EC
	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).

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[5]	Comentários
	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.[6]
	subjectPublicKey		<Chave Pública com modulus n de 2048 bits>		
	Unique Identifiers	4.1.2.8			O "*unique identifiers*" está presente para permitir a possibilidade de reutilizar os nomes do *subject* e/ou *issuer*[6].
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		o	
	keyIdentifier		<O key Identifier é composto pela hash de 160-bit SHA-1 do valor da BIT STRING do subject key identifier do certificado do emissor (excluindo a tag, length, e número de bits não usado)>	m	

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

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[5]	Comentários
	Subject Key Identifier	4.2.1.2	<O key Identifier é composto pela hash de 160-bit SHA-1 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		"0" selecionado		
	Non Repudiation		"0" selecionado		
	Key Encipherment		"0" selecionado		
	Data Encipherment		"0" selecionado		
	Key Agreement		"0" selecionado		
	Key Certificate Signature		"1" selecionado		
	CRL Signature		"1" selecionado		
	Encipher Only		"0" selecionado		
	Decipher Only		"0" selecionado		
	Certificate Policies	4.2.1.5		o	
	policyIdentifier		2.5.29.32.0	m	Identificador da Declaração de Práticas de Certificação da ECRCV.

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[5]	Comentários
					Valor do OID: 2.5.29.32.0 (AnyPolicy). Este policyIdentifier TEM de ser incluído.
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.1 cPSuri: http://ecrcv.cv/pub/pol/ec_raiz_cps_001_pt.html		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		2.16.132.1.3.2.1	m	Identificador da Declaração de Práticas de Certificação da EC IAC
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.1 cPSuri: http://pki.cni.gov.cv/pol/dpc_eciac.html	o	
	policyIdentifier		2.16.132.1.2.2.1.1.1	m	Identificador da Política de Certificados da EC do Cartão Nacional de Identificação
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.1 cPSuri: “http://pki.cni.gov.cv/pub/pol/pc_eceid.html”	o	Valor do OID: 1.3.6.1.5.5.7.2.1 (id-qt-cps PKIX CPS Pointer Qualifier)

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[5]	Comentários
					Descrição do OID: " O atributo cPSuri contém um apontador para a política de certificado da 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 CRÍTICA.
	CA		TRUE		
	PathLenConstraint		0		
	CRLDistributionPoints	4.2.1.14		O	
	distributionPoint		http://pki.cni.gov.cv/pub/lrc/eceid<nnnn>.crl	O	nnnn é o número sequencial da EC
	FreshestCRL		http://pki.cni.gov.cv/pub/lrc/eceid<nnnn>_delta.crl		nnnn é o número sequencial da EC
	Internet Certificate Extensions				
	Authority Information Access	4.2.2.1		o	
	accessMethod		1.3.6.1.5.5.7.48.2	o	Valor do OID value: 1.3.6.1.5.5.7.48.2 (id-ad-caIssuers) Descrição do OID: Certificate authority issuers
	accessLocation		http://pki.cni.gov.cv/pub/cert/eciac001.der	o	

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[5]	Comentários
	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. sha-256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }[6]
	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[7]).

8.1.4. Formato dos Nomes

Tal como definido na secção 2.2.

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 Directório X.500. A utilização de caracteres acentuados será da única responsabilidade do Grupo de Trabalho de Gestão 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 ("*policyQualifierID*: 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 ("*policyQualifierID*: 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 um apontador, na forma de URI, para a Declaração de Práticas de Certificação

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

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.

8.2. Perfil da lista de revogação de certificados

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

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

O perfil da LRC está de acordo com:

- Recomendação ITU.T X.509[3],
- RFC 5280 e,
- Política de Certificados da ICP-CV

8.2.1. Número da Versão

O campo "*version*" da LRC descreve a versão utilizada na codificação da LRC. Neste perfil, a versão utilizada é 2 (dois).

8.2.2. Extensões da LRC da EC eID

As componentes e as extensões definidas para as LRCs X.509 v2 fornecem métodos para associar atributos às LRCs.

Componente da Lista de Revogação de Certificados		Secção no RFC 5280	Valor	Tipo	Comentários
tbsCertList	**Version**	5.1.2.1	1	m	Versão v2 (o valor inteiro é 1)
	Signature	5.1.2.2	1.2.840.113549.1.1.11	m	Contém o identificador do algoritmo utilizado para assinar a LRC. O valor TEM que ser igual ao OID no campo *signatureAlgorithm* (abaixo)
	Issuer	5.1.2.3		m	
	Country (C)		"CV"		
	Organization (O)		"Sistema Nacional de Identificação e Autenticação Civil de Cabo Verde"		
	Organization Unit (OU)		"Entidades Certificadoras"		
	Organization Unit (OU)		"Identificação e Autenticação Civil"		
	Common Name (CN)		"Entidade Certificadora do Cartão Nacional de Identificação <nnnn>"		<nnnn> representa o número sequencial atribuído à EC
	thisUpdate	5.1.2.4	<data de emissão da LRC>	m	Implementações TÊM que utilizar o tempo UTC até 2049, e a partir dessa data devem utilizar o *GeneralisedTime*.
	nextUpdate	5.1.2.5	<data da próxima emissão da LRC = *thisUpdate* + N>	m	Este campo indica a data em que a próxima LRC vai ser emitida. A próxima LRC pode ser emitida antes da data indicada, mas não será emitida depois dessa data. Os emissores da CRL DEVEM emitir CRL com o tempo de *nextUpdate* maior ou igual a todas as LRC anteriores.

Componente da Lista de Revogação de Certificados		Secção no RFC 5280	Valor	Tipo	Comentários
					Implementações TÊM que utilizar o tempo UTC até 2049, e a partir dessa data devem utilizar o *GeneralisedTime*. N será no máximo 45 dias
	revokedCertificates	5.1.2.6	<lista de certificados revogados>	m	
	CRL Extensions	5.1.2.7		m	
	Authority Key Identifier	5.2.1		o	
	keyIdentifier		<O key Identifier é composto pela hash de 160-bit SHA-1 do valor da BIT STRING do subject key identifier do certificado do emissor (excluindo a tag, length, e número de bits não usado)>	m	
	CRL Number	5.2.3	<número sequencial único e incrementado>	m	
	CRL Entry Extensions	5.3			
	Reason Code	5.3.1		o	Valor tem que ser um dos seguintes: 1 – keyCompromise 2 – cACompromise 3 – affiliationChanged 4 – superseded

Componente da Lista de Revogação de Certificados		Secção no RFC 5280	Valor	Tipo	Comentários
					5 – cessationOfOperation 6 – certificateHold 8 – removeFromCRL 9 – privilegeWithdrawn 10 - aACompromise
	Signature Algorithm	5.1.1.2	1.2.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo utilizado no campo signature da sequência tbsCertList. sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1)
	Signature Value	5.1.1.3	<contém a assinatura digital emitida pela EC>	m	Contém a assinatura digital calculada sobre a *tbsCertList*.

9. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

9.1. 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).

9.2. 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).

9.3. 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

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

RFC 3279. 2002, *Algorithms and Identifiers for the 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 5280. 2008, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*

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

ANAC, Padrões e Algoritmos Criptográficos da ICP-CV