SISP – SOCIEDADE INTERBANCÁRIA E SISTEMAS DE PAGAMENTO

Política de Certificação da Entidade de Certificação Raiz da SISP

- PC da SISP-Root CA -

Cód.	PLRC003
Versão:	5.0
Data da versão:	17/06/2022
Criado por:	SISP
Aprovado por:	Direção Geral
Nível de confidencialidade:	Público

Histórico de alterações

Data	Versão	Autor	Descrição da alteração
16/01/2018	1.0	SISP	Criação do documento
21/03/2018	2.0	SISP	Atualização do documento
13/04/2018	3.0	SISP	Atualização do modelo de documento
31/07/2018	4.0	SISP	Alteração da estrutura hierárquica da PKI da SISP
30/06/2019	5.0	SISP	Alteração do perfil de certificado das SubCA's
17/06/2022	5.0	SISP	Revisão do documento

Documentos relacionados

Declaração de Praticas de Certificação da SISP Root CA

Índice

1. INTRODUÇÃO

1.1. OBJECTIVOS

O objetivo deste documento é definir as politicas utilizadas na emissão do certificado da Entidade da Certificação Raiz da SISP (SISP Root CA).

1.2. PÚBLICO-ALVO

Este documento é público e destina-se a todos quantos se relacionam com a Entidade de Certificação Raiz da SISP doravante designada de SISP Root CA.

1.3. ESTRUTURA DO DOCUMENTO

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

Este documento complementa a Declaração de Práticas de Certificação da Entidade de Certificação Raiz da SISP, presumindo-se que o leitor leu integralmente o seu conteúdo antes de iniciar a leitura deste documento.

[1] cf. RFC 3647. 2003, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

2. ACRÓNIMOS E DEFINIÇÕES

Encontra-se disponível, nas páginas seguintes, uma lista com definições e acrónimos pertinentes para a leitura deste documento.

2.1. ACRÓNIMOS

Acrónimo	
ANSI	***American National Standards Institute***
CA	***Certification Authority*** **(o mesmo que EC)**
DL	**Decreto-lei**
DN	***Distinguished Name***
DPC	**Declaração de Práticas de Certificação**
EC	**Entidade de Certificação**
SISP Root CA	**Entidade de Certificação Raiz da SISP**
ICP-CV	**Infra-estrutura de chaves públicas de Cabo Verde**
LCR	**Lista de Certificados Revogados**
MAC	***Message Authentication Codes***
OCSP	***Online Certificate Status Protocol***
OID	***Object Identifier*** **(Identificador de Objecto)**
PKCS	***Public-Key Cryptography Standards***
PKI	***Public Key Infrastructure*** **(Infra-estrutura de Chave Pública)**
SHA	***Secure Hash Algorithm***
SSCD	***Secure Signature-Creation Device***
URI	***Uniform Resource Identifier***

2.2. DEFINIÇÕES

Assinatura digital, conforme disposto no DL-nº33/2007, de 24 de Setembro	Modalidade de assinatura eletrónica 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 eletrónico 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 eletrónico foi alterado depois de aposta a assinatura.
Assinatura electrónica, conforme disposto no DL-nº33/2007, de 24 de Setembro	Dados sob forma eletrónica anexos ou logicamente associados a uma mensagem de dados e que sirvam de método de autenticação.
Assinatura electrónica avançada, conforme disposto no DL-nº33/2007, de 24 de Setembro.	Assinatura eletrónica que preenche os seguintes requisitos: i) Identifica de forma unívoca o titular como autor do documento; ii) A sua aposição ao documento depende apenas da vontade do titular; iii) É criada com meios que o titular pode manter sob seu controlo exclusivo; iv) A sua conexão com o documento permite detectar toda e qualquer alteração superveniente do conteúdo deste.
Assinatura eletróncia qualificada, conforme disposto no DL-nº33/2007, de 24 de Setembro.	Assinatura digital ou outra modalidade de assinatura eletrónica 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.
Autoridade Credenciadora, conforme disposto no DL-nº33/2007, de 24 de Setembro.	Entidade competente para a credenciação e fiscalização das Entidades de Certificação.
Certificado, conforme disposto no DL- nº33/2007, de 24 de Setembro	Documento eletrónico que liga os dados de verificação de assinatura ao seu titular e confirma a identidade desse titular.
Certificado qualificado, conforme disposto no DL-nº33/2007, de 24 de Setembro	Certificado que contém os elementos referidos no artigo 67.º do DL 33/2007 [6] e é emitido por entidade de certificação que reúne os requisitos definidos no

artigo 45.º do DL 33/2007.

