Declaração de Práticas de Certificação e Políticas de Certificados da Autoridade Certificadora Raiz do Estado de Moçambique

Instituto Nacional de Tecnologias de Informação e Comunicação

INTIC

Versão 1.0 - 24/7/2022

Resumo Executivo

A necessidade de introdução de novos processos e formas de comunicação, no relacionamento em sociedade, entre cidadãos, entidades privadas e o Estado e no seguimento da evolução das tecnologias de informação e comunicação, fomenta a implementação uma Infraestrutura de Chaves Públicas para os serviços do Estado de Moçambique, cujo objectivo é fortalecer a sociedade de informação e o governo electrónico.

Na forma de uma hierarquia de confiança, é estabelecida uma estrutura electrónica que proporciona a realização de transacções electrónicas seguras, a autenticação forte, um meio de assinar electronicamente transacções ou informações e documentos electrónicos, assegurando a identidade do seu autor, a integridade, o não repúdio e a confidencialidade das transacções electrónicas.

A ICP do Estado de Moçambique é constituída por uma Entidade Certificadora Raiz que, além de designar as âncoras electrónicas de confiança do Estado de Moçambique, executa e zela pela aplicação das políticas de certificados e directrizes aprovadas pelo Comité Gestor do Sistema de Certificação Digital de Moçambique.

Compete ainda à Entidade Certificadora Raiz prestar os serviços de certificação, no nível hierárquico imediatamente abaixo ao seu, na cadeia de certificação, de acordo com a legislação e normas aplicáveis às entidades de certificação estabelecidas em Moçambique para a emissão de certificados digitais.

Destinatários

- Recursos humanos ao serviço da Autoridade Certificadora Raiz do Estado de Moçambique;
- Entidades Auditoras da ACRaizEstado de Moçambique;
- Entidades Públicas;
- Público, em geral.

Objectivo

Este documento pretende apresentar procedimentos e práticas utilizadas pela Autoridade Certificadora Raiz do Estado de Moçambique, no suporte à sua actividade de certificação electrónica digital.

Sumário

Lista de Figuras

Lista de Tabelas

Acrónimos e Definições

AC	Autoridade Certificadora.
AC Raiz	Autoridade Certificadora Raiz.
ACR	Autoridade Certificadora Raiz do Estado.
ANSI	American National Standards Institute
AR	Autoridade de Registo.
CG	Comité Gestor.
CMP	*Certificate Management Protocol*.
CRL	*Certificate Revocation List* (o mesmo que LCR).
CT	Comité Técnico.
CSR	*Certificate Signing Request* (o mesmo que PKCS#10).
DL	Decreto Lei.
DN	Nome distinto ou *Distinguished Name*.
DPC	Declaração de Práticas de Certificação.
EC	Entidade Certificadora (o mesmo que AC).
ER	Entidade de Registo (o mesmo que AR).
GAR	Grupo de Administração de Registo.
GAS	Grupo de Administração de Sistemas.
GASeg	Grupo de Administração de Segurança.
GAudS	Grupo de Auditoria.
GC	Grupo de Custódia.
GG	Grupo de Gestão.
GOS	Grupo de Operação de Sistemas.
HSM	*Hardware Security Module* (o mesmo que MC).
ICP	Infraestrutura de Chaves Públicas.
ICPMZ	ICP de Moçambique.
LSECMZ	Lista de Serviços Electrónicos Confiáveis de Moçambique.
LCR	Lista de Certificados Revogados.
MC	Módulo Criptográfico.
OID	Identificador de Objetos ou *Object Identifier*.
OSCP	*On-line Certificate Status Protocol*.
PC	Política de Certificado.
PEM	*Privacy-Enhanced Mail*.
PKCS	*Public Key Cryptography Standard*.
PKCS#10	Formato padrão de Requisição para Assinatura de Certificado.
PKI	*Public Key Infrastructure* (o mesmo que ICP).
RFC	*Request For Comments*.
SHA	*Secure Hash Algorithm* (Algoritmo de Resumo Criptográfico).
SCDM	Sistema de Certificação Digital de Moçambique.
TIC	Tecnologias da Informação e Comunicação.
TSL	*Trusted Service List* (ver LSECMZ).
URI	*Uniform Resource Identifier*.
UTC	Tempo Universal Coordenado.

Alterações neste Documento

Nesta secção deve-se anotar as alterações realizadas na DPC. Alterações pequenas implicam em mudanças de sub-versões do documento. Alterações de maior porte, exigem novas versões. O versionamento é representado da seguinte forma: $v.s$, onde "v" e versão e "s" a sub-versão. A primeira versão do documento é a 1.0.

Se houver mudança de versão, deve ser atribuído um novo identificado de objectos, conforme [1].

Ver	Data	Autor	Seção	Natureza da Mudança
1.0	24/7/2022	LabSEC/UFSC		Versão inicial.

1 Introdução

Este documento apresenta a declaração de práticas de certificação (DPC) adoptadas, no âmbito da emissão e gestão de certificados, pela Autoridade Certificadora Raiz do Estado de Moçambique, doravante denominada de AC Raiz de Moçambique (AC Raiz MZ), e que deverão ser seguidas pelas partes confiantes que integrem a sua hierarquia de confiança.

1.1 Visão Geral

As práticas inerentes às actividades do ciclo de vida dos certificados, realizadas por uma Autoridade Certificadora, doravante denominada de AC, nomeadamente criação, assinatura, emissão e alteração de estado dos certificados, são fundamentais para garantir a fiabilidade e a confiança de uma Infraestrutura de Chaves Públicas, doravante denominada de ICP.

O presente documento aplica-se à AC Raiz de Moçambique (AC Raiz MZ), sendo que a sua criação, em termos estruturais, teve por base os seguintes normativos:

Lei n.º 3 de 2017: Regula as transacções electrónicas, o comércio electrónico e o governo electrónico, bem a garantia da segurança dos provedores e utilizadores das tecnologias de informação e comunicação, ao abrigo do disposto no número 1, do artigo 179, da Constituição da República de Moçambique [2].

Decreto n.º 59 de 2019: Cria e regulamenta o Sistema de Certificação Digital de Moçambique (SCDM) que visa garantir a autenticidade, integridade e validade jurídica de documentos em formato electrónico [3].

RFC 3647: *Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework* [4];

RFC 5280: *Internet X.509 PKI - Certificate and CRL Profile, com atualizações no RFC 6818 - Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* [5]. Este normativo possui as seguintes atualizações:

- **RFC 6818:** *Updates to the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile* [6].
- **RFC 8398:** *Internationalized Email Addresses in X.509 Certificates* [7].
- **RFC 8399:** *Internationalization Updates to RFC 5280* [8].

ETSI TS 119 612 *Electronic Signatures and Infrastructures (ESI); Trusted Lists* [9].

ETSI TS 319 411-1 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements* [10].

ETSI TS 319 411-2 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates* [11].

As noves secções deste documento apresentam os procedimentos e controlos adoptados na AC Raiz de Moçambique (AC Raiz MZ) para atingir os requisitos especificados nas normas aplicáveis.

1.2 Identificação do Documento

Este documento é referenciado num certificado através de um número único designado de "identificador de objecto" (OID). Este documento é identificado pelos dados constantes na Tabela 1:

Tabela 1: Informação do documento.

Versão do Documento	Versão v1
Estado	Aprovado
OID	2.16.508.1.1.1
Data de Emissão	24/7/2022
Validade	Enquanto não for expressamente revogado.
Localização	https://scee.scdm.mz/ac-raiz/dpc-acraiz-v1.pdf

1.3 Participantes da Infra-estrutura de Chaves Públicas

O Sistema de Certificação Digital de Moçambique (SCDM) é uma infra-estrutura constituída por várias entidades provedoras de serviços electrónicos, que em conjunto permitem fornecer serviços electrónicos confiáveis de assinatura electrónica e autenticação para o Estado de Moçambique.

Podem fazer parte da infraestrutura do SCDM:

a) ACs raízes do Estado (ACR) de Moçambique;

b) ACs raízes acreditadas pela ACR;

c) Entidades Certificadoras (EC);

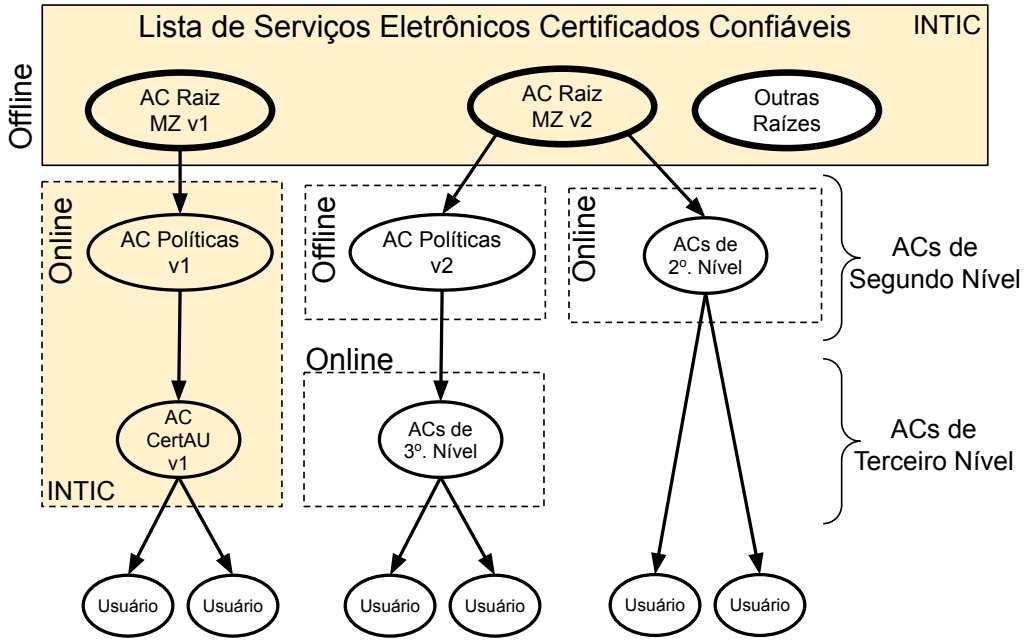
d) Entidades de Registo (ER);

e) Outros provedores de serviços electrónicos necessários ao bom funcionamento da infra-estrutura do Sistema de Certificação Digital de Moçambique.

1.3.1 Autoridades Certificadoras

A ICP do Estado de Moçambique está estruturada em 2 e 3 níveis de Autoridades Certificadoras, sendo elas hierarquicamente dependentes. A Figura 1 apresenta um esquema geral da ICP de Estado de Moçambique. Conforme ilustra a figura, A ICP de Moçambique é formada por cinco tipos de autoridades certificadoras: AC Raiz de Moçambique (AC Raiz MZ); AC Políticas; AC CertAU; AC de Segundo Nível; e AC de Terceiro Nível. Também faz parte a Lista de Serviços Electrónicos Confiáveis de Moçambique, onde é incluído os certificados digitais dos serviços electrónicos confiáveis acreditados pelo SCDM.

Figura 1: Esquema ICP do Estado de Moçambique.



Fonte: INTIC

1.3.1.1 AC Raiz de Moçambique (AC Raiz MZ)

A AC Raiz MZ é a entidade de certificação de primeiro nível, que estabelece a raiz da cadeia de confiança da ICP do Estado de Moçambique. Deste modo, a AC Raiz MZ assina:

a) O seu certificado auto-assinado;

b) Os certificados das ACs de políticas;

c) Os certificado das Autoridades Certificadoras de segundo nível;

d) A sua Lista de Certificados Revogados (LCR);

e) A Lista de Serviços Electrónicos Confiáveis de Moçambique (LSECMZ).

1.3.1.2 Autoridade Certificadora de Políticas

A AC Políticas é responsável por definir políticas de certificados de ACs de terceiro nível. A AC de Políticas não emite certificados de utilizadores finais.

1.3.1.3 Autoridade Certificadora de Assinatura Única

A AC emissora de certificados de assinatura única (AC CertAU) é um serviço online de emissão de certificados de assinaturas de documentos electrónicos. Sempre que um usuário final necessitar assinar um documento, um certificado é gerado e utilizado para assinar o referido documento. Assim que o documento for assinado, a chave privada associada ao certificado é destruída.

1.3.1.4 Autoridade Certificadora de Segundo Nível

A autoridade certificadora de segundo nível (AC de Segundo Nível) é criada pela AC Raiz MZ para a emissão de certificados para os utilizadores finais.

1.3.1.5 Autoridade Certificadora de Terceiro Nível

A autoridade certificadora de Terceiro Nível (AC de Terceiro Nível) é criada por ACs de Políticas. Esta AC emite certificados para os utilizadores finais.

1.3.2 Outras Autoridades Certificadoras

O SCDM pode integrar, após avaliação e acreditação pela Autoridade Supervisora e Acreditação, de outras ACs que não fazem parte, diretamente, da cadeia de certificados da AC Raiz MZ.

Este é o caso, por exemplo de acordos nacionais ou internacionais de acreditação, e tem por objectivo o reconhecimento universal das assinaturas electrónicas usadas pelas pessoas singulares e colectivas de Moçambique.

Após a acreditação, o certificado da AC Acreditada será incluído na Lista de Serviços Electrónicos Confiáveis de Moçambique (LSECMZ) e publicada no site do SCDM.

1.3.3 Autoridades de Registo

As Autoridades de Registo são entidades que executam serviços de identificação, registo de utilizadores de certificados, bem como a gestão de pedidos de renovação e revogação de certificados.

Uma vez feita a identificação e o registo do utilizador, estes dados assim como os os atributos de autenticação são geridos por um sistema de gerenciamento de identidades electrónicas.

1.3.4 Titulares dos Certificados

No âmbito do SCDM, os titulares dos certificados por ela emitidos são as pessoas colectivas, representadas por pessoa física, que aceitam o certificado e assumem a responsabilidade pela sua correcta utilização.

São considerados como titulares, aqueles cujo nome/designação está inscrito no campo "Subject" do certificado e utilizam o certificado e respectiva chave privada de acordo com o estabelecido nas diversas políticas de certificado descrito no presente documento, sendo consideradas as seguintes categorias de titulares:

a) Pessoa singular;

b) Pessoa colectiva;

c) Sistema ou equipamento tecnológico.

Não são considerados titulares, no âmbito deste documento, as seguintes categorias:

a) Autoridades Certificadoras, independentemente do nível a que se encontram;

b) Autoridades de Registo;

c) O pessoal das ACs e ARs, cujos certificados tem como uso exclusivo a operação dos respectivos sistemas.

O detentor do certificado da AC Raiz MZ é o Instituto Nacional de Tecnologias da Informação e Comunicação (INTIC).

1.3.5 Partes Confiantes

As partes confiantes ou destinatários são pessoas singulares, entidades ou serviços que confiam na validade dos mecanismos e procedimentos utilizados no processo de associação do nome do titular com a sua chave pública, ou seja, confiam que o certificado corresponde na realidade a quem diz pertencer.

Neste documento, considera-se uma parte confiante, aquela que confia no conteúdo, validade e aplicabilidade do certificado emitido na hierarquia de confiança do SCDM.

1.3.6 Outros Participantes

1.3.6.1 Autoridade Supervisora e Credenciadora

Cabe à Autoridade Supervisora e Credenciadora (ASC) disponibilizar serviços de auditoria/inspecção de conformidade, no sentido de aferir se os processos utilizados pelas ACs, nas suas actividades de certificação cumprem com os requisitos mínimos estabelecidos na legislação nacional e normas vigentes.

Assim, consideram-se como principais as seguintes responsabilidades:

a) Criar e disponibilizar Normas Técnicas e de Segurança às Autoridades Certificadoras;

b) Cooperar com o CG do SCDM;

c) Elaborar análises e pareceres regulamentares e técnicos para o CG a fim de este se pronunciar sobre a incorporação das proponentes Autoridades Certificadoras, exercendo competências no domínio das entidades subordinadas públicas e no domínio da actividade privada de certificação electrónica em Moçambique;

d) Registar, credenciar e fiscalizar as Autoridades Certificadoras, no cumprimento dos requisitos aplicáveis às actividades inerentes ao fornecimento de certificados digitais;

e) Criar, gerenciar e publicar a Lista de Serviços Electrónicos Confiáveis de Moçambique (LSECMZ), em particular, os certificados raízes que serão reconhecidos como confiáveis em Moçambique;

f) A inclusão de provedores na LSECMZ deverá ser previamente autorizada pelo CG;

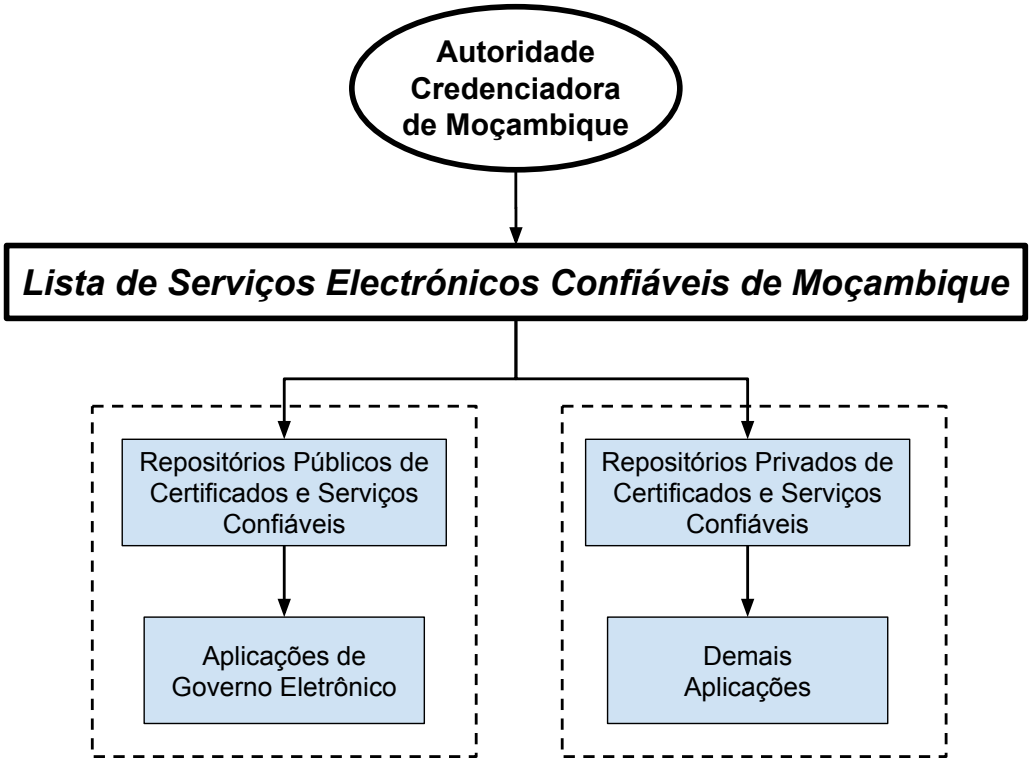
g) Fornecer mecanismos de fiscalização para as Autoridades Certificadoras para que estas demonstrem o seu cumprimento dos requisitos aplicáveis à sua actividade;

h) Supervisionar o cumprimento de práticas normativas e da legislação por parte dos fornecedores de serviços electrónicos confiáveis;

i) Interagir com entidades supervisoras de outros países, tendo em vista a cooperação e adopção de práticas que garantam o reconhecimento da sua actividade em outros países.

