Política de Certificados de Assinatura Digital Qualificada do Residente

Política

PJ.CNICV_24.1.2_0013_pt_eID

Versão: 3.0

Data: 19/09/2019

Classificação: Público

Identificador do documento: PJ.CNICV_24.1.2_0009_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	02/06/2010	Versão inicial	MULTICERT
2.0	02/11/2017	Revisão	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 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 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 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 Assinatura Digital, que complementa e está de acordo com a Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação.[1]

[1] *cf.* PJ.CNICV_24.1.1_0002_pt_eID, Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação.

Conteúdo

1. POLÍTICA DE CERTIFICADOS DE ASSINATURA ELETRÓNICA QUALIFICADA DO RESIDENTE

1.1. Objetivo e Âmbito

O objetivo deste documento é definir as políticas utilizadas na emissão do certificado de Assinatura Eletrónica Qualificada do Residente do Cartão Nacional de Identificação, pela Entidade de Certificação do Cartão Nacional de Identificação (EC eID).

1.1. Público-Alvo

Este documento deve ser lido por,

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

1.2. Estrutura do Documento

Este documento complementa a Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação, 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 dos mesmos. Não se pretende nomear regras legais ou obrigações, mas antes informar. Pretende-se assim que este documento seja simples, direto e entendido por um público alargado, incluindo pessoas sem conhecimentos técnicos ou legais.

Este documento descreve a política de certificados para a emissão e gestão do certificado de Assinatura Eletrónica Qualificada do Residente, emitido pela EC do Cartão Nacional de Identificação adiante denominada de EC eID.

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

2.1. Visão Geral

Este documento satisfaz e complementa os requisitos impostos pela Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação.

2.2. Designação e Identificação do Documento

Este documento é a Política de Certificados do certificado de Assinatura Digital Qualificada do Residente. A PC é representada num certificado através de um número único designado de "identificador de objeto" (OID).

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 3.000
Estado do Documento	Versão Final
OID	2.16.132.1.2.100.1.1.2.1
Data de Emissão	Outubro 2019
Validade	Não aplicável
Localização	http://pki.cni.gov.cv/pub/pol/pc_ass_residente.html

2.3. Participantes

Esta informação consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

2.4. Dados de Contacto

Esta informação consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

3. DISPOSIÇÕES GERAIS

3.1. Obrigações e Direitos

Esta informação consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

3.1.1. Obrigações da EC

3.1.2. Obrigações das Unidades de Registo

3.1.3. Obrigações dos Titulares de Certificados

3.1.4. Direito das partes confiantes

3.1.5. Obrigações de Repositório

3.2. Responsabilidades

Esta informação consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

3.2.1. Responsabilidades da EC

3.2.2. Responsabilidades das Unidades de Registo

3.3. Responsabilidade Financeira

Esta informação consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

3.3.1. Indemnização devida pela terceira parte

3.3.2. Relações fiduciárias

3.4. Interpretação e execução

Esta informação consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

3.4.1. Legislação

3.4.2. Forma de interpretação e notificação

3.4.3. Procedimentos para a resolução de disputas

3.5. Taxas de serviço

Esta informação consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

3.5.1. Taxas de emissão e renovação de certificados

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

3.5.3. Taxas para outros serviços

3.5.4. Política de reembolso

3.6. Publicação e repositório

Esta informação consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

3.6.1. Frequência da publicação

3.6.2. Controlo de acesso

3.6.3. Repositórios

3.7. Auditoria de Conformidade

Esta informação consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

3.7.1. Frequência ou motivo da auditoria

3.7.2. Identidade e qualificações do auditor

3.7.3. Relação entre o auditor e a Entidade Certificadora

3.7.4. Âmbito da auditoria

3.7.5. Procedimentos após uma auditoria com resultado deficiente

3.7.6. Comunicação de resultados

3.8. Sigilo

Esta informação consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

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

3.8.2. Quebra de sigilo por motivos legais

3.8.3. Informações a terceiros

3.8.4. Divulgação por solicitação do titular

3.8.5. Direitos de propriedade intelectual

4. IDENTIFICAÇÃO E AUTENTICAÇÃO

Esta informação consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

4.1. Registo Inicial

4.1.1. Disposições Legais

4.1.2. Tipos de nomes

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

O nome único deste certificado emitido pela EC 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	Título de Residência
Organization Unit	OU	Assinatura Eletrónica Qualificada
Surname	SN	<nome de família do Residente>
Given Name	givenName	<parte do nome do Residente que não é o nome de família nem os nomes intermédios>
Serial Number	serial number	TR<nnnnnnnnn>[2]
Common Name	CN	<concatenação do givenName e SN do Cidadão>

[2] <nnnnnnnnn> é um valor sequencial iniciado em "000000001" na emissão do primeiro certificado deste tipo.