Chave privada, conforme disposto no DL- nº33/2007, de 24 de Setembro	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, conforme disposto no DL- nº33/2007, de 24 de Setembro	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento electrónico pelo titular do par de chaves assimétricas, ou se cifra um documento electrónico a transmitir ao titular do mesmo par de chaves.
Credenciação, conforme disposto no DL- nº33/2007, de 24 de Setembro	Ato pelo qual é reconhecido a uma entidade, que o solicite e que exerça a actividade de entidade de certificação, o preenchimento dos requisitos definidos no DL-nº33/2007, de 24 de Setembro para os efeitos nele, previstos.
Dados de criação de assinatura, conforme disposto no DL-nº33/2007, de 24 de Setembro	Um conjunto único de dados, como códigos ou chaves criptográficas privadas, usado pelo signatário para a criação de uma assinatura electrónica.
Dados de verificação de assinatura, conforme disposto no DL-nº33/2007, de 24 de Setembro	Um conjunto de dados, como códigos ou chaves criptográficas públicas, usado para verificar a assinatura electrónica.
Dispositivo de criação de assinatura, conforme disposto no DL-nº33/2007, de 24 de Setembro	Suporte lógico ou dispositivo de equipamento utilizado para possibilitar o tratamento dos dados de criação de assinatura.
Dispositivo seguro de criação de assinatura, conforme disposto no DL-nº33/2007, de 24 de Setembro	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, conforme disposto no DL-nº33/2007, de 24 de Setembro.	Documento elaborado mediante processamento electrónico de dados.
Endereço electrónico, conforme disposto no DL-nº33/2007, de 24 de Setembro.	Identificação de um equipamento informático adequado para receber e arquivar documentos electrónicos.

3. CONTEXTO GERAL

3.1. INTRODUÇÃO

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

Este documento descreve a política de certificados para a emissão e gestão de certificados emitidos pela SISP *Root Certification Authority* (SISP Root CA).

Todos os certificados emitidos da hierarquia da SISP Root CA estão em conformidade com os requisitos da ICP-CV e com os seguintes standards:

a) *RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework;*
b) *RFC 5280 - Internet X.509 PKI - Certificate and CRL Profile*.

Os certificados emitidos pela SISP Root CA contêm uma referência à presente Politica de Certificados, código de documento PLRC003.05, de modo a permitir que Partes Confiantes e outras pessoas interessadas, possam encontrar informação sobre o certificado e sobre a entidade que o emitiu.

3.2. VISÃO GERAL

Esta PC satisfaz e complementa os requisitos impostos pela Declaração de Práticas de Certificação da Entidade de Certificação Raiz da SISP.

3. 3. IDENTIFICAÇÃO DO DOCUMENTO

Este documento é a Politica de Certificados da Entidade Certificadora, SISP Root CA. A PC é representada num certificado através de um número único designado de "identificador de objeto" (OID), sendo o valor do OID associado a este documento o 2.16.132.1.2.2.3.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 5.0
Estado do Documento	Aprovado
OID	2.16.132.1.2.2.3
Data de Emissão	30/06/2019
Validade	Não aplicável
Localização	https://pki.sisp.cv/

3.4. CONTACTO

A gestão desta DPC é da responsabilidade do Grupo de Trabalho de Segurança, que pode ser contactada pelos telefones e no seguinte endereço:

Nome:	Grupo de Trabalho de Segurança
Morada:	SISP, SA Conj. Habitacional Novo Horizonte, Rua Cidade de Funchal, Achada Santo Antonio – Praia, Cabo Verde
Correio electrónico:	pki@sisp.cv
Site:	www.sisp.cv
Telefone:	2606310/2626317

4 . IDENTIFICAÇÃO E AUTENTICAÇÃO

4.1 ATRIBUIÇÃO DE NOMES

A atribuição de nomes segue a convenção determinada pela DPC da SISP Root CA.