A Figura 2 ilustra a Lista de Serviços Electrónicos Confiáveis de Moçambique (LSECMZ) de Moçambique. Conforme ilustra a figura, os repositórios das aplicações dos usuários devem

Figura 2: Lista de Provedores de Serviços Electrónicos Confiáveis no Estado de Moçambique.



Fonte: INTIC

ser actualizados, periodicamente, com os dados advindos desta lista. Esse processo pode ser feito de forma manual ou automática.

Por exemplo, todos os certificados auto-assinados da AC Raiz MZ devem constar na LSECMZ. Assim, aplicações dos usuários podem aceder a lista, e obter os certificados raízes acreditados em Moçambique.

A ASC deve publicar, e manter actualizada, a lista LSECMZ no site principal do SCDMZ.

1.3.6.2 Comité Gestor

O Comité Gestor (CG) é o órgão máximo e decisor, responsável pela gestão global e administração do Sistema de Certificação Digital de Moçambique, competindo-lhe:

a) Definir as políticas e práticas de certificação, propostas pelo Comité Técnico e elaboradas de acordo com a legislação e as normas ou especificações internacionalmente reconhecidas, a serem observadas pelas Autoridades Certificadoras, Autoridades de Registo e demais prestadores de serviço de suporte integrantes do Sistema de Certificação Digital de Moçambique;

b) Garantir que as declarações de práticas de certificação das várias Autoridades Certificadoras que integram o Sistema de Certificação Digital de Moçambique estão em conformidade com a política e práticas de certificação definidas;

c) Propor os critérios para aprovação de integração no Sistema de Certificação Digital de Moçambiquedos pedidos das Autoridades Certificadoras;

d) Aferir a conformidade dos procedimentos seguidos pelas autoridades certificadoras com as políticas e práticas aprovadas, sem prejuízo das competências legalmente cometidas ao INTIC;

e) Pronunciar-se pela exclusão das autoridades certificadoras que não demonstrem conformidade com as políticas e práticas aprovadas, comunicando tal facto ao INTIC;

f) Solicitar Auditorias e fiscalização às ACs, assim como aos seus prestadores de serviço de suporte, sempre que suspeitem incumprimento das regras e práticas por si aprovadas;

g) Actualizar, ajustar e rever procedimentos e práticas estabelecidas para o SCDM, de modo a garantir a sua compatibilidade e promover a actualização tecnológica do sistema e a sua conformidade com as políticas de segurança;

h) Promover as actividades necessárias para o estabelecimento de acordos de interoperabilidade, com base em certificação cruzada, com outras infraestruturas de chaves públicas, de natureza privada ou pública, nacionais ou internacionais, nomeadamente, dar indicações à AC Raiz MZ para a atribuição e a revogação de certificados emitidos com base em certificação cruzada.

i) Aprovar a inclusão de serviços electrónicos na Lista de Serviços Electrónicos Confiáveis de Moçambique (LSECMZ);

j) Representar institucionalmente o SCDM.

1.3.6.3 Comité Técnico

O Comité Técnico (CT) é o órgão de apoio e aconselhamento técnico do CG do SCDM, para tomadas de decisões no âmbito da certificação electrónica. Este tem as seguintes competências e responsabilidades:

a) Propor políticas e práticas de certificação de acordo com a legislação e as normas ou especificações internacionalmente reconhecidas, no âmbito da certificação digital;

b) Monitorizar continuamente as melhores práticas internacionais de forma a identificar e propor acções de melhoria no sistema;

c) Emitir pareceres e esclarecimentos inerentes a questões técnicas e de segurança;

d) Apoiar o CG na tomada de decisão, no âmbito das suas competências;

e) Participar nas reuniões do CG, sempre que convocado, pronunciando-se de forma consertada, sustentando uma opinião técnica que apoie a análise estratégica e a tomada de decisão;

f) Cumprir outras atribuições que lhe forem conferidas por delegação do CG.

1.4 Utilização do Certificado

Os requisitos e regras definidos neste documento, aplicam-se a todos os certificados emitidos pela AC Raiz MZ.

Os certificados emitidos pela AC Raiz MZ são também utilizados pelas partes confiantes para verificação da cadeia de confiança de um certificado emitido na sua hierarquia, assim como para garantir a autenticidade e identidade do emissor de uma assinatura digital gerada pela chave privada correspondente à chave pública contida num certificado assinado pela AC Raiz MZ. Devem ser utilizados de acordo com a função e finalidade estabelecida neste documento, nas correspondentes Políticas de Certificados e de acordo com a legislação em vigor.

1.4.1 Aplicações Apropriadas Para os Certificados

Os certificados emitidos no domínio da AC Raiz MZ são utilizados com o objectivo de:

a) Identificar as ACs, no caso a AC Raiz MZ, AC Políticas e ACs emissoras de segundo nível;

b) Divulgar as chaves públicas da ACs;

c) Assinar as Listas de Certificados Revogados da AC Raiz MZ;

d) Assinar certificados de serviços complementares da AC Raiz MZ;

e) Conferir credibilidade aos certificados das ACs integrantes da AC Raiz MZ.

Estes serviços são obtidos com recurso à utilização de criptografia de chave pública, através da sua utilização na estrutura de confiança que a AC Raiz MZ proporcionam. Assim, os serviços de identificação e autenticação, integridade e não-repúdio são obtidos mediante a utilização de assinaturas digitais. A confidencialidade é garantida através dos recursos a algoritmos de cifra, quando conjugados com mecanismos de estabelecimento e distribuição de chaves.

1.4.2 Aplicações proibidas para os Certificados

Os certificados poderão ser utilizados noutros contextos apenas na extensão do que é permitido pelas regras do CG e pela legislação aplicável.

Os certificados emitidos pela AC Raiz MZ não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente.

Os serviços de certificação emitidos pela AC Raiz MZ, não foram desenhados nem está autorizada a sua utilização em actividades de alto risco ou que requeiram uma actividade isenta de falhas, como as relacionadas com o funcionamento de instalações hospitalares, nucleares, controlo de tráfego aéreo, controlo de tráfego ferroviário, ou qualquer outra actividade onde uma falha possa levar à morte, lesões pessoais ou danos graves para o meio ambiente.

1.5 Dados para Contacto

Esta secção apresenta os dados para contactar a AC Raiz MZ.

1.5.1 Entidade Responsável por Este Documento

A gestão deste documento é da responsabilidade do INTIC.

1.5.2 Ponto de Contacto

O ponto de contacto para esta PC/DPC e outros assuntos é aquele estabelecido na Tabela 2.

Tabela 2: Dados para Contacto.

Nome	Instituto Nacional de Tecnologias da Informação e Comunicação (INTIC).
Morada	Rua José Mateus, Nr.437, Bairro da Polana Cimento, Maputo.
Correio Electrónico	egov@intic.gov.mz
Página Institucional	http://www.intic.gov.mz/
Telefone	(258) 21 498786 e 21 498787

1.5.3 Responsável por Determinar a Adequabilidade da DPC à Política

A Autoridade Credenciadora é o órgão competente para determinar a adequação das práticas descritas neste documento, tendo por base o processo de auditoria previsto neste documento.

1.5.4 Procedimentos de Aprovação da DPC

A gestão e aprovação do presente documento competem ao responsável máximo da entidade que detém a gestão da AC Raiz MZ.

2 Responsabilidades referentes a publicações e repositórios

Esta seção apresenta as responsabilidades relacionadas á publicação de documentos pela AC Raiz e seus repositórios.

2.1 Repositórios

O repositório da AC Raiz MZ está no endereço https://scee.scdm.mz/ac-raiz.

A AC Raiz de Moçambique (AC Raiz MZ) é detentora de um repositório em ambiente Web, que permite às Partes Confiantes a realização de pesquisas online relativas às práticas de certificação por si exercidas, ao estado dos certificados por si emitidos e outra informação. A Tabela 3 lista os principais dados do repositório da AC Raiz MZ de Moçambique.

Tabela 3: Repositórios da AC Raiz MZ.

Conteúdo	Endereço URI
Site principal	https://scee.scdm.mz
LSECMZ	https://scee.scdm.mz/tslmz.xml
Certificado da AC Raiz MZ v1	https://scee.scdm.mz/ac-raiz/acraiz-v1.der
Certificado da AC Raiz MZ v2	https://scee.scdm.mz/ac-raiz/acraiz-v2.der
DPC e PC da AC Raiz MZ	https://scee.scdm.mz/ac-raiz/dpc-acraiz-v1.pdf
LCR da AC Raiz MZ v1	https://scee.scdm.mz/ac-raiz/lcr-acraiz-v1.crl
LCR da AC Raiz MZ v2	https://scee.scdm.mz/ac-raiz/lcr-acraiz-v2.crl
Serviço OCSP	https://scee.scdm.mz/ac-raiz/ocsp

2.2 Publicação de informações

Nos repositório listados na Tabela 3 serão publicadas as versões actuais da LSECMZ, LCR, DPC, PC, Certificados de ACs e ARs credenciadas e assim como dados para contacto com a AC Raiz MZ. Versões antigas dos documentos e arquivos podem ser obtidas no site principal da AC Raiz MZ.

2.3 Frequência de publicação

O repositório é actualizado no prazo máximo de 1 dia útil sempre que houver mudança nas informações listadas na Secção 2.2.

2.4 Controles de acesso aos repositórios

Todas as informações do repositório são públicas e podem ser acessadas de forma anónima.

A informação publicada no site da AC Raiz MZ pode ser livremente acessada.

3 Identificação e Autenticação

Esta secção apresenta as formas de identificação e de autenticação das entidades participantes do Sistema de Certificação Digital de Moçambique.

3.1 Nomes

3.1.1 Tipos de Nomes

As ACs integrantes na hierarquia da AC Raiz MZ, titulares de certificados, terão um nome que os identificam univocamente no âmbito do SCDM.

Os certificados atribuídos a cada entidade deverão conter no campo "Subject", um Distinguished Name (DN) para utilização como identificador único de cada entidade, de acordo com o RFC 5280 [5].

No caso dos certificados auto-assinados, o DN do emissor assume-se como o do titular. Encontram-se definidos os perfis de certificados emitidos na hierarquia do SCDM na Secção 7 (ver página 75).

3.1.2 Necessidade de Nomes Significativos

A AC Raiz MZ assegura que, na sua hierarquia de confiança, não existem certificados que, tendo o mesmo nome único identifiquem entidades (equipamento) distintas. As ACs e ARs integradas na hierarquia da AC Raiz MZ devem garantir que a relação entre o titular e a organização a que pertencem é a mesma que consta no certificado e que é facilmente perceptível e identificável.

3.1.3 Anonimato e Pseudónimo de Titulares

Não é permitida, no âmbito do SCDM a utilização de titulares com base no conceito de anonimato. Os titulares de certificados finais apenas podem optar pela utilização de pseudónimos.

A AC Raiz MZ não emite certificados para titulares de certificados finais, sendo que por isso não emite certificados com pseudónimos.

As AC's integradas na hierarquia da AC Raiz MZ, se emitirem certificados para titulares finais, podem utilizar pseudónimos[1], onde o atributo "CommonName" do campo "sub-

[1] Verificar a necessidade de pseudónimos!

ject" deverá começar pela palavra "Pseudo:", seguida do pseudónimo do titular (CN = Pseudo: <qualquer cadeia de caracteres>).

3.1.4 Interpretação de Formatos de Nomes

As regras utilizadas pela AC Raiz MZ para interpretar o formato dos nomes seguem o estabelecido na RFC 5280 [5], assegurando que todos os atributos DirectoryString dos campos issuer e subject do certificado são codificados numa UTF8String, com excepção dos atributos country e serialnumber que são codificados numa PrintableString.

3.1.5 Unicidade de Nomes

Os identificadores do tipo DN são únicos para cada uma das ACs integradas na hierarquia de confiança da AC Raiz MZ, não induzindo em ambiguidades.

De acordo com o seu processo de emissão, a AC Raiz MZ e as suas AC subordinadas rejeitam, a emissão de certificados com o mesmo DN para titulares distintos.

3.1.6 Procedimento Para Resolver Disputa de Nomes

A AC Raiz MZ reserva-se no direito de tomar todas as decisões no caso de existência de disputa de nomes resultante da igualdade de nomes entre diferentes pedidos de certificado.

3.1.7 Reconhecimento, Autenticação de Marcas Registadas

As entidades requisitantes de certificados, devem demonstrar que têm direito à utilização do nome requisitado, não podendo as designações usadas nos certificados emitidos pela AC Raiz MZ e pelas AC subordinadas infringir os direitos de propriedade intelectual de outros indivíduos ou entidades.

No procedimento de autenticação e identificação do titular do certificado, prévio à emissão do mesmo, a entidade requisitante do certificado terá que apresentar os documentos legais que demonstrem o direito à utilização do nome requisitado.

3.2 Validação de Identidade no Registo Inicial

3.2.1 Método de Comprovação de Posse de Chave Privada

Para as Autoridades Certificadoras subordinadas da AC Raiz MZ, é considerado um mecanismo aceitável como método de comprovação da posse de chave privada a utilização do PKIX Certificate Management Protocol (CMP), definido no RFC 4210 [12], atualizado com o RFC 6712 [13].

Na AC Raiz MZ a comprovação da posse da chave privada será garantida através da presença física de um representante autorizado da entidade subordinada, na cerimónia de emissão desse tipo de certificados. Nessa cerimónia, o representante da entidade subordinada apresentará o pedido de certificado no formato PKCS#10 [14, 15].

3.2.2 Autenticação da Identidade de uma Pessoa Singular

No âmbito da AC Raiz MZ, a autenticação de um individuo apenas se aplica para a autenticação da identidade dos representantes legais da AC's a integrar na hierarquia da AC Raiz MZ, uma vez que esta não emite certificados para titulares finais.

As AC's integradas da hierarquia da AC Raiz MZ que emitem certificados para titulares finais, devem na sua Declaração de Práticas e Políticas de Certificados descrever o método utilizados para autenticação da identidade de uma pessoa singular.

3.2.3 Autenticação da Identidade de uma Organização

O processo de autenticação da identidade de uma pessoa colectiva deve obrigatoriamente garantir que a pessoa colectiva para quem vai ser emitido o certificado é quem na realidade diz ser e que a criação de assinatura, através de dispositivo de criação de assinatura, exige a intervenção de pessoas singulares que, estatutariamente, representam essa pessoa colectiva.

A AC Raiz MZ verifica a identidade dos representantes legais da ICP de Moçambique, por meio legalmente reconhecido, garantindo, no caso de o pedido ser subscrito para outrem, os poderes bastantes do requerente para a referida subscrição.

Quando requerido pela pessoa colectiva a constar como titular do certificado, é subscrito pelos seus representantes legais.

3.2.4 Documentos para Efeitos de Identificação de ICP de Moçambique

A AC Raiz MZ responsabiliza-se pela guarda de toda a documentação utilizada para verificação da identidade da ICP de Moçambique, garantindo a verificação da identidade dos seus representantes legais, por meio legalmente reconhecido, e garantindo, no caso dos seus representantes legais não se encontrarem na cerimónia de emissão de certificado, os poderes bastantes do representante nomeado pela entidade para a referida emissão.

O documento que serve de base ao registo da ICP de Moçambique contém, entre outros, os seguintes elementos:

a) Denominação legal;

b) Número de Identificação Fiscal, sede, objecto social, nome dos titulares dos corpos sociais e de outras pessoas com poderes para a obrigarem;

c) Nome completo, número do bilhete de identidade ou qualquer outro elemento que permita a identificação inequívoca das pessoas singulares que estatutária ou legalmente a representam;

d) Endereço e outras formas de contacto;

e) Indicação de que o certificado é emitido para a entidade, enquanto autoridade certificadora subordinada da AC Raiz MZ, na sua hierarquia de confiança, de acordo com o presente documento;

f) Nome único (DN) a ser atribuído ao certificado;

g) Informação, se necessário, relativa à identificação e aos poderes do(s) representante(s) nomeados pela entidade para estarem presentes na cerimónia de emissão do certificado de ICP de Moçambique;

h) Outras informações relativas ao formato do pedido de certificado a serem apresentadas na cerimónia de emissão do certificado de ICP de Moçambique.

3.2.5 Validação Dos Poderes de Autoridade Ou Representação

Nada a assinalar.

3.2.6 Critérios para Interoperabilidade

No caso de solicitação por parte das ICP de Moçambique de acordos de interoperabilidade, tendo como base certificação cruzada com outras infraestruturas de chaves públicas, a AC Raiz MZ deve exigir no mínimo a seguinte documentação:

a) Declaração de Práticas de Certificação e Política de Certificados;

b) O último relatório de auditoria, demonstrando a total conformidade com o estabelecido na PC e na DPC;

c) Os parâmetros respeitantes a validação técnica da certificação cruzada;

d) Todos os pedidos de acordos de interoperabilidade devem ser devidamente aprovados pelo CG.

3.3 Identificação e Autenticação para Renovação

3.3.1 Identificação e Autenticação para Pedidos de Renovação de Chaves

A identificação e autenticação para a renovação de certificados seguem os procedimentos utilizados para a autenticação e identificação inicial ou, utilizando pedidos assinados digitalmente, mediante o certificado original que se pretende renovar, sempre que este tenha expirado e não exista pedido para a sua revogação.

3.3.2 Identificação e Autenticação para Pedidos de Renovação de Chaves Depois de Revogação

Após revogado um certificado, será gerado novo par de chaves e emitido o respectivo certificado. A identificação e autenticação seguem os procedimentos para a autenticação e identificação inicial.

3.4 Identificação e Autenticação para Pedidos de Revogação de Chaves

Qualquer entidade integrada na cadeia de confiança da AC Raiz MZ, pode solicitar a revogação de um determinado certificado, sempre que se verifique ou se suspeite de compromisso da chave privada do titular ou qualquer outro acto que recomende esta acção.

Toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efectua o pedido de revogação pela AC Raiz MZ é guardada. Desta documentação refere-se, entre outra:

i. Representante legal da Autoridade Credenciadora, com poderes de representação para o pedido de revogação de certificados;

ii. Parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferentes dos previstos.

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

a) Denominação legal;

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

c) Nome completo, número de um documento de identificação que permita a identificação inequívoca da entidade (ou seu representante) que inicia o pedido de revogação;

d) Endereço e outras formas de contacto;

e) Indicação de pedido de revogação, indicando o nome único (DN) atribuído ao certificado, assim como a sua validade;

f) Indicação do motivo para revogação do certificado;

g) Informação das actividades a efectuar pela ICP de Moçambique para revogar todos os certificados emitidos pela mesma, no caso de revogação de certificado de ICP de Moçambique.