4.1.3. Necessidade de nomes significativos

4.1.4. Unicidade de nomes

4.1.5. Procedimento para resolver disputa de nomes

4.1.6. Reconhecimento, autenticação, e função das marcas registadas

4.1.7. Método de comprovação da posse de chave privada

4.1.8. Autenticação da identidade de uma pessoa singular

Para os certificados emitidos para pessoa singular, residente, é obrigatório que o registo inicial seja efetuado presencialmente, ou seja, a validação inicial da identidade do requerente é feita pelo método de "cara-a-cara".

Conforme a situação, o procedimento de validação por variar, no caso de ser uma primeira emissão do Título de Residência os dados do residente são validados através de documento de identificação válido emitido no país de origem, por exemplo o Passaporte, ou em falta deste por outro documento de identificação considerado, pelos registos e notariados de origem fidedigna.

4.1.9. Autenticação da identidade de uma pessoa coletiva

Não são emitidos certificados de Assinatura Digital Qualificada para pessoas coletivas.

4.1.10. Critérios para interoperabilidade

Esta informação consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

4.2. Identificação e Autenticação para pedidos de renovação de chaves

A informação desta secção consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

4.3. Identificação e autenticação para pedido de revogação

A informação desta secção consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

5. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

5.1. Pedido de Certificado

A informação desta secção consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

5.1.1. Requisitos

5.1.2. Quem pode subscrever um pedido de certificado?

5.1.3. Processo de registo e responsabilidades

5.2. Processamento do pedido de certificado

A informação desta secção consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

5.2.1. Requisitos

5.2.2. Processos para a identificação e funções de autenticação

5.2.3. Aprovação ou recusa de pedidos de certificado

5.2.4. Prazo para processar o pedido de certificado

5.3. Emissão de Certificado

A informação desta secção consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

5.3.1. Procedimentos para a emissão de certificado

5.3.2. Notificação da emissão do certificado ao titular

5.4. Aceitação do Certificado

Esta informação consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

5.4.1. Procedimentos para a aceitação de certificado

5.4.2. Publicação do certificado

5.4.3. Notificação da emissão de certificado a outras entidades

5.5. Uso do certificado e par de chaves

Esta informação consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

5.5.1. Uso do certificado e da chave privada pelo titular

A EC do Cartão Nacional de Identificação é a emissora do certificado de Assinatura Eletrónica Qualificada do Residente, sendo este o titular do mesmo. A sua chave privada é utilizada para a assinatura de documentos digitais, com valor probatório, ou seja com o mesmo valor que uma

assinatura manuscrita realizada perante entidades competentes para autenticar e reconhecer uma assinatura, garantindo e permitindo verificar a integridade dos mesmos.

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

Esta informação consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

5.6. Renovação de Certificados

Esta prática não é suportada na ICP-CV.

5.6.1. Renovação de Certificados

5.6.2. Motivos para renovação de certificado

5.6.3. Quem pode submeter o pedido de renovação de certificado

5.6.4. Processamento do pedido de renovação de certificado

5.6.5. Notificação de emissão de novo certificado ao titular

5.6.6. Procedimentos para aceitação de certificado

5.6.7. Publicação de certificado após renovação

5.6.8. Notificação da emissão do certificado a outras entidades

5.7. Modificação de Certificados

Esta prática não é suportada na ICP-CV.

5.8. Suspensão e revogação de certificado

A informação desta secção consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

5.8.1. Revogação

5.8.1.1. Circunstâncias para revogação

5.8.1.2. Quem pode submeter o pedido de revogação

5.8.1.3. Procedimento para o pedido de revogação

5.8.1.4. Prazo para processar o pedido de revogação

5.8.2. Suspensão

5.8.2.1. Motivos para suspensão

5.8.2.2. Quem pode efetuar o pedido de suspensão

5.8.2.3. Procedimentos para pedido de suspensão

5.8.2.4. Limite do período de suspensão

5.8.3. Frequência de emissão de LCR

5.8.4. Requisitos de verificação on-line de revogação

5.8.5. Outras formas disponíveis para divulgação de revogação

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

5.8.7. Requisitos especiais em caso de comprometimento de chave privada

5.9. Serviços sobre o estado certificado

A informação desta secção consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

5.9.1. Características operacionais

5.9.2. Disponibilidade do serviço

5.9.3. Características opcionais

5.10. Fim de subscrição

A informação desta secção consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

5.11. Retenção e recuperação de chaves (Key escrow)

As chaves dos certificados de Assinatura Eletrónica Qualificada do Residente não são retidas.