O pedido de revogação será analisado pelo CG, sendo que este avaliará a pertinência do pedido e tomará a decisão final.

4 Requisitos Operacionais do Ciclo de Vida do Certificado

Esta secção especifica os requisitos impostos aos certificados emitidos pela AC Raiz MZ para ACs credenciadas, autoridades de registo e listas de certificados revogados.

4.1 Pedido de Certificado

Devem ser cumpridos os seguintes requisitos no acto de solicitação de certificado:

i. Conformidade com as políticas definidas pela AC Raiz MZ;

ii. Pedido de certificado mediante apresentação de um pedido de certificado PKCS#10 válido;

iii. No caso de AC Emissora, o processo de credenciação da AC em questão já deve ter ocorrido e a mesma já deve ter autorização de início de actividade.

4.1.1 Quem pode Subscrever um Pedido de Certificado

O certificado auto-assinado da AC Raiz MZ apenas pode ser solicitado pelo seu detentor legal.

A AC Emissora deve ter sido previamente autorizada pelo CG, dentro da autorização é necessário identificar que pessoas podem efectuar a petição do certificado de AC.

O pedido de um certificado para uma AC Emissora é efectuado numa intervenção com objectivo de geração de par de chaves criptográficas, em ambiente seguro. O pedido é realizado por pessoa colectiva ou entidade com poder para representar a AC Emissora.

4.1.2 Processo de Registo e Responsabilidades

O processo de registo de AC Emissora é constituído pelos seguintes passos a serem efectuados pela entidade de certificação subordinada requerente:

1) Geração do par de chaves (chave pública e privada) pela AC Emissora;

2) Geração do PKCS#10 correspondente pela AC Emissora, em formato *Privacy-Enhanced Mail* (PEM) [16];

3) Gravação do Arquivo do PKCS#10 em mídia física, por exemplo, em uma USB flash drive (Pen Drive);

4) Preenchimento pela AC Emissora do documento de validação da identidade da entidade, de acordo com a Secção 4.1.1;

5) Envio do Pen Drive e do documento correctamente preenchido ao contacto da AC Raiz MZ.

4.2 Processamento do Pedido de Certificado

Os pedidos de certificado, depois de recebidos pela AC Raiz MZ, são considerados válidos se os seguintes requisitos forem cumpridos:

i. Recepção e verificação de toda a documentação e autorizações exigidas;

ii. Verificação da identidade do requisitante;

iii. Verificação da exactidão e integridade do pedido de certificado;

iv. Criação e assinatura do certificado;

v. Disponibilização do certificado ao titular.

A Secção 4.3 descreve detalhadamente todo o processo.

4.2.1 Processos para a Identificação e Funções de Autenticação

O grupo de trabalho de Administração de Segurança da AC Raiz MZ:

1) Identifica e a autentica toda a informação necessária nos termos da Secção 3.2.3;

2) Aprova a candidatura para um certificado de AC Emissora quando os seguintes critérios são preenchidos:

   i. Identificação e autenticação bem-sucedida de toda a informação necessária nos termos da Secção 3.2.3 (toda a documentação utilizada para verificação da identidade e de poderes de representação é guardada);

   ii. Formulário de pedido de emissão correctamente preenchido e aprovado pelo CG;

   iii. PKCS#10 válido.

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

Após a emissão do certificado, os Administradores de Segurança da AC Raiz MZ são responsáveis por entregar o certificado e restantes dados necessários pelo método "cara-a-cara" – tal acto é registado através do preenchimento e assinatura de um formulário.

4.2.2 Aprovação ou Recusa de Pedidos de Certificado

A aprovação de certificado passa pelo cumprimento dos requisitos exigidos nas secções 4.2 e 4.2.1. Quando tal não se verifique, é recusada a emissão do certificado.

4.2.3 Prazo para Processar o Pedido de Certificado

Após a aprovação do pedido de certificado, este deverá ser emitido no prazo máximo de 7 (sete) dias úteis.

4.3 Emissão de Certificado

4.3.1 Procedimentos para a Emissão de Certificado

4.3.1.1 AC Raiz MZ A emissão do certificado auto assinado da AC Raiz MZ é efectuada por meio de uma intervenção que decorre na zona de alta segurança da AC Raiz MZ, em que se encontram presentes, no mínimo:

a) Três (3) elementos pertencentes aos Grupos de Trabalho (a segregação de funções não possibilita a presença de um número inferior de elementos), sendo presença obrigatória o auditor de sistemas;

b) Um (1) membro da Autoridade Credenciadora;

c) Outros elementos autorizados pelo Grupo de Gestão (GG) da AC Raiz MZ.

A cerimónia de emissão de certificado da AC Raiz MZ é constituída pelos seguintes passos:

1) Auditor identifica e autentica todas as pessoas presentes em sala, garantindo que os membros do Grupo de Trabalho têm os poderes necessários para os actos a praticar, registando-os no livro de presenças;

2) Os membros dos Grupos de Trabalho executam:

   a) Procedimentos de arranque de processamento da AC Raiz MZ;
   b) Procedimentos de Emissão de Certificado;
   c) Gravação do certificado em Pen Drive;
   d) Procedimentos de finalização de processamento da AC Raiz MZ.

3) Auditor dá como finalizada a intervenção. O certificado emitido inicia a sua vigência no momento da sua emissão.

4.3.1.2 AC Emissora A emissão do certificado é efectuada por meio de uma intervenção que decorre na zona de alta segurança da AC Raiz MZ e, em que se encontram presentes:

a) Os representantes legais da Autoridade Certificadora do Estado requerente ou o(s) representante(s) nomeado(s) para esta intervenção;

b) Três (3) elementos pertencentes aos Grupos de Trabalho (a segregação de funções não possibilita a presença de um número inferior de elementos), sendo presença obrigatória o Auditor de Sistemas;

c) Outros elementos autorizados pelo GG da AC Raiz MZ.

A cerimónia de emissão de certificado para AC Emissora é constituída pelos seguintes passos:

1) Auditor, identifica e autentica todas as pessoas presentes na intervenção, garantindo que o(s) representante(s) da AC Emissora requerente e os membros dos Grupo de Trabalho têm os poderes necessários para os atos a praticar;

2) Representante(s) da AC Emissora requerente entregam em mão, aos membros do Grupo de Trabalho da AC Raiz MZ:

   a) Pen Drive com o pedido de certificado (ficheiro PKCS#10);

   b) Formulário de pedido de emissão do certificado;

3) Os membros do Grupo de Trabalho da AC Raiz MZ:

   a) Preenchem e assinam o formulário de pedido de emissão de certificado, devolvendo-o ao(s) representantes da AC Emissora requerente;

   b) Executam os procedimentos de arranque de processamento da AC Raiz MZ;

   c) Emitem o certificado (correspondente ao PKCS#10 fornecido no Pen Drive) em formato PEM;

   d) Gravam o certificado em formato PEM num Pen Drive;

   e) Preenchem o formulário de recepção e aceitação de certificado, em duplicado, assinando as ambas as cópias;

   f) Entregam o formulário de recepção e aceitação de certificado, original e duplicado, devidamente preenchidos ao(s) representante(s) da AC Emissora requerente solicitando a sua verificação e assinatura;

4) Os representante(s) da AC Emissora assinam os formulários de recepção e aceitação de certificado e devolvem uma das cópias aos membros dos Grupos de Trabalho;

5) Os membros do Grupo de Trabalho, entregam o Pen Drive com o certificado em formato PEM ao(s) representante(s) da AC Emissora;

6) Os membros do Grupo de Trabalho executam procedimentos de finalização de processamento da AC Raiz MZ;

7) Auditor dá como finalizada a intervenção.

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

4.3.2 Notificação da Emissão do Certificado ao Titular

A emissão do certificado é efectuada de forma presencial, de acordo com Secção 4.3.1.

4.4 Aceitação do Certificado

4.4.1 Procedimentos para a Aceitação de Certificado

O(s) representante(s) da Autoridade Certificadora para quem foi emitido o certificado é(são) responsável(veis) pela operação e instalação do certificado.

Após efectuados os procedimentos descritos na Secção 4.3.1, o certificado considera-se aceite.

4.4.2 Publicação do Certificado

No caso do certificado auto assinado da AC Raiz MZ, este é disponibilizado no endereço electrónico identificado na Secção 2.1.

A publicação dos certificados emitidos para as AC Emissora fica à sua responsabilidade, devendo estar disponíveis no seu respectivo repositório.

4.5 Utilização do Certificado e Par de Chaves

O titular do certificado deve tomar as devidas medidas de segurança física, lógica e processual de forma a garantir a protecção da sua chave privada.

O titular do certificado é responsável por assegurar que a utilização da sua chave privada apenas se destina para os fins definidos por ela, de acordo com o estabelecido nos campos “KeyUsage” do certificado.

4.5.1 Utilização do Certificado e da Chave Privada do Titular

A AC Raiz MZ apenas utiliza a sua chave privada para:

i. Assinatura de Certificados para AC Emissora,

ii. Assinatura de certificados para serviço validação online (OCSP);

iii. Assinar LCR.

As AC Emissoras apenas utilizam a sua chave privada para:

i. Emissão de certificados para serviços complementares à sua actividade de certificação,

ii. Lista de Certificados Revogados

iii. Titulares finais ou para ACs subordinadas.

4.5.2 Utilização do Certificado e da Chave Pública Pelas Partes Confiantes

As partes confiantes apenas confiam nos certificados tendo em conta apenas o que é estabelecido neste documento. Assim, deve ser garantido, entre outras, o cumprimento das seguintes condições:

i. Ter conhecimento e perceber a utilização e funcionalidades proporcionadas pela criptografia de chave pública e certificados;

ii. Ser responsável pela sua correcta utilização;

iii. Verificar os certificados (validação de cadeias de confiança) e LCR, tendo especial atenção às suas extensões marcadas como críticas e propósito das chaves;

iv. apenas utilizar os certificados válidos.

4.6 Renovação de Certificados

Podem-se distinguir dois processos de renovação de certificado, quanto ao par de chaves:

i. A renovação sem geração de par de chaves: processo em que a emissão de um novo certificado utiliza os dados anteriores do certificado, não havendo alteração das chaves ou qualquer outra informação, com excepção do período de validade do certificado. Esta prática não é suportada no SCDM.

ii. A renovação com geração de novo par de chaves (certificate re-key): processo em que um titular gera um novo par de chaves e submete o pedido para emissão de novo certificado. Este processo, no âmbito do SCDM, é designado por renovação de certificado com geração de novo par de chaves. O processo de renovação segue os mesmos procedimentos de uma nova emissão de certificado.

4.6.1 Motivo para a Renovação de Certificado

Considera-se motivo válido para a renovação de certificado com geração de novo par de chaves, sempre que sejam verificadas as seguintes situações:

1) Fim do período de validade, ou proximidade do mesmo;
2) O suporte do certificado esteja danificado ou indicia deterioração que poderá comprometer a sua utilização a curto prazo;
3) A informação do certificado não corresponda à realidade, ou sofra alterações;
4) Comprometimento das chaves ou perda de fiabilidade das mesmas.

4.6.2 Quem Pode Submeter o Pedido de Certificação de Uma Nova Chave Pública

Tal como descrito na Secção 4.1.1.

4.6.3 Processamento do Pedido de Renovação de Certificado

Tal como descrito na Secção 4.2.

4.6.4 Notificação da Emissão de Novo Certificado ao Titular

Tal como descrito na Secção 4.3.2.

4.6.5 Procedimentos para Aceitação de Um Novo Certificado

Tal como descrito na Secção 4.4.1.

4.6.6 Publicação de Certificado Renovado Com Geração de Novo Par de Chaves

Tal como descrito na Secção 4.4.2.

4.7 Renovação Com Geração de Novo Par de Chaves (Certificate Re-Key)

Tal como descrito na Secção 4.6.

4.8 Modificação de Certificados

Esta prática não é suportada no âmbito do SCDM.

4.9 Suspensão e Revogação de Certificado

A suspensão é acção pela qual um certificado perde temporariamente a sua validade, podendo após verificadas determinadas condições voltar ao estado Activo, ou caso contrário ser Revogado. A AC Raiz MZ não suspende certificados.

A revogação de certificados é a acção através da qual o certificado deixa de estar válido antes do fim do seu período de validade, perdendo a sua operacionalidade, ao contrário da suspensão, esta acção é irreversível.

4.9.1 Circunstâncias para Revogação

Qualquer uma das seguintes situações poderá originar à revogação de um certificado:

1) Comprometimento ou suspeita de comprometimento da chave privada;
2) Perda da chave privada;
3) Inexactidões graves nos dados fornecidos;
4) Fim de operação do certificado;
5) Perda, destruição ou deterioração do dispositivo de suporte da chave privada (por exemplo, suporte/token criptográfico);
6) Incumprimento por parte da AC ou titular das responsabilidades previstas na presente DPC;

7) Sempre que haja razões credíveis que induzam que os serviços de certificação possam ter sido comprometidos, de tal forma que coloquem em causa a fiabilidade dos certificados;

8) Por resolução judicial ou administrativa;

9) Por cessação de actividade da AC titular do certificado.

AC Raiz MZ pode revogar ou determinar a revogação do certificado ou da certificação cruzada, conforme o caso, da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas para o SCDM.

4.9.2 Quem Pode Submeter o Pedido de Revogação

A revogação do certificado de uma AC Emissora só poderá ser efectuada por:

i. Determinação do Comité Gestor;

ii. Determinação da AC Raiz MZ;

iii. Solicitação da própria AC Emissora; ou

iv. Determinação judicial.

A AC Raiz MZ guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efectua o pedido de revogação, garantindo a verificação da identidade dos seus representantes legais, por meio legalmente reconhecido, não aceitando poderes de representação para o pedido de revogação do certificado de AC Emissora.

4.9.3 Procedimento para o Pedido de Revogação

Os pedidos de revogação de certificado são efectuados a partir de um formulário e submetidos à AC Raiz MZ devem estar assinados electronicamente com um certificado de assinatura digital reconhecido em Moçambique, ou de forma manuscrita, sendo que neste último caso se deverá identificar o solicitante.

O pedido será avaliado pelo GG da AC Raiz MZ que junto do CG aprova ou não, a sua revogação. Deverão ser de seguida executadas as seguintes actividades:

a) Identificação e autenticação da entidade que efectua o pedido de revogação;

b) Registo e arquivo do formulário de pedido de revogação;

c) Mediante o parecer do GG da AC Raiz MZ, o responsável do organismo que a tutela, decide a aprovação ou recusa do pedido de revogação do certificado;

d) Sempre que se decidir revogar um certificado, a revogação é publicada na respectiva LCR.

Em qualquer dos casos, é arquivada a descrição pormenorizada de todo o processo de decisão, ficando documentado:

i. Data do pedido de revogação;

ii. Nome do titular do certificado (assinante);

iii. Exposição pormenorizada dos motivos para o pedido de revogação;

iv. Nome e funções da pessoa que solicita a revogação;

v. Informação de contacto da pessoa que solicita a revogação;

vi. Assinatura da pessoa que solicita a revogação.

4.9.4 Produção de Efeitos da Revogação

Após terem sido efectuados todos os procedimentos e seja verificado que o pedido é válido, o pedido não pode ser anulado. A revogação terá efeitos imediatos.

4.9.5 Prazo para Processar o Pedido de Revogação

O pedido de revogação deve ser tratado de forma imediata, pelo que em caso algum poderá ser superior a 24 horas.

4.9.6 Requisitos de Verificação da Revogação pelas Partes Confiantes

Antes da utilização de um certificado, as partes confiantes têm como responsabilidade verificar o estado de todo os certificados, através das LCR ou através do serviço de validação online (OCSP).

4.9.7 Circunstâncias para a Suspensão

Não é permitida, no âmbito do SCDM, a suspensão de certificados emitido para Autoridade Certificadora.

4.9.8 Quem Pode Solicitar Suspensão

Não aplicável.

4.9.9 Procedimentos para Pedido de Suspensão

Não aplicável.

4.9.10 Limite do Período de Suspensão

Não aplicável.

4.9.11 Frequência de Emissão da LCR

É publicada uma nova LCR no repositório, sempre que haja uma revogação. Quando não haja alterações ao estado de validade dos certificados, ou seja, se nenhuma revogação tiver sido produzida, a AC Raiz MZ disponibiliza uma nova LCR a cada 90 (noventa) dias.

4.9.12 Período Máximo Entre a Emissão e a Publicação da LCR

O período máximo entre a emissão e publicação da LCR não deverá ultrapassar as 3 horas.

4.9.13 Disponibilidade de Verificação Online do Estado / Revogação de Certificado

Para além da disponibilização da LCR, a AC Raiz MZ fornece um serviço de validação online de certificados por si emitidos. O endereço de acesso consta na secção 2.1.

4.9.14 Requisitos de Verificação Online de Revogação

No caso de ser utilizado o serviço de validação online (OCSP), as partes confiantes deverão dispor de software capaz de operar o protocolo OCSP, de forma a obter a informação sobre o estado do certificado.

4.9.15 Outras Formas Disponíveis para Divulgação de Revogação

Nada a assinalar.

4.9.16 Requisitos Especiais em Caso de Comprometimento de Chave Privada

Apenas quando se trate do comprometimento da chave privada de uma AC. Neste caso deverão ser adotados os procedimentos descritos na secção 5.7.3.

4.9.17 Fim de Subscrição

O fim da operacionalidade de um certificado acontece quando se verificarem uma das seguintes situações:

i. Revogação do certificado;

ii. Por ter caducado o prazo de validade do certificado.

4.10 Serviços sobre o Estado do Certificado

4.10.1 Características Operacionais

O estado dos certificados emitidos está disponível publicamente através das LCR e do serviço de validação online com implementação do protocolo OCSP, de acordo com o estipulado na RFC 6960 [17].

4.10.2 Disponibilidade do Serviço

O serviço sobre o estado do certificado está disponível 24 horas por dia, 7 dias por semana. No entanto, salvaguarda-se a possibilidade de interrupção por causa justificada e divulgada.

5 Controles operacionais, gerenciais e de instalações físicas

Esta secção descreve aspectos não técnicos de segurança que possibilitam, de modo seguro, realizar as funções de geração de chaves, autenticação dos titulares, emissão de certificados, revogação de certificados, auditorias e arquivo. Todos estes controlos não técnicos de segurança são críticos para garantir a confiança dos serviços disponibilizados.

5.1 Medidas de Segurança Física

5.1.1 Construção e Localização Física das Instalações da AC

O centro de processamento de dados da AC Raiz MZ é uma infraestrutura física que fornece um ambiente capaz de controlar e auditar o acesso aos sistemas de certificação, estando fisicamente protegida do acesso não autorizado, dano, ou interferência.

A arquitectura utiliza o conceito de profundidade, ou seja, por níveis de segurança, garantindo-se que o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado o nível imediatamente anterior, nunca sendo possível, em qualquer local das instalações, aceder ao nível de segurança (n) a partir de outro que não seja o nível (n-1).

As operações da AC Raiz MZ são realizadas numa sala com elevada segurança, dentro de um edifício que reúne diversas condições de segurança, nomeadamente o controlo total de acessos que previne, detecta e impede acessos não autorizados, baseado em múltiplos níveis de segurança física.

A sua construção são áreas que obedecem às seguintes características:

a) Paredes em alvenaria, betão ou tijolo;

b) Tecto e pavimento com construção similar à das paredes;

c) Porta de segurança, com chapa em aço, com as dobradiças fixas e ombreira igualmente em aço, com fechadura de segurança accionável electronicamente, características corta-fogo e funcionalidade antipânico.

Adicionalmente, as seguintes condições de segurança são garantidas:

a) Perímetros de segurança claramente definidos;

b) Paredes, chão e tecto em alvenaria, que impedem acessos não autorizados;

c) Trancas e fechaduras anti-roubo de alta segurança nas portas de acesso ao ambiente de segurança;

d) O perímetro do edifício é estanque na medida em que não existem portas, janelas ou outras brechas não controladas, que possibilitem acessos não autorizados;

e) Acesso ao ambiente passa obrigatoriamente por áreas de controlo humano, e por outros meios de controlo que restringem o acesso físico apenas a pessoal devidamente autorizado.

5.1.2 Acesso Físico ao Local

Os sistemas da AC Raiz MZ estão protegidos por 3 níveis de segurança física hierárquicos, garantindo-se que o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado os privilégios necessários ao nível imediatamente anterior.

As actividades operacionais sensíveis da CA, a criação e armazenamento de material criptográfico, quaisquer actividades no âmbito do ciclo de vida do processo de certificação como autenticação, verificação e emissão ocorrem dentro da zona mais restrita. O acesso a cada nível de segurança requer, pelo menos, o uso de um cartão de proximidade. Acessos físicos são automaticamente registados e gravados em circuito fechado de TV para efeitos de auditorias. Os sistemas estão integrados e em funcionamento de forma ininterrupta 24 horas, todos os dias do ano.

A pessoal, não acompanhado, incluindo colaboradores ou visitantes não autenticados não é permitida a sua entrada e permanência em áreas de segurança. A não ser que todo o pessoal que circule dentro destas áreas de segurança seja garantidamente reconhecido por todos, é obrigatória a utilização do respectivo cartão de acesso de modo visível, assim como garantir que não circulam indivíduos não reconhecidos sem o respectivo cartão de acesso visível.

O acesso ao centro de dados requer controlo duplo, cada um deles utilizando dois factores de autenticação. O hardware criptográfico e tokens físicos seguros dispõem de protecção adicional, sendo guardados em cofres e armários seguros. O acesso à zona mais restrita, assim como ao hardware criptográfico e aos tokens físicos seguros é restrito, de acordo com as necessidades de segregação de responsabilidades dos vários Grupos de Trabalho.

Todas as actividades e cerimónias (intervenções), assim como os acessos de visitantes à sala da AC, são registadas manualmente num Livro de Registo que se encontra no seu interior.

5.1.3 Energia e Ar Condicionado

A sala segura onde está localizada a AC Raiz MZ tem o seguinte equipamento redundante, que garante condições de funcionamento 24 horas por dia, 7 dias por semana:

a) Alimentação de energia garantindo alimentação contínua e ininterrupta com a potência suficiente para manter autonomamente a rede eléctrica durante períodos de falta de corrente e para proteger os equipamentos face a flutuações que os possam danificar (o equipamento redundante consiste em baterias de alimentação ininterrupta de energia, e geradores de electricidade a diesel); e

b) Refrigeração/ventilação/ar condicionado que controlam os níveis de temperatura e humidade, garantindo condições adequadas para o correcto funcionamento de todos os equipamentos electrónicos e mecânicos presentes na sala. É efectuada monitorização contínua das boas condições de suporte ao funcionamento das infraestruturas.

5.1.4 Exposição à Água

A sala segura onde está localizada a AC Raiz MZ tem instalado mecanismos (detectores de inundação) para minimizar o impacto de inundações nos sistemas.

5.1.5 Prevenção e Protecção Contra Incêndio

A sala segura onde está localizada a AC Raiz MZ tem instalado mecanismos necessários para evitar e apagar fogos ou outros incidentes derivados de chamas ou fumos.

Dispõe de sistemas detecção e extinção de incêndios instalados nos vários níveis físicos de segurança. Os equipamentos fixos e móveis estão disponíveis, colocados em sítios estratégicos e de fácil acesso de modo a poderem ser rapidamente usados no início de um incêndio e extinguilo com sucesso.

Os materiais da sala e portas utilizadas são de material não combustível e resistentes ao fogo. Estão definidos procedimentos de emergência.

5.1.6 Salvaguarda de Suportes de Armazenamento

Os suportes de informação sensível estão armazenados de forma segura em cofres e armários de segurança dentro da zona segura, assim como num ambiente distinto externo ao edifício com controlos de acessos físicos e lógicos apropriados para restringir o acesso apenas a elementos autorizados dos Grupos de Trabalho. Para além das restrições de acessos, também tem implementado mecanismos de protecção contra acidentes (e.g., causados por água ou fogo).

Quando, para efeito de arquivo de cópias de segurança, a informação sensível é transportada da zona de alta segurança para o ambiente externo, o processo é executado sob supervisão de pelo menos 2 (dois) elementos do Grupo de Trabalho que têm por obrigação garantir o transporte seguro da informação até ao local de destino. A informação (ou o token de transporte da informação) deverá estar sempre sob controlo visual dos membros do Grupo de Trabalho.

Em situações que impliquem a deslocação física de hardware de armazenamento de dados (i.e., discos rígidos, entre outros) para fora da zona de alta segurança, por motivos que não o arquivo de cópias de segurança, cada elemento do hardware deverá ser verificado para garantir que não contém dados sensíveis. Nestas situações, a informação é eliminada usando todos os meios necessários para o efeito (a título de exemplo: formatação lógica, reset do hardware criptográfico ou mesmo destruição física do equipamento de armazenamento).

5.1.7 Eliminação de Resíduos

Todos os documentos e materiais em papel que contenham informação sensível deverão ser triturados antes da sua eliminação, sob supervisão de um elemento do Grupo de trabalho de Auditoria que regista essa acção.

Antes de serem eliminados quaisquer suportes de informação utilizados para armazenar ou transmitir informação sensível, devem ser eliminados todos os dados e informações através de formatação "segura" de baixo nível ou destruição física.

Todos os equipamentos criptográficos ou chaves físicas de acesso lógico são fisicamente destruídos ou seguem as recomendações de destruição do respectivo fabricante, antes da sua eliminação.

Outros equipamentos de armazenamento (discos rígidos, tapes, entre outros) deverão ser devidamente limpos de modo a não ser possível recuperar nenhuma informação (através de formatações seguras, ou destruição física dos equipamentos).

5.1.8 Instalações Externas (Alternativa) para Recuperação de Segurança

Todas as cópias de segurança são armazenadas em ambiente seguro em instalações geograficamente distintas das instalações primárias ficando alojadas em cofres e armários seguros situados em zonas com controlos de acesso físicos e lógicos, de modo a restringir o acesso apenas a pessoal autorizado, garantindo também a protecção contra danos acidentais (e.g., causados por água ou fogo).

5.2 Medida de Segurança dos Processos

Os indivíduos considerados de confiança incluem todos os elementos aos quais foram atribuídos acesso aos activos da ICP do SCDM, principalmente ao ambiente mais restrito de toda a infraestrutura onde são executadas as operações criptográficas.

5.2.1 Funções de Confiança

São consideradas funções de confiança, todas as aquelas que incluem actividades como:

1) Gestão dos sistemas tecnológicos da infraestrutura;
2) Gestão dos sistemas de segurança da infraestrutura;
3) Gestão do ciclo de vida dos certificados digitais, nomeadamente:
   a) Validação dos pedidos de emissão de certificado digital;
   b) Aceitação, rejeição, pedido de revogação, de renovação ou outro processo de emissão de Certificado digital;
   c) Emissão, revogação de certificados digitais;
   d) Disseminação dos certificados digitais;
   e) Gestão dos estados dos certificados digitais.

As funções de confiança são agrupadas mediante as actividades em questão, sendo que dão origem à criação de grupos de trabalho, com responsabilidade diferenciadas.

De forma a minimizar a importância individual de cada indivíduo, são constituídos vários grupos de trabalho com separação de deveres e responsabilidades, garantindo que as operações sensíveis são efectadas por diferentes pessoas autenticadas , eventualmente pertencentes a diferentes Grupos de Trabalho.

Assim, estabelecem-se funções de confiança agrupadas por 7 grupos de trabalho. Sendo que destes grupos, 6 serão considerados grupos de trabalho operacionais, pois intervêm directamente na infraestrutura tecnológica e 1 será considerado de suporte, denominado de Grupo de Custódia, não tendo qualquer intervenção na infraestrutura, tem à sua responsabilidade activos necessários à operacionalização que disponibilizam, mediante regras bem definidas, aos grupos de trabalho operacionais.

Cada grupo de trabalho operacional deve ser constituído por um mínimo de 3 (três) indivíduos, a fim de garantir a sua redundância.

Os grupos de trabalho operacionais são:

i. Administração de Segurança;
ii. Auditoria;
iii. Administração de Sistemas;
iv. Operação de Sistemas;

v. Administração de Registo;

vi. Gestão.

O grupo de trabalho de suporte, denominado de Grupo de Custódia, deverá ser subdividido em dois, a fim de garantir a disponibilidade 24x7 dos activos à sua responsabilidade, aos elementos dos grupos de trabalho operacionais, sendo que, no mínimo, cada um deve ser constituído por 2 elementos.

5.2.1.1 Grupos Operacionais

5.2.1.1.1 Grupo de Administração de Segurança

O Grupo de Trabalho de Administração de Segurança é responsável pela segurança global dos sistemas, nomeadamente a implementação das regras e práticas de segurança definidas para a AC Raiz MZ e pelas AC Emissora que a integram, assegurando que se encontram atualizadas de forma a garantir que toda a informação indispensável ao funcionamento e auditoria do sistema se encontra disponível ao longo do tempo.

São responsabilidades deste grupo de trabalho:

1) Gerir os activos à sua responsabilidade;

2) Detentor de tokens de administração do hardware segurança (HSM) que armazena as chaves criptográficas da AC;

3) Coordenar os restantes elementos dos grupos de trabalho;

4) Explicar todos os mecanismos de segurança aos recursos humanos que devam conhecê-los e de consciencializá-los para as questões de segurança levando-os a fazer cumprir as normas e políticas de seguranças estabelecidas;

5) Calendarizar intervenções em ambiente de produção, verificando as necessidades relativamente a recursos humanos, activos de informação e procedimentos necessários;

6) Gerir todas as políticas da AC Raiz MZ e garantir que se encontram atualizadas e adaptadas à sua realidade;

7) Cumprir e fazer cumprir as políticas definidas;

8) Gerir qualquer aspecto inerente à segurança física, das aplicações, da rede, dos recursos humanos;

9) Resolver os incidentes de segurança e eliminar todas as vulnerabilidades detectadas;

10) Gerir os controlos dos sistemas de segurança física do ambiente de produção e de todos os controlos de acesso;

11) Configurar a aplicação de gestão de ciclo de vida de certificados digitais, no que diz respeito a:

    a) Acessos;

    b) Perfis de certificados digitais.

12) Gerir as palavras-chave do sistema;

13) Estabelecer os calendários para a execução de análise de vulnerabilidades, testes, e formação bem como dos planos de continuidade de serviço e auditoria dos sistemas de informação;

14) Colaborar com os Auditores em tudo aquilo que lhe for solicitado.

5.2.1.1.2 Grupo de Auditoria de Sistemas

É responsável por efectuar a auditoria interna a todas as acções relevantes e necessárias para assegurar a correcta operacionalização da infraestrutura. Deverá este estar representado em todas as intervenções na infraestrutura. As responsabilidades deste grupo são:

1) Gerir os activos de informação à sua responsabilidade;

2) Verificar a execução e confirmar a exatidão dos processos e intervenções na infraestrutura;

3) Verificar a coerência da documentação e dos procedimentos executados nas intervenções na infraestrutura;

4) Verificar o conhecimento dos procedimentos por parte do pessoal implicado;

5) Verificar e analisar periodicamente a protecção dos sistemas (exposição a vulnerabilidades, registos de acesso, utilizadores, etc.);

6) Verificar e analisar periodicamente a funcionalidade dos controlos de segurança (dispositivos de alarme, de controlo de acessos, sensores de fogo, etc.) existentes nos vários ambientes;

7) Registar todos os procedimentos passíveis de auditoria;

8) Registar os resultados de todas as acções por si realizadas;

9) Verificar que todos os activos de informação e de suporte utilizados nas intervenções são seguros;

10) Verificar periodicamente o armazenamento dos activos de informação e de suporte inerentes à infraestrutura que são utilizados nas intervenções;

11) Verificar a adequação das práticas executadas com a legislação e normativos em vigor;

12) Verificar o cumprimento das regras definidas internamente e internacionalmente na operação e manutenção do sistema;

13) Executar os planos de Auditoria Interna definidos pelo grupo de trabalho de administração de segurança.

5.2.1.1.3 Grupo de Administração de Sistemas

É responsável por executar as tarefas manutenção do Hardware e Software do sistema de gestão do ciclo de vida de certificados digitais. É da sua responsabilidade:

a) Gerir os activos de informação à sua responsabilidade;

b) Instalar e configurar o software de base da infraestrutura;

c) Gerir e actualizar o software instalado;

d) Executar tarefas de manutenção do sistema, ao nível de Hardware e Software;

e) Garantir a prestação do serviço com o adequado nível de qualidades e fiabilidade em função do grau de criticidade do mesmo;

f) Monitorizar, reportar e quantificar todos os eventos inerentes a software e hardware, comunicando ao Grupo de Trabalho de Administração de Segurança e despoletando os processos apropriados à correcção dos mesmos;

g) Colaborar com os auditores em tudo aquilo que lhe for solicitado.

5.2.1.1.4 Grupo de Operação de Sistemas

É responsável por executar as tarefas de rotina essenciais ao bom funcionamento e operacionalidade da infraestrutura. Nenhum membro deste grupo está autorizado a entrar no "Ambiente de Produção" sem a presença de um membro do "Grupo de Trabalho de Administração de Segurança" e/ou do "Grupo de Trabalho de Auditoria". Este grupo deve ser constituído por pelo menos 4 (quatro) elementos e deve ter um cofre onde depositará activos que ficarão à sua responsabilidade, ao qual será atribuída a designação de "Ambiente de Operação". As responsabilidades deste grupo são:

a) Gerir os activos de informação à sua responsabilidade;

b) Cada um dos elementos é detentor de 1 de N tokens de autenticação do hardware criptográfico (HSM) que armazena as chaves criptográficas da AC permitindo o acesso às mesmas.

c) Executar as tarefas de rotina dos sistemas;

d) Realizar operações de cópias de segurança dos seus sistemas, garantindo a sua actualização;

e) Manter o inventário dos equipamentos e servidores que compõem a infraestrutura.

Esta função pode ser acumulada pelo grupo de trabalho de Administração de Sistemas.

5.2.1.1.5 Grupo de Administração de Registo

O grupo de trabalho de Administração de Registo é responsável:

a) Pela validação dos pedidos de certificados, efectados pelas AC's;

b) Pela aprovação da emissão de certificados digitais;

c) Pela validação dos pedidos de alteração de estado dos certificados digitais (suspensão e revogação);

d) Colabora com os Auditores em tudo aquilo que lhe for solicitado.

5.2.1.1.6 Grupo de Gestão (GG)

Este grupo de trabalho é responsável pela nomeação de indivíduos para integrar os grupos de trabalho identificados e pela tomada de decisões de nível crítico para a AC Raiz MZ. As suas responsabilidades são:

a) Rever e aprovar as políticas propostas pelo Grupo de Trabalho de Administração de Segurança;

b) Pedir a aprovação de Políticas ao CG;

c) Designar os membros dos restantes grupos de trabalho;

d) Disponibilizar a identificação de todos os indivíduos que pertencem aos vários Grupos de Trabalho, em um ou mais pontos de acesso facilmente acessíveis pelos indivíduos autorizados;

e) É o ponto de contacto com o CG.

5.2.1.2 Grupo de Suporte

5.2.1.2.1 Grupo de Custódia

Em complemento e contrariamente aos grupos de trabalho identificados anteriormente, este é constituído por elementos externos e, consequentemente, não terão qualquer autorização de acesso à infraestrutura tecnológica, nem a dados sensíveis da AC Raiz MZ, é considerado um grupo de trabalho de suporte.

É responsável por um ambiente denominado de ambiente de custódia, normalmente um cofre, onde estão armazenados activos (exemplo: chaves de cofres, tokens de autenticação, entre outros) que de modo isolado, não têm qualquer utilidade. Estes activos apenas poderão ser acedidos/levantados pelos membros dos outros grupos de trabalho, mediante a satisfação de determinadas condições previamente definidas, por exemplo, verificação de identidade de quem solicita o levantamento, garantia de pertença aos grupos de trabalho e autorização de acesso ao referido activo.

No sentido de melhorar os níveis de segurança, operacionalidade e permitir a continuidade do serviço da AC Raiz MZ, poderão existir várias instâncias deste grupo, cada qual encarregue da custódia de um conjunto distinto de activos.

As responsabilidades deste grupo são:

a) Gerir o "Ambiente de Custódia" respectivo;

b) Guardar os activos armazenados no referido ambiente, usando os meios adequados que respondam às necessidades de segurança respectivas;

c) Registar e conservar os registos de levantamento e depósito de artefactos;

d) Disponibilizar de forma segura os activos a membros de grupos autorizados e explicitamente indicados com permissões de acesso, e após o cumprimento dos procedimentos apropriados de segurança.

5.2.2 Número de Pessoas Exigidas por Tarefa

De modo a garantir que actividades sensíveis são executadas por um conjunto múltiplo de indivíduos autenticados, são definidos procedimentos de controlo que obrigam à divisão de responsabilidades tendo em conta as especificidades de cada Grupo de Trabalho.

Os referidos procedimentos são elaborados de forma a garantir um mínimo de 2 indivíduos autenticados para se ter acesso físico ou lógico aos equipamentos de segurança. O acesso ao hardware criptográfico segue procedimentos específicos que obrigam vários indivíduos

autorizados a aceder-lhe durante o seu ciclo de vida, desde a recepção, inspecção e utilização, até à sua destruição física e/ou lógica.