5.11.1. Políticas e práticas de recuperação de chaves

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

6. MEDIDAS DE SEGURANÇA FÍSICA, DE GESTÃO E OPERACIONAIS

6.1. Medidas de segurança física

A informação desta secção consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

6.1.1. Construção e Localização Física das Instalações da EC

6.1.2. Acesso físico ao local

6.1.3. Energia e ar condicionado

6.1.4. Exposição à água

6.1.5. Prevenção e proteção contra incêndio

6.1.6. Salvaguarda de suportes de armazenamento

6.1.7. Eliminação de resíduos

6.1.8. Instalações externas (alternativa) para recuperação de segurança

6.2. Medida de segurança dos processos

A informação desta secção consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

6.2.1. Funções de Confiança

6.2.2. Número de pessoas exigidas por tarefa

6.2.3. Identificação e Autenticação para cada função

6.3. Medidas de Segurança de Pessoal

A informação desta secção consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

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

6.3.2. Procedimento de verificação de antecedentes

6.3.3. Requisitos de formação e treino

6.3.4. Frequência e requisitos para ações de reciclagem

6.3.5. Frequência e sequência da rotação de funções

6.3.6. Sanções para ações não autorizadas

6.3.7. Requisitos para prestadores de serviços

6.3.8. Documentação fornecida ao pessoal

7. CONTROLOS TÉCNICOS DE SEGURANÇA

A informação desta secção consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

7.1. Geração e instalação do par de chaves

7.1.1. Geração do par de chaves

7.1.2. Entrega da chave privada ao titular

7.1.3. Entrega da chave pública ao emissor do certificado

7.1.4. Disponibilização de chave pública da EC às partes confiantes

7.1.5. Tamanho de chave

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

7.1.6. Parâmetros de chave pública e verificação de qualidade

7.1.7. 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 do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

7.2.1. Normas e medidas de segurança do módulo criptográfico

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

7.2.3. Retenção da chave privada (key escrow)

7.2.4. Cópia de segurança (backup) de chave privada

7.2.5. Transferência da chave privada para/módulo criptográfico

7.2.6. Armazenamento da chave privada no módulo criptográfico

7.2.7. Método para ativação da chave privada

7.2.8. Método para desativação da chave privada

7.2.9. Padrões de referência do módulo criptográfico

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 do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.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 dos certificados de Assinatura Digital Qualificada corresponde a 5 anos.

7.4. Dados de activação

Esta informação consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html).

7.4.1. Geração e instalação dos dados de ativação

7.4.2. Proteção dos dados de ativação

7.4.3. Outros aspetos dos dados de activação

7.5. Medidas de segurança informática

Esta informação consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

7.5.1. Requisitos técnicos específicos

7.5.2. Avaliação/nível de segurança

7.6. Ciclo de vida das medidas técnicas de segurança

Esta informação consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

7.7. Medidas de Segurança da Rede

Esta informação consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

7.8. Validação cronológica (Time-stamping)

Esta informação consta no documento de Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação (http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf).

8. PERFIL DE CERTIFICADO

8.1. Perfil de Certificado

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

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

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

O perfil do certificado de Assinatura Eletrónica Qualificada do Residente está de acordo com:

- Recomendação ITU.T X.509[3],
- RFC 5280[4] e
- Política de Certificados da ICP-CV

[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.*

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.

Componente do Certificado		Secção no RFC5280	Valor	Tipo [5]	Comentários
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)		"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> numero sequencial incrementado a cada nova 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 RFC5280	Valor	Tipo 5	Comentários
	Not Before		<data de emissão>		
	Not After		<data de emissão + 5 anos>		
	Subject	4.1.2.6		m	
	Country (C)		"CV"		
	Organization (O)		"Sistema Nacional de Identificação e Autenticação Civil de Cabo Verde"		
	Organization Unit (OU)		" Título de Residência "		
	Organization Unit (OU)		"Assinatura Eletrónica Qualificada"		
	Common Name (CN)		<concatenação do *givenName* e SN do residente>		
	Surname (SN)		<nome de família do residente>		
	Given Name (*givenName*)		<nome(s) próprio(s) do residente>		
	Serial Number (serialNumber)		TR<nnnnnnnnn>[6]		

[6] < nnnnnnnnn > é um valor sequencial iniciado em "000000001" na emissão do primeiro certificado deste tipo.

Componente do Certificado		Secção no RFC5280	Valor	Tipo 5	Comentários
	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.[7]
	subjectPublicKey		<Chave Pública com modulus n de 2048 bits>		
	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	

[7] *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 RFC5280	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		"1" selecionado		Se o bit nonRepudiation for seleccionado, este NÃO DEVE ser combinado com qualquer outro bit do key usage, i.e., se seleccionado, DEVE ser o único seleccionado.[8]
	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		o	

[8] *cf.* RFC 3039, 2001, Internet X.509 Public Key Infrastructure Qualified Certificates Profile.