5.2.3 Identificação e Autenticação para cada Função

Os indivíduos pertencentes aos grupos de trabalho autenticam-se em conta própria para acesso às máquinas sendo que o acesso à aplicação de gestão do ciclo de vida dos certificados digitais é executado com recurso à utilização de um certificado digital próprio emitido para o efeito, na própria infraestrutura.

Relativamente ao HSM, a autenticação é efectada através de técnicas de segredo partilhado, utilizando vários tokens à responsabilidade de vários elementos dos grupos de trabalho.

A autenticação complementa-se com as correspondentes autorizações para aceder a determinados activos de informação dos sistemas da AC Raiz MZ.

5.2.4 Separação Funcional de Responsabilidades

A Tabela 4 identifica as funções incompatíveis, dentre as funções operacionais identificadas. As funções incompatíveis são aquelas em que um indivíduo não possa ter duas funções marcadas como "incompatíveis".

Tabela 4: Incompatibilidade de Funções.

Grupo	G-Seg	G-Reg	G-Adm	G-Oper	G-Audit	G-Gest
G-Seg		✓	✗	✓	✗	✗
G-Reg	✓		✓	✓	✗	✗
G-Adm	✗	✓		✓	✗	✗
G-Oper	✓	✓	✓		✗	✗
G-Audit	✗	✗	✗	✗		✗
G-Gest	✗	✗	✗	✗	✗	

Nesta tabela, o símbolo ✓significa compatível e o símbolo ✗, incompatível.

Da matriz de incompatibilidade e podendo-se acumular funções, é possível reorganizar competências com intuito de minimizar a alocação de recursos e esforço (custo) inerentes à operação da AC Raiz MZ. Para alcançar este objectivo restringir a 4, os 6 grupos de trabalho operacionais anteriormente identificados, passando a AC Raiz MZ a ser constituída pelos seguintes grupos de trabalho:

i. Administração de Segurança;
(não acumula funções)

ii. Administração de Sistemas;
(acumula funções com Administração de Registo e Operação de Sistemas)

iii. Auditor de Sistemas;
(não acumula funções)

iv. Gestão.
(não acumula funções)

5.3 Medidas de Segurança Pessoal

Todos os elementos que desempenhem funções de confiança devem cumprir os seguintes requisitos:

1) Terem sido formalmente nomeados para a função;

2) Apresentarem provas de idoneidade;

3) Apresentarem provas de antecedentes, qualificações e experiência necessárias para a realização das tarefas dos Grupos de Trabalho;

4) Tiverem recebido formação e treino adequado para o desempenho da respectiva função;

5) Garantir que não é revelada informação sensível sobre a AC ou dados de identificação dos titulares;

6) Garantir que conhecem os termos e condições para o desempenho da respectiva função;

7) Garantir que não desempenham funções que possam causar conflito com as suas responsabilidades nas actividades da AC Raiz MZ.

5.3.1 Requisitos Relativos às Qualificações, Experiência, Antecedentes e Credenciação

A selecção de pessoal para desempenho de funções no SCDM deve obedecer a requisitos compatíveis com a necessidade de preservação da confiança no sistema. Esses requisitos devem ser particularmente verificados no momento de admissão, mas também devem ser periodicamente reverificados.

5.3.2 Procedimento de Verificação de Antecedentes

A admissão de pessoal para desempenho de funções no SCDM deve ter em atenção a especial confiança e idoneidade necessárias para assegurar que o sistema não é comprometido por falhas no processo de selecção de tal pessoal.

Nessa medida, são estabelecidos os seguintes requisitos para o processo de admissão:

a) Devem ser adoptados critérios rígidos para o processo de selecção, com o propósito de selecionar, para o desempenho de funções no SCDM de pessoas reconhecidamente idóneas e sem antecedentes que possam comprometer a segurança ou credibilidade do sistema.

b) O pessoal admitido deve estar autorizado a aceder a informação classificada com o grau de sigilo "Confidencial".

c) Não serão admitidos estagiários no exercício de actividades directamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gestão de certificados.

d) No momento da admissão, a pessoa seleccionada assinará um termo de compromisso assumindo o dever de manter sigilo, mesmo após a cessação de funções, sobre todos os activos de informações do SCDM.

e) Devem ser verificados os antecedentes do candidato, verificando o respectivo registo criminal, disciplinar e avaliação de desempenho profissional.

f) Deve ser realizada entrevista de admissão, por profissional qualificado, com o propósito de confirmar e/ou identificar dados não detectados ou não confirmados, durante o processo de admissão.

5.3.3 Requisitos de Formação e Treino

O SCDM ou parte integrante, deve monitorizar e avaliar periodicamente os recursos humanos com intuito de obter informação concisa sobre a necessidade de actualização de conhecimentos técnicos e de segurança, devendo por isso ter um plano anual de formação de forma a garantir a actualização de conhecimentos dos seus recursos.

Ainda neste contexto devem ser apresentados aos seus recursos humanos e prestadores de serviço as normas e procedimentos relativos ao tratamento e manuseamento dos activos de informação, a fim de desenvolver e manter uma efectiva conscientização de segurança, assim como instruir o seu fiel cumprimento.

Os elementos dos Grupos de Trabalho estão sujeitos a um plano de formação anual, englobando os seguintes tópicos:

a) Certificação digital e Infra-estruturas de Chave Pública;

b) Conceitos gerais sobre segurança da informação;

c) Formação específica para o seu papel dentro do Grupo de Trabalho;

d) Funcionamento do software e/ou hardware usado pela AC;

e) Política de Certificados e Declaração de Práticas de Certificação;

f) Recuperação face a desastres;

g) Procedimentos para a continuidade da actividade;

h) Aspectos legais básicos relativos à prestação de serviços de certificação.

Sempre que necessário deve ser ministrada formação complementar aos membros dos Grupos de Trabalho, de modo a garantir o nível pretendido de conhecimento para a execução competente e satisfatória das suas responsabilidades. Em particular:

a) Sempre que se verifique qualquer alteração tecnológica, introdução de novas ferramentas ou modificação de procedimentos, é realizada adequada formação para todos os elementos dos grupos de trabalho;

b) Sempre que são introduzidas alterações no presente documento são realizadas sessões de reciclagem.

5.3.4 Frequência e Requisitos para Acções de Reciclagem

Os elementos dos Grupos de Trabalho estão sujeitos a um plano de formação anual e sempre que verificada necessidade de formação complementar.

5.3.5 Frequência e Sequência da Rotação de Funções

Esta rotatividade não tem carácter obrigatório e por isso não está estipulado nenhum plano de rotação na atribuição de tarefas ao pessoal do SCDM.

5.3.6 Sanções para Acções não Autorizadas

Consideram-se acções não autorizadas todas as acções que desrespeitem os documentos regulamentadores do SCDM, sejam cometidas de forma deliberada ou por mera negligência.

Se for cometida alguma infracção, a entidade gestora da AC suspenderá de forma imediata, o acesso a todos os sistemas, às pessoas envolvidas com o conhecimento destas.

O incumprimento pelo pessoal afeto a funções no SCDM das instruções do CG ou do GG integrada no sistema é passível de sanção disciplinar, nos termos do quadro legal aplicável à relação entre o infractor e a sua entidade empregadora.

Caso tal incumprimento envolva a quebra de sigilo inerente ao SCDM, o infractor será ainda sujeito às sanções criminais aplicáveis à divulgação de informação sob segredo de Estado e à violação de sigilo profissional.

5.3.7 Requisitos para Contratação de Pessoal

A selecção de pessoal para desempenho de funções no SCDM deve obedecer a requisitos compatíveis com a necessidade de preservação da confiança no sistema. Esses requisitos devem ser particularmente verificados no momento de admissão, mas também devem ser periodicamente reverificados.

5.3.8 Documentação Fornecida ao Pessoal

É disponibilizada aos membros dos Grupos de Trabalho toda a informação adequada para que estes possam realizar as suas tarefas de modo competente e satisfatório.

5.4 Procedimentos de Auditoria de Segurança

5.4.1 Tipos de Eventos Registados

Todas as acções executadas pelos membros dos grupos de trabalho alocados à AC Raiz MZ, no desempenho de suas funções, são registadas de modo que cada uma delas esteja associada ao indivíduo que a realizou.

São registados em arquivos de auditoria todos os eventos relacionados com a segurança do sistema de certificação. De entre outros, registam-se os seguintes:

i. Tentativas de sucesso ou fracasso da alteração dos parâmetros de segurança do sistema operativo;

ii. Arranque e paragem de aplicações;

iii. Tentativas de sucesso ou fracasso de início e fim da sessão;

iv. Tentativas de sucesso ou fracasso na criação, modificação ou eliminação contas do sistema;

v. Tentativas de sucesso ou fracasso na solicitação, geração, assinatura, emissão ou revogação de chaves e certificados;

vi. Tentativas de sucesso ou fracasso na geração ou emissão de Listas de Certificados Revogados (LCRs);

vii. Publicação das LCR's;

viii. Tentativas de sucesso ou fracasso na criação, modificação ou eliminação de informação dos titulares dos certificados;

ix. Tentativas de sucesso ou fracasso de acesso às instalações por parte de pessoal autorizado, ou não;

x. Cópias de segurança, recuperação ou arquivo dos dados;

xi. Alterações ou atualizações de software e hardware;

xii. Manutenção do sistema;

xiii. Tentativas de iniciação, remoção, atribuição ou remoção de utilizadores nos sistemas;

xiv. Alteração de perfis de certificados;

xv. Alterações na configuração da AC e/ou nas suas chaves;

xvi. Geração de chaves e das bases de dados de gestão de chaves.

São também recolhidas e consolidadas, electrónica ou manualmente, informações de segurança não geradas directamente pelo sistema de certificação, tais como:

i. Registos de acessos físicos;

ii. Manutenção e mudanças na configuração dos seus sistemas;

iii. Mudanças de pessoal;

iv. Relatórios de discrepância e comprometimento;

v. Registos de destruição de dispositivos de armazenamento contendo chaves criptográficas, dados de activação de certificados ou informação pessoal de utilizadores;

vi. Remoção ou introdução de equipamentos informáticos na infraestrutura de chaves públicas. As entradas nos registos incluem a informação seguinte:

vii. Data e hora do evento;

viii. Identidade do sujeito que causou o evento;

ix. Categoria do evento;

x. Descrição do evento.

5.4.2 Frequência da Auditoria de Registos

Os registos de auditoria deverão ser analisados seguindo procedimentos manuais e automáticos, no mínimo, trimestralmente, ou em caso de suspeita de comprometimento da segurança.

Tal análise envolve uma inspecção breve de todos os registos, verificando que não foram alterados, seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades detectadas nos mesmos.

Todos os eventos significativos deverão ser registados e explicados em relatório de auditoria aquando a sua verificação assim como todas as acções tomadas em decorrência dessa análise serão documentadas.

5.4.3 Período de Retenção dos Registos de Auditoria

Os registos de auditoria referidos na secção 5.4.1 deverão ser mantidos nas usas instalações por pelo menos 2 (dois) meses, caso não esteja legislado esta periodicidade e, posteriormente, devem ser armazenados:

a) Certificados de assinatura digital e respectivas LCRs deverão ser retidos permanentemente, para fins de consulta histórica;

b) As cópias dos processos de acreditação de ACs, devem ser retidos por, no mínimo, 20 (vinte) anos a contar da data de expiração ou revogação do certificado, caso não esteja legislada esta periodicidade;

c) As demais informações, inclusive arquivos de auditoria, deverão ser retidas por, no mínimo, 6 (seis) anos.

5.4.4 Protecção dos Registos de Auditoria

Os registos de auditoria deverão estar protegidos e armazenados fisicamente cumprindo os mesmos requisitos de segurança implementados na sua origem. Os eventos registados deverão estar protegidos mediante técnicas criptográficas, de forma que nada, salvo as próprias aplicações de visualização de eventos, com seu devido controlo de acessos, lhes possa aceder.

A destruição de um registo de auditoria só poderá ser efectada após recomendação escrita, emitida por um Administrador de Segurança e Auditor de Sistemas e aprovada pelo GG da AC Raiz MZ.

5.4.5 Procedimentos para a Cópia de Segurança dos Registos

Os registos de auditoria devem, ser alvo de cópias de segurança que deverão ser armazenadas em local externo à infraestrutura principal da AC, recebendo o mesmo tipo de protecção utilizada por ela e seguindo os períodos de retenção definidos para os registos dos quais são cópias.

Os procedimentos de cópia de segurança (backup) e de recuperação devem estar documentados, mantidos atualizados e devem ser regularmente, pelo menos a cada 6 (seis) meses, testados, de modo a garantir a disponibilidade da informação.

5.4.6 Sistema de Recolha de Registos (Interno / Externo)

Os registos são recolhidos em simultâneo interna e externamente ao sistema da AC.

5.4.7 Notificação de Agentes Causadores de Eventos

Todos os eventos auditáveis devem ser registados no sistema de auditoria e guardados de modo seguro. Salienta-se que se verificado evento anómalo ou suspeito, este deverá analisado ao pormenor e, caso de justifique deverá ser solicitado esclarecimento ao sujeito causador, caso contrário não haverá qualquer outra notificação.

5.4.8 Avaliação de Vulnerabilidades

Os eventos que representem uma possível vulnerabilidade ou fragilidade para o sistema, detectada na análise efectada dos registos de auditoria são analisados detalhadamente e, dependendo da sua gravidade, devem ser registados em separado. Em consequência, o resultado da análise deve ser acompanhado de um plano de acções correctivas e remetido para apreciação e aprovação ao GG da AC Raiz MZ. A sua implementação deverá ser alvo de registo para fins de auditoria.

5.5 Arquivo de Registos

5.5.1 Tipos de Dados Arquivados

Todos os dados auditáveis são arquivados, assim como informação de pedidos de certificados e documentação de suporte ao ciclo de vida das várias operações. Os dados auditáveis serão entre outros:

i. Solicitações de certificados;

ii. Solicitações de revogação de certificados;

iii. Notificações de comprometimento de chaves privadas;

iv. Emissões e revogações de certificados;

v. Emissões de LCR;

5.5.2 Período de Retenção em Arquivo

Os dados sujeitos a arquivo são retidos pelo período de tempo definido pela legislação nacional, no caso de omissão deverão ser arquivados pelo período de 20 (vinte anos).

5.5.3 Protecção dos Arquivos

O arquivo é protegido de modo a que:

i. Apenas membros autorizados dos Grupos de Trabalho possam consultar e ter acesso ao arquivo;

ii. O arquivo é protegido contra qualquer modificação ou tentativa de o remover;

iii. O arquivo é protegido contra a deterioração do dispositivo de armazenamento, através de migração periódica para um dispositivo de armazenamento novo;

iv. O arquivo é protegido contra a obsolescência do hardware, sistemas operativos e outro software, pela conservação do hardware, sistemas operativos e outro software que passam a fazer parte do próprio arquivo, de modo a permitir o acesso e uso dos registos guardados, de modo intemporal, e

v. Os arquivos são guardados de modo seguro em ambientes externos.

5.5.4 Procedimentos para as Cópias de Segurança do Arquivo

Cópias de segurança dos arquivos são executadas de modo incremental ou total e guardados em dispositivos WORM (Write Once Read Many).

5.5.5 Requisitos para Validação Cronológica dos Registos

Algumas das entradas dos arquivos contêm informação de data e hora. Tais informações de data e hora não têm por base uma fonte de tempo segura.

5.5.6 Sistema de Recolha de Dados de Arquivo (Interno / Externo)

Os sistemas de recolha de dados de arquivo são internos.

5.5.7 Procedimentos de Recuperação e Verificação de Informação Arquivada

Apenas membros autorizados dos Grupos de Trabalho têm acesso aos arquivos. A integridade do arquivo deve ser verificada através da sua restauração.

5.6 Troca de Chaves (key changeover)

Os procedimentos de mudança de chave permitem a transição de certificados de CA a expirar para novos certificados.

No fim de vida útil da chave privada de uma AC, esta deixa de a utilizar para assinar certificados (antes de expirar) utilizando-a apenas para assinar as LCR's.

Antes expirar o certificado da AC é gerado um novo par de chaves sendo que todos os certificados e LCRs emitidos posteriormente passam a ser assinados com a nova chave privada.

Tanto o antigo, quanto o novo par de chaves podem estar activos simultaneamente. Este processo de mudança de chave ajuda a minimizar quaisquer efeitos adversos inerentes à expiração do Certificado de uma AC.

Este processo no âmbito do SCDM segue os procedimentos de uma nova emissão de certificado descritos na secção 4.

5.7 Recuperação em Caso de Desastre ou Comprometimento

Esta secção descreve os requisitos relacionados com os procedimentos de notificação e de recuperação no caso de desastre ou de comprometimento.

5.7.1 Procedimentos em Caso de Incidente ou Comprometimento

Cópias de segurança das chaves privadas da AC e dos registos arquivados (secção 5.4.1) são guardados em ambientes seguros externos e disponíveis em caso de desastre ou de comprometimento.

5.7.2 Corrupção dos Recursos Informáticos, do Software e/ou dos Dados

No caso dos recursos informáticos, software e/ou dados estarem corrompidos ou existir suspeita de corrupção, as cópias de segurança da chave privada da AC e os registos arquivados podem ser obtidos para verificação da integridade dos dados originais.

Se for confirmado que os recursos informáticos, software e/ou dados estão corrompidos, devem ser tomadas medidas apropriadas de resposta ao incidente.

A resposta ao incidente pode incluir o restabelecimento do equipamento/dados corrompidos, utilizando equipamento similar e/ou recuperando cópias de segurança e registos arquivados. Até que sejam repostas as condições seguras, o GG da AC Raiz MZ suspenderá os seus serviços e notificará o CG.

5.7.3 Procedimentos em Caso de Comprometimento da Chave Privada da Entidade

No caso da chave privada da AC Raiz MZ ser comprometida ou haver suspeita do seu comprometimento, devem ser tomadas medidas apropriadas de resposta ao incidente. A resposta a este incidente será:

1) Notificar:

   i. INTIC;
   ii. CG;
   iii. Autoridade Credenciadora
   iv. Todas as AC's integradas no "ramo" da hierarquia de confiança da AC Raiz MZ, assim como os titulares finais de que será revogado o certificado da AC Raiz MZ;

2) Revogar:

   i. Todos os certificados emitidos no "ramo" da hierarquia de confiança da AC Raiz MZ, pela seguinte ordem:
      a) Titulares finais
         Emissão e disponibilização de LCR da AC subordinada;
      b) Revogação do certificado digital da AC subordinada;
         Emissão e disponibilização de LCR da AC Emissora;
      c) AC Emissora;
         Emissão e disponibilização de LCR da AC Raiz MZ;
   ii. Certificado da AC Raiz MZ

3) Geração de novo par de chaves para a AC Raiz MZ, e emissão de novo certificado;

4) Renovação de todos os certificados emitidos no "ramo" da hierarquia de confiança da AC Raiz MZ.