Componente do Certificado		Secção no RFC5280	Valor	Tipo 5	Comentários
	policyIdentifier		2.16.132.1.3.2.1.1.1	m	Identificador da Declaração de Práticas de Certificação da EC eID.
	policyQualifiers		policyQualiflierID: 1.3.6.1.5.5.7.2.1 cPSuri: http://pki.cni.gov.cv/pub/pol/dpc_eceid.html	o	Valor do OID: 1.3.6.1.5.5.7.2.1 (id-qt-cps PKIX CPS Pointer Qualifier) Descrição do OID: "O atributo cPSuri contém um apontador para a Declaração de Práticas de Certificação publicada pela EC. O apontador está na forma de um URI." (http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.1.html)
	policyIdentifier		2.16.132.1.2.100.1.1.2.1	m	Identificador da Política de Certificados de Assinatura Qualificada do Residente
	policyQualifiers		policyQualiflierID: 1.3.6.1.5.5.7.2.2 cPSuri: “http://pki.cni.gov.cv/pub/pol/pc_ass_residente.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		c	Esta extensão é marcada CRÍTICA.
	CA		FALSE		
	PathLenConstraint		0		

Componente do Certificado		Secção no RFC5280	Valor	Tipo 5	Comentários
	CRLDistributionPoints	4.2.1.14		o	
	distributionPoint		http://pki.cni.gov.cv/pub/lrc/eceid<nnnn>.crl	o	<nnnn> numero sequencial incrementado a cada nova EC
	Freshest CRL	4.2.1.16		o	
	distributionPoint		http://pki.cni.gov.cv/pub/lrc/eceid<nnnn>_delta.crl	o	<nnnn> numero sequencial incrementado a cada nova EC
	Subject Diretory Attributes	-		o	
	Qualified Certificate Statement	-		o	Não é uma extensão definida no RFC 3280. A extensão QCStatements é uma extensão introduzida pelo PKIX Qualified Certificate Profile8 e ETSI[9]. (http://javadoc.iaik.tugraz.at/iaik_jce/current/iaik/x509/extensions/qualified/QCStatements.html)
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcCompliance = "0.4.0.1862.1.1"		A aposição desta componente ao certificado significa que o mesmo é emitido com a qualidade de certificado Qualificado, de acordo com o Anexo I e II da Directiva 1999/93/EC do Parlamento Europeu e do Conselho de 13 de Dezembro de 1999 sobre "a Community framework for electronic signatures", e conforme transposição para a legislação do país identificado na componente "issuer" do certificado. A declaração QcEuCompliance (id-etsi-qcs-QcCompliance) corrsponde ao OID "0.4.0.1862.1.1".

[9] *cf.* ETSI TS 101 862, 2001-06, Qualified certificate profile, v1.2.1.

Componente do Certificado		Secção no RFC5280	Valor	Tipo 5	Comentários
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcSSCD = " 0.4.0.1862.1.4"		Declaração efetuada pela respetiva EC, indicando que a chave privada associada à chave pública no certificado está guardada num dispositivo seguro de criação de assinaturas (Secure Signature Creation Device), de acordo com o anexo III da Directiva 1999/93/EC e da lei do país onde a EC está estabelecida.
	Authority Information Access	4.2.2.1		o	
	accessMethod		1.3.6.1.5.5.7.48.1	o	Valor do OID: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp) Descrição do OID: Online Certificate Status Protocol
	accessLocation		http://ocsp.eciad.cni.gov.cv/publico/ocsp	o	
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha256WithRSAEncryption {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1)
	Signature Value	4.1.1.3	<contém a assinatura digital emitida pela EC>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (subject) do certificado.

8.1.3. OID do Algoritmo

O campo "*signatureAlgorithm*" do certificado contém o OID do algoritmo criptográfico utilizado pela EC para assinar o certificado: 1.2.840.113549.1.1.11 (sha-256WithRSAEncryption[10]).

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 Comissão Executiva da EC.

8.1.6. OID da Política de Certificados

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

Os qualificadores opcionais ("*policyQualiflierID*: 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 ("*policyQualiflierID*: 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 publicada pela EC e, o "*userNotice explicitText*" que contém um apontador, na forma de URI, para a Política de Certificados.

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

8.1.9. Semântica de processamento para a extensão crítica Certificate Policies

Nada a assinalar.

9. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

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

9.1. Procedimentos de mudança de especificação

9.2. Políticas de publicação e notificação

9.3. Procedimentos para aprovação

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-256). 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).