5.7.4 Capacidade de Continuidade da Actividade em Caso de Desastre

O INTIC dispõe dos recursos de computação, software, cópias de segurança e registos, necessários para restabelecer ou recuperar operações essenciais (emissão e revogação de certificados, com a publicação de informação de revogação) após um desastre natural ou outro. Estes recursos estão armazenados em ambientes externos ao centro de dados.

5.8 Procedimentos em Caso de Extinção de AC ou AR

Em caso de cessação de actividade como prestador de serviços de Certificação, a AC Raiz MZ deve, com uma antecedência mínima de 3 (três) meses, proceder às seguintes acções:

a) Informar os titulares de certificados em vigor;

b) Informar os titulares qual a entidade para a qual transmite a sua documentação,

c) Revogar todos os certificados emitidos, colocando a sua documentação à guarda da INTIC;

d) Efectuar uma notificação final aos titulares 2 (dois) dias antes da cessação formal da actividade;

e) Garantir a transferência (para retenção por outra organização) de toda a informação relativa à actividade da AC, nomeadamente, chave da AC, certificados, documentação em arquivos (interno ou externo), repositórios e arquivos de registo de eventos.

Em caso de alterações do organismo/estrutura responsável de gestão da actividade da AC, esta deve informar de tal facto às entidades listadas nas alíneas anteriores.

6 Controles Técnicos de Segurança

6.1 Geração e instalação do par de chaves

A geração do par de chaves da AC Raiz é processada de acordo com os requisitos e algoritmos definidos neste documento.

6.1.1 Geração do par de chaves

A AC Raiz utiliza um componente seguro de Hardware (HSM), para a geração do seu par de chaves criptográficas, sendo ele gerado pela própria AC Raiz.

A geração das chaves criptográficas da AC Raiz é efectuada pelos membros dos Grupos de Trabalho, numa intervenção planeada e auditada de acordo com procedimentos das operações a realizar. Todas as operações realizadas são registadas, datadas e assinadas pelos elementos envolvidos nos Grupos de Trabalho.

Relativamente ao par de chaves das ACs de segundo nível, ou seja as AC de nível imediatamente subsequente ao da AC Raiz, é gerado pela própria requerente, após a aprovação do seu pedido de credenciação e consequente autorização de funcionamento no âmbito do SCDM.

6.1.2 Entrega da chave privada ao titular

No âmbito do SCDM, esta actividade não se aplica.

6.1.3 Entrega da chave pública ao emissor do certificado

Sendo o certificado da AC Raiz auto-assinado não se aplica esta acção. Relativamente à chave pública das ACs de segundo e terceiro níveis, a entrega é efectuada de acordo com os procedimentos indicados na Secção 4.3.1.

6.1.4 Entrega da chave pública das ACs às partes confiantes

A chave pública da AC Raiz é disponibilizada através do seu certificado, conforme Secção 4.4.2.

6.1.5 Dimensão das chaves

O tamanho das chaves criptográficas assimétricas das ACs a integrar a hierarquia de confiança do SCDM encontra-se na Secção 6.3.2.

6.1.6 Parâmetros da chave pública e verificação da qualidade

A geração dos parâmetros da chave pública e verificação da qualidade dos mesmos, tem por base a norma que define o algoritmo. A geração das chaves das Autoridades Certificadoras é baseada em processos descritos no ANSI X9.17 (Anexo C), de acordo com o estipulado no PKCS#1.

6.1.7 Fins a que se destinam as chaves (campo "key usage" x.509 v3)

Descrito na Secção 4.5.1.

6.2 Protecção da chave privada e características do módulo criptográfico

6.2.1 Normas e Medidas de Segurança do Módulo Criptográfico

O módulo criptográfico utilizado para a geração, armazenamento e manutenção das chaves da AC Raiz, cumpre os requisitos FIPS 140-2 nível 3, permitindo a geração, manutenção, armazenamento e todas as operações que envolvem chaves criptográficas utilizando exclusivamente o hardware.

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

A chave privada da AC Raiz tem controlo multi-pessoal. Estão implementados mecanismos e técnicas que obrigam à participação de vários membros do Grupo de Trabalho para a execução de operações criptográficas sensíveis.

Para além dos controlos de acesso necessários para entrar na sala segura onde se encontra a chave privada da AC Raiz, estão implementados outros controlos no que diz respeito ao seu acesso e activação. São necessários pelo menos 3 indivíduos para permitir a utilização da chave privada da AC Raiz, sendo que os dados de activação da chave privada são compostos por 2 componentes, código de activação e chaves criptográficas de autenticação (M de N). O código de activação está à responsabilidade de um dos 3 elementos e, relativamente às chaves

de autenticação, estas estão divididas em partes, sendo necessárias duas (m) partes de um total de n.

6.2.3 Retenção e recuperação de chaves (key escrow)

A AC Raiz só efectua a retenção da sua chave privada.

6.2.4 Cópia de segurança da chave privada

É realizada cópia de segurança da chave privada da AC Raiz utilizando uma ligação directa entre os dois HSM's, o de produção e o de Backup. A geração da cópia de segurança é o último passo da emissão de um novo par de chaves da AC Raiz. A cópia de segurança é efectada de e para um HSM, com autenticação de dois fatores em que vários indivíduos, detentores de chaves criptográficas de autenticação, autenticam-se antes que seja possível efectuar a cópia de segurança. A HSM Backup contendo a cópia de segurança da chave privada da AC Raiz é colocado num cofre seguro em instalações seguras secundárias, e acessível apenas aos membros autorizados dos Grupos de Trabalho. O controlo de acesso físico a essas instalações impede a outras pessoas de obterem acesso não autorizado às chaves privadas.

6.2.5 Arquivo da chave privada

A chave privada não é arquivada. Quando expirado o certificado da AC Raiz, é eliminada a chave privada do HSM e de todas as cópias de segurança que possam existir.

6.2.6 Transferência da chave privada para outro módulo criptográfico

A chave privada da AC Raiz é gerada no HSM especificado na Secção 6.2.1. Apenas haverá transferência, em modo cifrado para um HSM de Backup ou directamente para um novo HSM, tal como indicado na Secção 6.2.4.

6.2.7 Armazenamento da chave privada no módulo criptográfico

A chave privada da AC Raiz é armazenada num HSM, após a sua geração é efectada pelos membros dos Grupos de Trabalho, numa intervenção planeada e auditada de acordo com procedimentos das operações a realizar. Todas as operações realizadas são registadas, datadas e assinadas pelos elementos envolvidos nos Grupos de Trabalho.

Estando o HSM numa área restrita com acesso controlado, e apenas concedido a membros dos grupos de trabalho devidamente autorizados, o acesso e activação da chave privada será obtido como descrito na Secção 6.2.2.

6.2.8 Método de activação da chave privada

Os sistemas da AC Raiz estão desligados, sendo considerada, por isso, uma AC offline. Neste contexto, a sua chave privada deve ser activada quando o sistema é ligado através da autenticação no HSM por elementos dos grupos de trabalho, sendo obrigatória a utilização de autenticação de pelo menos dois factores (consola de autenticação portátil e chaves de activação com código PIN associado), descrito na Secção 6.2.2.

Pode-se obter mais informação sobre dados de activação, na Secção 6.4.

6.2.9 Método de desativação da chave privada

A chave privada da AC Raiz é desativada sempre que concluída a necessidade da sua utilização, sendo que para a sua desativação é necessária, no mínimo, a intervenção de 2 elementos do Grupo de Trabalho. Uma vez desativada, esta permanecerá inativa até que o processo de activação seja executado.

6.2.10 Método de destruição da chave privada

As chaves privadas da AC Raiz (incluindo as cópias de segurança) são destruídas num procedimento devidamente identificado e auditado assim que concluída a sua data de validade (ou se revogadas antes deste período). Neste processo são utilizadas funções de formatação disponibilizadas pelo hardware criptográfico ou outros meios apropriados para a sua destruição, de forma a garantir que não restarão resíduos que permitam a sua recuperação/reconstrução.

6.2.11 Avaliação do módulo criptográfico

Descrito na Secção 6.2.1.

6.3 Outros aspetos da gestão do par de chaves

6.3.1 Arquivo da chave pública

A chave pública da AC Raiz é alvo de cópia de segurança efectada pelos membros dos Grupos de Trabalho ficando armazenada após a expiração do certificado correspondente, para verificação de assinaturas geradas durante o seu prazo de validade.

6.3.2 Períodos de validade do certificado e das chaves

A validade do certificado determina o período de utilização das chaves privadas, pelo que após a expiração dos certificados, as chaves privadas respectivas 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 emitidos pela AC Raiz e o seu período de renovação, é mostrado na Tabela 5.

Tabela 5: Tamanho de Chaves e Período de Validade de Certificados

Certificado	Tamanho mínimo da Chave [Bits RSA]	Validade Máxima [anos]
AC Raiz	4096	30
AC Segundo Nível	2048	30
AC Terceiro Nível	2048	30
OCSP responder	2048	5

6.4 Dados de activação

6.4.1 Geração e instalação dos dados de activação

Os dados de activação necessários para a utilização da chave privada da AC Raiz são divididos em várias partes (guardadas em chaves de activação), ficando à responsabilidade de diferentes membros do Grupo de Trabalho. As diferentes partes são geradas de acordo com o definido no processo/cerimónia de geração de chaves e obedecem aos requisitos definidos pela norma FIPS 140-2, nível 3 [18].

6.4.2 Protecção dos dados de activação

Os dados de activação (em partes separadas e/ou palavra-passe) são memorizados e/ou guardados em tokens que evidenciem tentativas de violação e/ou guardados em envelopes

que são guardados em cofres seguros.

As chaves privadas são armazenadas de forma cifrada, em hardware criptográfico.

6.4.3 Outros aspectos dos dados de activação

Em caso de necessidade de transmissão de dados de activação das chaves privadas, esta será efectuada de forma segura garantindo que não serão perdidos, roubados, alterados nem divulgados os dados.

6.5 Medidas de segurança informática

6.5.1 Requisitos técnicos específicos

A geração do par de chaves da AC Raiz e a emissão dos certificados das ACs de segundo nível são actividades realizadas num ambiente offline, para impedir o acesso remoto não autorizado.

As informações utilizadas nesses procedimentos são mantidas no ambiente offline, com acesso restrito.

O servidor da AC Raiz, directamente relacionado com a emissão, expedição, distribuição, revogação e gestão dos certificados tem as seguintes características:

- Controle de acessos;
- Separação das tarefas e atribuições relacionadas a cada perfil da AC Raiz;
- Geração e armazenamento de registos de auditoria;
- Mecanismos internos de segurança para garantia da integridade de dados e processos críticos e,
- Mecanismos para cópias de segurança (backup).

Essas características são implementadas pelo sistema operativo ou por meio da combinação deste com o software de gestão do ciclo de vida dos certificados e mecanismos de segurança física.

O acesso ao servidor é restrito aos membros dos Grupos de Trabalho com uma razão válida para esse acesso. Sendo offline, é desligado no fim de cada emissão de certificado ou de qualquer outra intervenção técnica necessária e que cumpra os requisitos necessários para identificação, autenticação, controlo de acessos, administração, auditorias, reutilização, responsabilidade e recuperação de serviços e troca de informação.

6.5.2 Avaliação/nível de segurança

Os vários sistemas e produtos utilizados pela AC Raiz são fiáveis e protegidos contra modificações.

O módulo criptográfico em Hardware onde se encontra a chave privada a AC Raiz satisfaz tem certificação de segurança FIPS 140-2, nível 3.

6.6 Ciclo de vida das medidas técnicas de segurança

6.6.1 Medidas de desenvolvimento do sistema

Os requisitos de segurança são tidos em conta para aquisição de sistemas. As aplicações são desenvolvidas e implementadas por terceiros de acordo com as suas regras de desenvolvimento de sistemas e de gestão de mudanças.

É fornecida metodologia auditável que permite verificar que o software da AC Raiz não foi alterado antes da sua primeira utilização. Toda a configuração e alterações do software são executadas e auditadas por membros do Grupo de Trabalho.

6.6.2 Medidas para a gestão da segurança

Existem mecanismos e/ou Grupos de Trabalho, para controlar e monitorizar a configuração dos sistemas da AC Raiz. O sistema, quando utilizado pela primeira vez, é verificado para garantir que o software utilizado é fidedigno e legal e que não foi alterado depois da sua instalação.

6.6.3 Ciclo de vida das medidas de segurança

As operações de instalação, actualização e manutenção dos produtos e sistemas são realizadas de acordo com as recomendações dos respectivos fabricantes e seguindo os procedimentos definidos. São executadas por membros do Grupo de Trabalho, com adequada formação para o efeito. Em casos excepcionais, por questões técnicas, poderão ser estas operações realizadas por terceiros, sendo que deverão ser previamente autorizados pelo GG da AC Raiz.

6.7 Medidas de segurança da rede

A AC Raiz não se encontra ligada a qualquer rede.

6.8 Validação cronológica (time-stamping)

Certificados, LCRs e outras entradas na base de dados contêm sempre informação sobre a data e hora dessas entradas, determinadas através de fonte de tempo segura. Tal informação não é baseada em mecanismos criptográficos.

7 Perfis dos Certificados, LCR e OCSP

7.1 Perfil dos Certificados

O formato de todos os certificados emitidos pela AC Raiz MZ está em conformidade com a RFC 5280 [5].

O conteúdo de todos os certificados emitidos no âmbito do SCDM, incluídos auqles não explicitamente listados neste documento, estão em conformidade com o padrão ITU X.509 [19] ou ISO/IEC 9594-8 [20]. Nesta secção são apresentados os perfis de certificados no âmbito do Sistema de Certificação Digital de Moçambique.

Tabela 6: Perfil dos Certificados da AC Raiz MZ.

Campo ou Extensão	**Valor**
Número Serial	Deve ser único, com 64 bits, gerado por um gerador de número pseudo-aleatório criptograficamente seguro (CSPRNG).
Nome distinto do Emissor	AC Raiz MZ v<n>, onde n é um número que representa uma instância do certificado da AC Raiz. For exemplo, AC Raiz MZ v1, AC Raiz MZ v2, etc.
Nome distinto do Sujeito	Idem ao Nome distindo do Emissor.
Período de Validade	Até 30 anos.
Restrições Básicas	Crítico. cA=True, pathLengh constraint absent,
Uso da Chave	Crítico. keyCertSign, cRLSign.

Tabela 7: Perfil dos Certificados da AC de Políticas.

Campo ou Extensão	**Valor**
Número Serial	Deve ser único, com 64 bits, gerado por um gerador de número pseudo-aleatório criptograficamente seguro (CSPRNG).
Nome distinto do Emissor	Derivado do Certificado da AC Emissora.
Nome distinto do Sujeito	C=MZ, O=INTIC, CN=AC Politicas v<n>, onde n é um número que representa uma instância do certificado da AC de Políticas.
Período de Validade	Até 30 anos.
Restrições Básicas	Crítico. cA=True, pathLengh constraint 0,
Uso da Chave	Crítico. keyCertSign, cRLSign, digitalSignature.
Extended Key Usage	A ser definido
Certificate Policies	Policy Qualifier Id=DPC, Qualifier: URL para esta DPC
Authority Information Access	Contém a URL da AC Emissora.
CRL Distribution Points	Contém a URL da LCR.

Tabela 8: Perfil dos Certificados da AC CertAU.

Campo ou Extensão	Valor
Número Serial	Deve ser único, com 64 bits, gerado por um gerador de número pseudo-aleatório criptograficamente seguro (CS-PRNG).
Nome distinto do Emissor	Derivado do Certificado da AC Emissora.
Nome distinto do Sujeito	C=MZ, O=INTIC, CN=AC CertAU v<n>, onde n é um número que representa uma instância do certificado da AC de Certificados de Assinatura Única.
Período de Validade	Até 30 anos.
Restrições Básicas	Crítico. cA=True, pathLengh constraint 0,
Uso da Chave	Crítico. keyCertSign, cRLSign, digitalSignature.
Extended Key Usage	A ser definido.
Certificate Policies	Policy Qualifier Id=DPC, Qualifier: URL para esta DPC
Authority Information Access	Contém a URL da AC Emissora.
CRL Distribution Points	Contém a URL da LCR.

7.1.1 Versão

Todos os certificados emitidos pela AC deverão implementar a versão 3 de certificado definida no padrão X.509, de acordo com o perfil estabelecido na RFC 5280 [5].

7.1.2 Extensões

Conforme Secção 7.1.

7.1.3 Identificadores de objecto dos algoritmos

As informações referentes aos identificadores de objecto dos algoritmos podem ser encontradas na respectivas normas internacionais.

7.1.4 Formatos dos nomes

Conforme Secção 7.1.

Tabela 9: Perfil dos Certificados da AC de Segundo Nível.

Campo ou Extensão	Valor
Número Serial	Deve ser único, com 64 bits, gerado por um gerador de número pseudo-aleatório criptograficamente seguro (CS-PRNG).
Nome distinto do Emissor	Derivado do Certificado da AC Emissora.
Nome distinto do Sujeito	Nome da AC de Segundo Nível.
Período de Validade	Até 30 anos.
Restrições Básicas	Crítico. cA=True, pathLengh constraint 0,
Uso da Chave	Crítico. keyCertSign, cRLSign, digitalSignature.
Extended Key Usage	A ser definido
Certificate Policies	Policy Qualifier Id=DPC, Qualifier: URL para esta DPC
Authority Information Access	Contém a URL da AC Emissora.
CRL Distribution Points	Contém a URL da LCR.

Tabela 10: Perfil dos Certificados da AC de Terceiro Nível.

Campo ou Extensão	Valor
Número Serial	Deve ser único, com 64 bits, gerado por um gerador de número pseudo-aleatório criptograficamente seguro (CS-PRNG).
Nome distinto do Emissor	Derivado do Certificado da AC Emissora.
Nome distinto do Sujeito	Nome da AC de Terceiro Nível.
Período de Validade	Até 30 anos.
Restrições Básicas	Crítico. cA=True, pathLengh constraint 0,
Uso da Chave	Crítico. keyCertSign, cRLSign, digitalSignature.
Extended Key Usage	A ser definido
Certificate Policies	Policy Qualifier Id=DPC, Qualifier: URL para esta DPC
Authority Information Access	Contém a URL da AC Emissora.
CRL Distribution Points	Contém a URL da LCR.

7.1.5 Restrições para nomes

A AC Raiz do Sistema de Certificação Digital de Moçambique estabelece as seguintes restrições para os nomes, aplicáveis a todos os certificados: não deverão ser utilizados sinais de acentuação, tremas ou cedilhas.

Além dos caracteres alfanuméricos, poderão ser utilizados os símbolos especiais listados na Tabela 11.

Tabela 11: Símbolos admitidos em nomes.

Símbolo	Descrição	Código NBR9611 (hexadecimal)
	espaço em branco	0x20
!	ponto de exclamação	0x21
#	Cerquilha	0x23
$	Dólar	0x24
%	Percentual	0x25
&	e comercial	0x26
(	abre parênteses	0x28
)	fecha parênteses	0x29
*	Asterisco	0x2A
+	Mais	0x2B
,	Vírgula	0x2C
-	Menos	0x2D
.	Ponto	0x2E
/	Barra	0x2F
:	Dois pontos	0x3A
;	ponto e vírgula	0x3B
=	Igual	0x3D
?	ponto de interrogação	0x3F
@	Arroba	0x40
\	Barra invertida	0x5C

7.1.6 Identificador de objecto da PC

O OID da Política de Certificado/Declaração de Práticas de Certificação (PC/DPC) da AC Raiz da Instituto Nacional de Tecnologias da Informação e Comunicação é 2.16.508.1.1.1 [1].

7.1.7 Uso da extensão Policy Constraints

Não estipulado.

7.1.8 Sintaxe e semântica dos qualificadores de política

O ponteiro para a DPC contém uma URL para um documento em formato PDF disponível via protocolo HTTPS [21].

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

Não estipulado.

7.2 Perfil da LCR

O formato da LCR emitida pela AC Raiz está em conformidade com a RFC 5280 [5] conforme é descrito na Tabela 12.

Tabela 12: Campos da LCR da AC Raiz

Campo	Conteúdo
Version	V2
Signature algorithm	A LCR é assinada com os mesmos algoritmos criptográficos usados pela AC Raiz.
Issuer	DN conforme a Tabela 6.
ThisUpdate	Data da emissão da LCR.
NextUpdate	Data da emissão da próxima LCR. O prazo de validade da AC Raiz depende da árvore de certificados subordinada.
RevokedCertificates	Número de série e data de revogação de todos os certificados revogados que ainda não expiraram.

7.2.1 Versão

Todas as LCRs emitidas pela AC Raiz deverão seguir a versão 2 de listas de certificados revogados de acordo com a RFC 5280 [5].

7.2.2 Extensões da LCR e de entradas da LCR

Não estipulada.

7.3 Perfil do OCSP

A AC Raiz não irá prover o serviço OCSP.

7.3.1 Versão

Não se aplica.

7.3.2 Extensões do OCSP

Não se aplica.

8 Auditorias de Conformidade

Serão realizadas, pelo Grupo de Trabalho de Auditoria de Sistemas, inspecções regulares de conformidade ao descrito neste documento e a outras regras, procedimentos, cerimónias e processos.

Para além das auditorias de conformidade, por determinação do CG, poderão ser realizadas outras fiscalizações e investigações para assegurar a conformidade da AC Raiz MZ com a legislação nacional e normas aplicáveis. A execução destas auditorias, fiscalizações e investigações poderá ser delegada a uma entidade externa de auditoria, identificada na bolsa de Auditores da Autoridade Credenciadora, sem aviso prévio.

8.1 Frequência ou Motivo da Auditoria

As auditorias de conformidade são realizadas anualmente de acordo com a legislação em vigor [3], sendo que o Relatório de Auditoria de Segurança é entregue até 31 de Março.

A AC Raiz MZ deverá provar, com a auditoria e relatório de segurança anuais (produzidos pelo auditor de segurança acreditado), que a avaliação dos riscos foi assegurada, tendo sido identificadas e implementadas todas as medidas necessárias para a segurança de informação.

8.2 Identidade e Qualificações do Auditor

O auditor é uma pessoa ou organização, devidamente credenciado pela Autoridade Credenciadora, reconhecido como idóneo, com experiência e qualificações comprovadas na área da segurança da informação e dos sistemas de informação, infraestruturas de chave pública, familiarizado com as aplicações e programas de certificação digital e na execução de auditorias de segurança.

Deverá ser seleccionado pela Autoridade Certificadora para a realização da auditoria, de entre os disponibilizados na Bolsa de Auditores da Autoridade Credenciadora, devendo ter independência a nível orgânico da AC Raiz MZ (para os casos de auditorias externas).

8.3 Relação entre o Auditor e a AC

Será tida em conta a necessidade de independência entre o auditor e membros da sua equipa para que, no exercício da sua função, actue de forma imparcial em relação à entidade que é submetida à auditoria. Garante-se que:

i. O auditor de segurança (ou qualquer elemento da equipa de auditoria) não executa funções parciais ou discriminatórias ligadas à AC;

ii. O auditor de segurança (ou qualquer elemento da equipa de auditoria) não tem nem teve, nos últimos três anos qualquer relação contratual com a AC, fora do âmbito de auditoria externa;

iii. O auditor de segurança (ou qualquer elemento da equipa de auditoria) não tem nenhuma relação, actual ou prevista, financeira, legal ou de qualquer outro género que possa originar um conflito de interesses;

iv. O cumprimento do estabelecido na legislação em vigor sobre a protecção de dados pessoais é tido em conta por parte do auditor, na medida em que este poderá aceder a dados pessoais constantes dos ficheiros dos membros dos diversos grupos de trabalho afectos à AC, assim como aos dados fornecidos no pedido de emissão de um certificado para Autoridades Certificadoras do Estado.

8.4 Âmbito da Auditoria

O âmbito das auditorias e outras avaliações inclui a conformidade com a legislação nacional, Políticas emitidas pela Autoridade Credenciadora, CG, com este documento e outras regras, procedimentos e processos (especialmente os relacionados com operações de gestão de chaves, recursos, controlos de gestão e operação e, gestão de ciclo de vida de certificados).

8.5 Procedimentos após uma Auditoria com Resultado Deficiente

Se numa auditoria resultarem irregularidades e não-conformidades:

a) A entidade auditada deve estipular prazos para cumprir as irregularidades ou não-conformidades detectadas;

b) Devem ser dadas a conhecer à Autoridade Credenciadora para servirem de referência a futuras fiscalizações.

9 Outras situações e Assuntos Legais

9.1 Taxas

Nada a assinalar.

9.2 Responsabilidade Financeira

Nada a assinalar.

9.3 Confidencialidade

9.3.1 Âmbito

É considerada informação confidencial, aquela que não pode ser divulgada a terceiros, nomeadamente:

i. As chaves privadas;

ii. Informação relativa aos parâmetros de segurança, controlo e procedimentos de auditoria;

iii. Informação de carácter pessoal, salvo se houver autorização explícita para a sua divulgação;

iv. Planos de continuidade de negócio e recuperação;

v. Registos de transacções, incluindo os registos completos de auditoria;

vi. Todos os documentos relacionados com a AC Raiz MZ (regras, políticas, cerimónias, formulários e processos), incluindo conceitos organizacionais, que constituem informação financeira/comercial secreta, confidencial e/ou privilegiada, sendo propriedade do INTIC. Apenas poderão ser disponibilizados, a terceiros, com autorização prévia e explícita do INTIC;

vii. Todos os elementos de segurança física e lógica (pins, passwords, cartões de acesso, entre outros), relacionados com a operação da AC Raiz MZ;

viii. A localização dos ambientes da AC Raiz MZ e seu conteúdo.

9.3.2 Informação Confidencial

Considera-se informação não sigilosa:

i. Certificados;

ii. Lista de Certificados Revogados;

iii. Informações corporativas ou pessoais que necessariamente façam parte deles ou do domínio público;

iv. Políticas de Certificados;

v. Declaração de Práticas de Certificação;

vi. Toda a informação classificada como "pública" (informação não expressamente considerada como "pública" será considerada confidencial).

9.3.3 Responsabilidade de Proteção da Confidencialidade da Informação

Os elementos dos Grupos de Trabalho ou outras entidades que recebam informação confidencial são responsáveis por assegurar que esta não é copiada, reproduzida, armazenada, traduzida ou transmitida a terceiras partes por quaisquer meios sem antes terem o consentimento explícito do INTIC.

Nenhum documento, informação ou registo, identificado como confidencial, que esteja sob a guarda da AC Raiz MZ deve ser fornecido a terceiros excepto se houver autorização explícita do CG.

9.4 Privacidade de Dados Pessoais

9.4.1 Medidas para Garantia da Privacidade

A AC Raiz MZ não emite certificados para pessoas singulares. No entanto, terá nos pedidos de certificados para AC Raiz MZdados dos representantes legais destas Entidades, sendo que apenas serão utilizados para este fim e serão armazenados em ambiente seguro com acesso restrito aos elementos dos grupos de trabalho da AC Raiz MZ.

O titular de um certificado e/ou o seu representante legal terão amplo acesso a quaisquer dos seus próprios dados e identificações, podendo autorizar formalmente a divulgação de seus registos a outras pessoas. As autorizações formais podem ser apresentadas de duas formas:

a) Por meio electrónico, contendo assinatura válida, garantida por certificado reconhecido pelo Sistema de Certificação Digital de Moçambique (SCDM); ou

b) Por meio de pedido escrito com assinatura manuscrita reconhecida.

Nenhuma liberação de informação é permitida sem autorização formal.

9.4.2 Informação Privada

Toda e qualquer informação fornecida no acto do pedido de certificado, que não esteja divulgada no certificado, é considerada privada.

9.4.3 Informação não Protegida pela Privacidade

É considerada informação não protegida pela privacidade, toda a informação fornecida no acto do pedido de certificado que seja disponibilizada no certificado.

9.4.4 Responsabilidade de Protecção de Informação Privada

Todos os dados inerentes ao pedido de certificado, são armazenados em ambiente seguro e apenas acedidos pelos elementos dos grupos de trabalho.

9.4.5 Comunicação e Consentimento para Utilização da Informação Privada

A informação apenas é utilizada no âmbito da emissão do certificado.

9.4.6 Divulgação Resultante de Processo Judicial ou Administrativo

Mediante ordem judicial, serão fornecidos quaisquer documentos, informações ou registos sob a guarda da AC Raiz MZ.

9.4.7 Outras Circunstâncias para Revelação de Informação

Nada a assinalar.

9.5 Direitos de Propriedade Intelectual

Todos os direitos de propriedade intelectual, incluindo os que se referem a certificados e LCR emitidos, OID e DPC bem como qualquer outro documento, propriedade da AC Raiz MZ pertencem ao INTIC.

9.6 Representação e Garantias

9.6.1 Representação e Garantias da AC Raiz MZ

A AC Raiz MZ está obrigada a:

1) Realizar as suas operações de acordo com este documento e demais normativos aplicáveis;
2) Declarar de forma clara todas as suas Práticas de Certificação no documento apropriado;
3) Assegurar que as demais entidades envolvidas têm conhecimento dos seus direitos e obrigações;
4) Gerir e proteger todos seus activos de forma segura;
5) Emitir certificados de acordo com o standard X.509;
6) Emitir certificados que estejam conformes com a informação conhecida no momento da sua emissão e livres de erros de entrada de dados;
7) Emitir certificados para Autoridades Certificadoras do Estado;
8) Notificar os subscritores dos seus certificados assim que se verificar:
    i. A suspeita de comprometimento da sua chave;
    ii. A emissão de um novo par de chaves e do certificado correspondente;
    iii. A Alteração do estado do seu certificado, indicando o motivo que originou esta acção;
    iv. Cessação de actividade;
    v. Utilizar sistemas, assim como produtos fiáveis, que cumpram os seguintes requisitos:
    vi. Se encontrem protegidos contra toda e qualquer alteração não autorizada
    vii. Garantam a segurança técnica e criptográfica dos processos de certificação;
    viii. Garantam o armazenamento de certificados reconhecidos que permitam comprovar a sua autenticidade e impedindo a alteração de dados;
9) Arquivar sem alteração os certificados emitidos;

10) Garantir que pode ser determinada com precisão a data e hora em que se emitiu, revogou ou suspendeu um certificado;

11) Revogar os certificados nos termos da Secção 4.9 deste documento e publicar os certificados revogados na LCR do repositório, com a frequência estipulada na Secção 4.9.11;

12) Publicar este documento no seu repositório garantindo o acesso às versões atuais assim como as versões anteriores;

13) Identificar e registar todas as acções executadas, conforme as normas, práticas e regras estabelecidas pela Autoridade Credenciadora;

14) Manter a conformidade dos seus processos, procedimentos e actividades com as normas, práticas e regras do CG e com a legislação em vigor;

15) Colaborar com as auditorias dirigidas pela Autoridade Credenciadora, para validar a renovação das suas próprias chaves;

16) Operar de acordo com a legislação aplicável;

17) Proteger, em caso de existirem, as chaves que estejam sobre sua custódia;

18) Garantir a disponibilidade da LCR;

19) Em caso de cessar a sua actividade, comunicar o facto com uma antecedência mínima de três meses a todos os responsáveis dos certificados emitidos para Autoridades Certificadoras Subordinadas;

20) Cumprir com a legislação em vigor sobre Protecção de Dados Pessoais;

21) Conservar toda a informação e documentação relativa a um certificado reconhecido e as Declarações de Práticas de Certificação vigentes em cada momento o estipulado na Secção 5.4.3.

9.6.2 Representação e Garantias das Autoridades de Registo

A AC Raiz MZ não é detentora de Autoridade de Registo, ela própria efectua a validação dos pedidos de Entidades do Estado que pretendam integrar a sua hierarquia de confiança.

9.6.3 Representação e Garantias dos Titulares de Certificados

É obrigação dos titulares dos certificados emitidos:

a) Tomar conhecimento dos direitos e obrigações, contemplados neste documento e outros documentos aplicáveis da AC Raiz MZ;

b) Limitar e adequar a utilização dos certificados de acordo com as utilizações previstas nas Políticas de Certificado;

c) Tomar todos os cuidados e medidas necessárias para garantir a posse exclusiva da sua chave privada;

d) Solicitar de imediato a revogação de um certificado em caso de ter conhecimento ou suspeita de compromisso da chave privada correspondente à chave pública contida no certificado, de acordo com a Secção 4.9;

e) Não utilizar um certificado digital que tenha perdido a sua eficácia, quer por ter sido revogado, suspenso ou por ter expirado o período de validade;

f) Fornecer de modo completo e preciso todas as informações necessárias para a sua identificação. Devem informar a AC Raiz MZ de qualquer modificação desta informação e,

g) Não monitorizar, manipular ou efectuar acções de "engenharia inversa" sobre a implantação técnica (hardware e software) dos serviços de certificação, sem a devida autorização prévia, por escrito, da AC Raiz MZ.

9.6.4 Representação e Garantias das Partes Confiantes

É obrigação das partes que confiam nos certificados emitidos pela AC Raiz MZ:

a) Limitar a fiabilidade dos certificados às utilizações permitidas para os mesmos em conformidade com o expresso no presente documento;

b) Verificar a validade dos certificados no momento de realizar qualquer operação baseada nos mesmos;

c) Assumir a responsabilidade na comprovação da validade, revogação ou suspensão dos certificados em que confia;

d) Ter pleno conhecimento das garantias e responsabilidades aplicáveis na aceitação e uso de certificados em que confia e aceitar sujeitar-se às mesmas;

e) Notificar qualquer acontecimento ou situação anómala relativa ao certificado, que possa ser considerado como causa de revogação do mesmo, utilizando os meios que a AC Raiz MZ publique no seu sítio Web.

9.7 Renúncia de Garantias

A AC Raiz MZ recusa todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas neste documento.

9.8 Limitações de Responsabilidade

De acordo com a legislação em vigor.

9.9 Idemnizações

De acordo com a legislação em vigor

9.10 Termo e Cessação

Em caso de decisão de términos de actividade são identificadas neste documento algumas acções a serem executadas.

9.10.1 Notificação de Cessação de Actividade

A primeira acção será a de Notificação, que pretende dar conhecimento a todas as entidades, singulares ou coletivas, que de alguma forma intervêm na actividade. Desta forma o INTIC deverá informar de forma imediata:

i. Autoridade Credenciadora;

ii. CG do SCDM;

iii. Autoridades Certificadoras para quem tenham sido emitidos certificados e que ainda se encontrem válidos, à data da decisão de cessação de actividade.

A notificação inclui, no mínimo, a seguinte informação:

i. Autoridade Credenciadora e CG do SCDM:

ii. Comunicação para efeitos de cancelamento das credenciações de segurança;

iii. Autoridades Certificadoras na hierarquia da AC Raiz MZ:

iv. Informar as ACs de que os seus certificados, emitidos no âmbito do SCDM, irão ser revogados, deixando por isso de ser válidos para utilização.

9.10.2 Cessação de Relações Contratuais

Serão cessadas as relações contratuais com todas as entidades terceiras que, de alguma forma, intervenham nas actividades inerentes à AC Raiz MZ.

9.10.3 Revogação dos Certificados

Todos os certificados emitidos no âmbito do SCDM, serão revogados. Assim, as actividades serão as seguintes:

1. Revogação de todos os certificados emitidos pela AC Raiz MZ, subsequentes ACs, restantes certificados, que ainda se encontrem válidos;
2. Emissão e disponibilização pública da LCR da AC Raiz MZ, sendo que as restantes ACs de níveis subsequentes deverão efectuar o mesmo procedimento;
3. Destruição das Chaves Privadas da AC Raiz MZ, sendo que as restantes ACs de níveis subsequentes deverão efectuar o mesmo procedimento;
4. Garantir a transferência e manutenção para retenção por outra organização (se for o caso) de toda a informação relativa à actividade da AC Raiz MZ, nomeadamente, documentação em arquivos (interno ou externo), repositórios e arquivos de registo de eventos, durante o período de tempo legalmente exigido.

Todas as Listas de Certificados Revogados serão mantidas acessíveis publicamente no repositório da AC Raiz MZ, até à expiração do último certificado emitido.

9.11 Notificação Individual e Comunicação aos Participantes

Todos os participantes devem utilizar métodos razoáveis para comunicação. Esses métodos podem incluir correio electrónico assinado digitalmente, fax, formulários assinados, ou outros, dependendo da criticidade e assunto da comunicação.

As comunicações inerentes à cessação de actividade deverão ser executadas, também, na página institucional da AC Raiz MZ, sendo que as ACs subsequentes também deverão comunicar na página institucional as acções inerentes a esta situação.

9.12 Alterações

Os documentos relacionados com a AC Raiz MZ (incluindo este documento) tornam-se efectivos assim que sejam aprovados pelo Grupo de Gestão (GG) e apenas são eliminados ou

alterados por sua ordem e/ou do CG.

Este documento entra em vigor a partir do momento da sua publicação no repositório da AC Raiz MZ e manter-se-á enquanto não for substituída pela emissão de uma nova versão.

9.12.1 Procedimento para Alterações

No sentido de alterar este documento ou alguma das políticas de certificado, é necessário submeter um pedido formal ao INTIC, utilizando os dados de contacto existentes neste documento. Esse pedido deve conter (pelo menos):

a) A identificação da pessoa que submeteu o pedido de alteração;

b) A razão do pedido;

c) As alterações pedidas.

O INTIC irá rever o pedido e, se verificar a sua pertinência, solicita ao Grupo de Trabalho de Administração de Segurança que efectue as actualizações necessárias ao documento, resultando numa nova versão de rascunho do documento. O novo rascunho do documento é depois disponibilizado a todos os membros do Grupo de Trabalho e às partes afetadas (se alguma) para permitir o seu escrutínio.

Contando a partir da data de disponibilização, as várias partes têm 10 dias úteis para submeter os seus comentários. Quando esse período terminar, o Grupo de Trabalho de Administração de segurança tem mais 15 dias úteis para analisar todos os comentários recebidos e, se relevante, incorporá-los no documento.

O documento é de seguida analisado pelo GG e, se for o caso, aprovado. Depois da sua aprovação, será publicado no repositório público da AC Raiz MZ, tornando-se as alterações finais e efectivas.

9.12.2 Substituição e Revogação deste Documento

O GG pode decidir em favor substituição de um documento relacionado com a AC (incluindo este documento), quando:

a) Os seus conteúdos são considerados incompletos, imprecisos ou erróneos;

b) Os seus conteúdos foram comprometidos.

Neste caso o documento substituído será substituído por uma nova versão.

Após o GG decidir em favor da substituição de um documento relacionado com a AC, o Grupo de Trabalho de Administração de Segurança tem 30 dias úteis para submeter para aprovação pelo GG o(s) documento(s) substituto(s).

As obrigações e restrições que estabelece este documento, em referência a auditorias, informação confidencial, obrigações e responsabilidades da AC, nascidas sob sua vigência, serão substituídas por uma nova versão em tudo o que não se oponha a esta.

Sempre que um documento for considerado, pelo GG, obsoleto, ou seja quando for considerada a sua existência desnecessária, será revogado e, quando este for um documento público, será retirado do repositório público, garantindo-se contudo que será conservado durante o período definido para a retenção de registos.

9.12.3 Prazo e Mecanismo de Notificação

Sempre que as alterações à especificação possam afetar a aceitabilidade dos certificados para propósitos específicos, comunicar-se-á aos utilizadores dos certificados correspondentes que se efectuou uma mudança e que devem consultar a nova versão deste documento no repositório estabelecido.

9.12.4 Motivos para Mudar de OID

O Grupo de Trabalho de Administração de Segurança deve determinar se as alterações a este documento obrigam a uma mudança no OID da política de Certificados ou no URL que aponta para o mesmo.

Nos casos em que, a julgamento do Grupo de Trabalho de Administração de Segurança, as alterações não afetem a aceitação dos certificados proceder-se-á ao aumento do número de versão do documento. Não se considera necessário comunicar este tipo de modificações aos utilizadores dos certificados.

No caso em que o Grupo de Trabalho de Administração de Segurança julgue que as alterações à especificação podem afetar à aceitabilidade dos certificados para propósitos dever-se-á criar novo OID para este documento incrementando o último número atribuído ao documento deste AC (2.16.508.1.1.1+1).

Este tipo de modificação comunicar-se-á aos utilizadores dos certificados.

9.13 Disposições para Resolução de Conflitos

Todas as reclamações entre utilizadores e AC Raiz MZ deverão ser comunicadas pela parte em disputa ao CG, com o fim de tentar resolvê-lo entre as mesmas partes.

Para a resolução de qualquer conflito que possa surgir com relação a este documento, as partes, com renúncia a qualquer outro foro que pudesse corresponder-lhes, submetem-se à Jurisdição de Contencioso Administrativo.

9.14 Legislação Aplicável

É aplicável à actividade das Autoridades Certificadoras, estabelecidas em Moçambique a seguinte legislação específica:

a) Lei das transacções electrónicas no. 03 de 2017 [2];

b) Decreto n0. 59 de 2019, que regulamenta o Sistema de Certificação Digital de Moçambique (SCDM) [3].

9.15 Conformidade com a Legislação em Vigor

Este documento é objecto de aplicação de leis nacionais e directivas internacionais utilizadas como referência, regras, regulamentos, ordenações, decretos e ordens incluindo, mas não limitadas a, restrições na exportação ou importação de software, hardware ou informação técnica.

É responsabilidade do CG zelar pelo cumprimento da legislação aplicável listada na Secção 9.14.

9.16 Providências Várias

9.16.1 Acordo Completo

Todas as partes confiantes assumem na sua totalidade o conteúdo da última versão deste documento.

9.16.2 Independência

No caso em que uma ou mais estipulações deste documento sejam ou tendam a ser inválidas, nulas ou irreclamáveis, em termos jurídicos, deverão ser consideradas como não efectivas.

A situação anterior é valida, apenas e só nos casos em que tais estipulações não sejam consideradas essenciais. É responsabilidade do CG a avaliação da essencialidade das mesmas.

9.16.3 Severidade

Nada a assinalar.

9.16.4 Execuções (Taxas de Advogados e Desistência de Direitos)

Nada a assinalar.

9.16.5 Força Maior

Nada a assinalar.

9.17 Outras Providências

Nada a assinalar.

Referências

[1] INTIC. *Identificadores de Objecto na Infraestrutura de Chaves Públicas de Moçambique*. v1.0. Maputo, MZ, 2022.

[2] MOÇAMBIQUE. *Lei Nº 3, de 9 de Janiero de 2017. Lei de Transações Electrónicas*. Maputo, MZ: [s.n.], 2017. https://www.inage.gov.mz/wp-content/uploads/2018/05/LEI-DE-TRANSACC%C3%95ES-ELECTR%C3%93NICAS.pdf.

[3] MOÇAMBIQUE. *Decreto Nº 59, de 3 de Julho de 2019. Regulamenta o Sistema de Certificação Digital de Moçambique (SCDM)*. Maputo, MZ: [s.n.], 2019. https://gazettes.africa/archive/mz/2019/mz-government-gazette-series-i-dated-2019-07-03-no-127.pdf.

[4] CHOKHANI, S. et al. *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*. IETF, 2003. RFC 3647 (Informational). (Request for Comments, 3647). Disponível em: <http://www.ietf.org/rfc/rfc3647.txt>.

[5] COOPER, D. et al. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. IETF, 2008. RFC 5280 (Proposed Standard). (Request for Comments, 5280). Updated by RFC 6818. Disponível em: <http://www.ietf.org/rfc/rfc5280.txt>.

[6] YEE, P. *Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. IETF, 2013. RFC 6818 (Proposed Standard). (Request for Comments, 6818). Disponível em: <http://www.ietf.org/rfc/rfc6818.txt>.

[7] MELNIKOV, A.; CHUANG, W. *Internationalized Email Addresses in X.509 Certificates*. RFC Editor, 2018. RFC 8398. (Request for Comments, 8398). Disponível em: <https://www.rfc-editor.org/info/rfc8398>.

[8] HOUSLEY, R. *Internationalization Updates to RFC 5280*. RFC Editor, 2018. RFC 8399. (Request for Comments, 8399). Disponível em: <https://www.rfc-editor.org/info/rfc8399>.

[9] ETSI. *Electronic Signatures and Infrastructures (ESI); Trusted Lists*. Sophia-Antipolis Cedex, France, 2016.

[10] ETSI. *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements*. Sophia-Antipolis Cedex, France, 2021.

[11] ETSI. *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates*. Sophia-Antipolis Cedex, France, 2021.

[12] ADAMS, C. et al. *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*. IETF, 2005. RFC 4210 (Proposed Standard). (Request for Comments, 4210). Updated by RFC 6712. Disponível em: <http://www.ietf.org/rfc/rfc4210.txt>.

[13] KAUSE, T.; PEYLO, M. *Internet X.509 Public Key Infrastructure – HTTP Transfer for the Certificate Management Protocol (CMP)*. IETF, 2012. RFC 6712 (Proposed Standard). (Request for Comments, 6712). Disponível em: <http://www.ietf.org/rfc/rfc6712.txt>.

[14] NYSTROM, M.; KALISKI, B. *PKCS #10: Certification Request Syntax Specification Version 1.7*. IETF, 2000. RFC 2986 (Informational). (Request for Comments, 2986). Updated by RFC 5967. Disponível em: <http://www.ietf.org/rfc/rfc2986.txt>.

[15] TURNER, S. *The application/pkcs10 Media Type*. IETF, 2010. RFC 5967 (Informational). (Request for Comments, 5967). Disponível em: <http://www.ietf.org/rfc/rfc5967.txt>.

[16] JOSEFSSON, S.; LEONARD, S. *Textual Encodings of PKIX, PKCS, and CMS Structures*. IETF, 2015. RFC 7468 (Proposed Standard). (Request for Comments, 7468). Disponível em: <http://www.ietf.org/rfc/rfc7468.txt>.

[17] SANTESSON, S. et al. *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*. IETF, 2013. RFC 6960 (Proposed Standard). (Request for Comments, 6960). Disponível em: <http://www.ietf.org/rfc/rfc6960.txt>.

[18] NIST. FIPS 140-2: Security requirements for cryptographic modules. *Information Technology Laboratory, National Institute of Standards and Technology*, 2001.

[19] ITU-T. *The Directory - Overview of Concepts, Models and Service*. Geneva, Switzerland, 1993.

[20] ISO. *X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*. Geneva, Switzerland, 2014.

[21] FIELDING, R.; RESCHKE, J. *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*. IETF, 2014. RFC 7230 (Proposed Standard). (Request for Comments, 7230). Disponível em: <http://www.ietf.org/rfc/rfc7230.txt>.

[22] KENT, S. *Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management*. IETF, 1993. RFC 1422 (Historic). (Request for Comments, 1422). Disponível em: <http://www.ietf.org/rfc/rfc1422.txt>.

Glossário

Aplicativos informáticos Conjunto de ferramentas desenhadas para realizar tarefas e trabalhos específicos no seu computador;

Assinatura digital Modalidade de assinatura electrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento electrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento electrónico foi alterado depois de aposta a assinatura.

Assinatura electrónica Resultado de um processamento electrónico de dados susceptíveis de constituir objecto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento electrónico.

Assinatura Electrónica Avançada Assinatura electrónica que simultaneamente:

i. É capaz de identificar o signatário de forma unívoca;

ii. É criada utilizando meios que o signatário pode manter sob seu controlo exclusivo;

iii. A sua conexão com o documento permite detectar toda e qualquer alteração superveniente do conteúdo deste.

Assinatura Electrónica Qualificada Assinatura digital ou outra modalidade de assinatura electrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura.

Auditor de Segurança Entidade credenciada pela Autoridade Credenciadora, a quem compete verificar a conformidade das actividades das Entidades Certificadoras com os requisitos estabelecidos no presente diploma, elaborando relatórios para instrução dos pedidos de credenciação;

Autoridade Certificadora Entidade que emite certificados digitais.

Autoridade Certificadora Acreditada São todas as autoridades certificadoras devidamente avaliadas e acreditadas pela Autoridade Supervisora e Credenciadora de Moçambique. Os certificados digitais dessas ACs são publicadass no site do SCDM.

Autoridade de Registo Entidade que identifica, autentica e regista os titulares de certificados digitais;

Autoridade Certificadora Raiz do Estado Órgão certificador de topo da cadeia de certificação do SCDM que executa as políticas de certificados e directrizes aprovadas pelo Comité Gestor do SCDM;

Autoridade Supervisora e Credenciadora Entidade competente para a credenciação e fiscalização das Autoridades Certificadoras.

Certificado Estrutura de dados assinado electronicamente por um prestador de serviços de certificação e que vincula ao titular os dados de validação de assinatura que confirma a sua identidade.

Certificado Digital Tecnologia que provê mecanismos de segurança capazes de garantir autenticidade, confidencialidade e integridade às informações e documentos utilizados em transacções electrónicas.

Certificado Qualificado Certificado que cumpre com os requisitos estabelecidos e emitido por provedores de serviços de certificação credenciados, nos termos previsto na Lei de Transacções Electrónicas 03/2017

Chave privada Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento electrónico, ou se decifra um documento electrónico previamente cifrado com a correspondente chave pública.

Chave pública Código utilizado para validar uma assinatura realizada em documentos e transacções electrónicas.

Comité Gestor Órgão responsável pela gestão e administração do SCDM.

Credenciação Ato pelo qual é reconhecido a uma entidade, que o solicitante exerça a actividade de certificação digital.

Criptografia É a disciplina que engloba princípios, meios e métodos para a transformação de dados por forma a esconder o conteúdo da sua informação, estabelecer a sua autenticidade, evitar a sua modificação não detectada, evitar o seu repúdio e /ou evitar a sua utilização não autorizada.

Dados de criação de assinatura electrónica Dados únicos, tais como códigos ou chaves privadas codificadas, que são utilizadas pelo signatário para criar uma assinatura electrónica.

Dados Pessoais Qualquer informação relativa a uma pessoa singular que possa ser identificada directa ou indirectamente através da referência a um número de identificação ou a um ou mais factores específicos à mesma.

Dispositivo de criação de assinatura Suporte lógico ou dispositivo de equipamento utilizado para possibilitar o tratamento dos dados de criação de assinatura.

Dispositivo seguro de criação de assinatura Dispositivo de criação de assinatura que assegure, através de meios técnicos e processuais adequados, que:

i. Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura só possam ocorrer uma única vez e que a confidencialidade desses dados se encontre assegurada;

ii. Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura não possam, com um grau razoável de segurança, ser deduzidos de outros dados e que a assinatura esteja protegida contra falsificações realizadas através das tecnologias disponíveis;

iii. Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura possam ser eficazmente protegidos pelo titular contra a utilização ilegítima por terceiros;

iv. Os dados que careçam de assinatura não sejam modificados e possam ser apresentados ao titular antes do processo de assinatura.

Documento electrónico Conjunto de dados lógicos armazenados em suporte susceptível de poder ser lido por equipamentos electrónicos de processamento.

Endereço electrónico Identificação de um equipamento informático adequado para receber e arquivar documentos electrónicos.

Entidade Certificadora uma entidade que realiza actividades de certificação digital. O mesmo que AC.

Entidade de Registo uma entidade a qual uma Entidade Certificadora delega a actividade de recolha e registo dos dados a incluir em certificados. O mesmo que AR.

Equipamentos periféricos são aparelhos ou placas de expansão que enviam ou recebem informações do computador, tais como: computadores, impressoras, discos, entre outros.

Grupo de Administração de Registo (GAR) Grupo de trabalho responsável pela validação dos pedidos de certificados, aprovação da emissão de certificados digitais e validação dos pedidos de alteração de estado dos certificados digital;

Grupo de Administração de Sistemas (GAS) Responsável por executar as tarefas manutenção do Hardware e Software do SCDM;

Grupo de Administração de Segurança (GASeg) Responsável pela segurança global dos sistemas, nomeadamente a implementação das regras e práticas de segurança definidas para a AC Raiz MZe pelas ACs subordinadas que a integram, assegurando que se encontram atualizadas de forma a garantir que toda a informação indispensável ao funcionamento e auditoria do sistema se encontra disponível ao longo do tempo;

Grupo de Auditoria de Sistemas (GAudS Responsável por efectuar a auditoria interna a todas as acções relevantes e necessárias para assegurar a correcta operacionalização da infraestrutura;

Grupo de Custódia (GC) Responsável por um ambiente denominado de ambiente de custódia, normalmente um cofre, onde estão armazenados activos. Exemplo: chaves de cofres, tokens de autenticação, entre outros.

Grupo de Gestão (CG) Grupo de trabalho responsável pela nomeação de indivíduos para integrar os grupos de trabalho identificados e pela tomada de decisões de nível crítico para a AC Raiz MZ.

Grupo de Operação de Sistemas (GOS) Responsável por executar as tarefas de rotina essenciais ao bom funcionamento e operacionalidade da infraestrutura.

Governo electrónico Uso de tecnologias de informação e comunicação, principalmente a Internet, pelo governo para providenciar informação e serviços ao cidadão.

HSM Um *Hardware Security Module* (HSM) é um equipamento especialmente desenvolvido para a gestão segura do ciclo de vida de chaves criptográficas.

Internet É uma rede internacional de computadores interligados que possibilita o acesso e troca de informação em qualquer lugar do mundo.

LSECMZ A Lista de Serviços Electrónicos Confiáveis de Moçambique (LSECMZ) é uma lista que contém os provedores de serviços electrónicos acreditados pelo Estado de Moçambique. A lista é geralmente codificada em XML, actualizada de forma periódica e publicada no site do SCDMZ. É desejável que todos os sistemas de tecnologia da informação e comunicação e respectivas aplicações dos usuários actualizem, periodicamente, seus repositórios de serviços confiáveis com os dados desta lista.

Meios electrónicos São todos os meios tecnológicos usados para a obtenção de dados no formato analógico ou digital, seu processamento, armazenamento, transmissão bem como a sua apresentação.

Mensagem de dados Informação gerada, enviada, recebida ou armazenada por meios electrónicos, ópticos ou semelhantes, de forma não limitativa, intercâmbio de dados electrónicos (IDE), texto, voz, imagem ou a combinação de um ou mais.

Módulo Criptográfico Equipamento especialmente desenvolvido para a gestão e protecção de chaves criptográficas e outros dados considerados sensíveis em sistemas de TIC.

PEM Definido na RFC 1422 [22], é um formato de contêiner que pode incluir apenas o certificado público ou pode incluir uma cadeia de certificados, incluindo chave pública, chave privada e certificados raiz. também pode ser usado para codificar um CSR, pois o formato PKCS#10 pode ser traduzido em PEM. O nome é de *Privacy Enhanced Mail* (PEM).

Pen Drive Pen Drive ou Memória USB Flash Drive é um dispositivo de armazenamento de dados que inclui memória flash (EEPROM) e possui uma interface USB (tipo A).

PKCS#10 Também conhecido como *Certificate Signing Request* (CSR) ou solicitação de assinatura de certificado, é uma mensagem enviada de um solicitante a uma autoridade de registo da infraestrutura de chaves públicas para solicitar um certificado digital. Geralmente contém a chave pública para a qual o certificado deve ser emitido, informações de identificação (como um nome de domínio) e protecção de integridade (por exemplo, uma assinatura digital).

Política de Certificado Documento que estabelece os termos, condições e âmbito de utilização do certificado e os requisitos que a declaração de práticas de certificação está obrigada a conter.

Provedor de serviços de certificação Pessoa singular ou colectiva que emita certificados e que pode fornecer outros serviços relacionados com assinatura electrónicas.

Sistema de Certificação Digital de Moçambique Sistema que visa garantir a autenticidade, integridade e validade jurídica de documentos em formato electrónico, ao abrigo dos artigos 54 e 55, conjugado com o artigo 74 da Lei n.º 3/2017, de 9 de Janeiro, Lei de Transacções Electrónicas.

Subscritor Pessoa singular ou colectiva identificada num certificado como detentora de um dispositivo de criação de assinatura. O mesmo que titular.

Titular Pessoa singular ou colectiva identificada num certificado como detentora de um dispositivo de criação de assinatura. O mesmo que subscritor.

Transacção electrónica Qualquer comunicação ou actividade entre duas partes conduzidas por meios electrónicos.

Validação cronológica Declaração de Entidade Certificadora que atesta a data e hora da criação, expedição ou recepção de um documento electrónico.