4.1.1 TIPOS DE NOMES

O certificado da SISP Root CA é identificado por nome único (*DN – Distinguished Name*) de acordo com a norma X.509. O nome único do certificado da SISP Root CA é identificado pelos seguintes componentes:

Atributo	Codigo	Valor
Country	C	Cabo Verde
Organization	O	SISP – Sociedade Interbancaria e Sistemas de Pagamentos, SA
Common Name	CN	SISP Root CA

4.1.2 USO CERTIFICADO E PAR DE CHAVES PELO TITULAR

A SISP é a titular do certificado de SISP Root CA assinada pela ECR-CV, utilizando a sua chave privada para a assinatura de certificados de Entidades de Certificação Subordinadas, assinatura do certificado da Entidade Certificadora de Validação Cronológica (SISP TSA), assinatura da respetiva Lista de Certificados Revogados (CRL) bem como para assinatura de certificados destinados ao serviço OCSP, de acordo com a sua DPC.

4.2 VALIDAÇÃO DA IDENTIDADE NO REGISTO INICIAL

4.2.1 MÉTODO DE COMPROVAÇÃO DA POSSE DE CHAVE PRIVADA

No certificado da SISP Root CA, a comprovação da posse da chave privada será garantida através da presença física dos vários Grupos de Trabalho relevantes e de um representante da Entidade Credenciadora, na cerimónia de emissão desse tipo de certificados. Nessa cerimónia, será gerado e apresentado o pedido de certificado no formato PKCS#10, cuja assinatura sobre a informação da chave pública será validade pela ECR-CV.

4.2.2 AUTENTICAÇÃO DA IDENTIDADE DE UMA PESSOA COLECTIVA

A SISP responsabiliza pela guarda de toda a documentação utilizada para verificação da identidade da entidade de certificação, 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 processo de autenticação da identidade de uma pessoa coletiva, deve obrigatoriamente garantir que a pessoa coletiva 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 coletiva.

O documento que serve de base à emissão do certificado de uma EC contém, entre outros os seguintes elementos:

a) Documentos, para efeitos de identificação de EC e sua denominação legal;

b) Número de Identificação Fiscal, sede, objeto 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 EC subordinada à SISP Root CA, na hierarquia de confiança PKI da SISP e da ICP-CV, de acordo com a presente DPC;

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

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 EC;

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

4.2.3 AUTENTICAÇÃO DA IDENTIDADE DE UMA PESSOA SINGULAR

Nada a assinalar.

4.2.4 INFORMAÇÃO DE SUBSCRITOR/TITULAR NÃO VERIFICADA

Toda a informação descrita nos pontos 4.2.2 e 4.2.3 é verificada.

4.2.5 VALIDAÇÃO DE AUTORIDADE

Nada a assinalar.

4.2.6 CRITÉRIOS PARA INTEROPERABILIDADE

Nada a assinalar.

4.3 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDO DE REVOGAÇÃO

Dadas as consequências da revogação do certificado da SISP Root CA, é exigido um documento formal do Conselho de Administração da SISP que inclui entre outros:

a) A decisão do Conselho de Administração de revogar o certificado da SISP Root CA;
b) Os motivos da revogação do certificado;
c) Informação, se necessário, relativa à identificação e aos poderes do(s) representante(s) nomeado(s)

pela entidade para estar(em) presente(s) na cerimónia de revogação do certificado da SISP Root CA.

5 . PERFIS DE CERTIFICADO E CRL

5.1 PERFIL DE CERTIFICADO

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

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

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

O perfil do certificado da raiz da SISP Root CA está de acordo com os requisitos da ICP-CV e com os seguintes standards:

a) RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework;
b) RFC 5280 - Internet X.509 PKI - Certificate and CRL Profile;
c) Legislação caboverdiana.

5.1.1 NÚMERO DA VERSÃO

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

5.1.2 EXTENSÕES DE CERTIFICADO

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

5.1.3 PERFIL DO CERTIFICADO

Componente do Certificado	Componente do Certificado	Secção no RFC5280	Valor	Tipo	Comentários
	Version	4.1.2.1	3	m	O valor 3 identifica a utilização de certificados ITU-T X.509 versão 3
	Serial Number	4.1.2.2	<atribuído pela EC a cada certificado>	m	
	Signature	4.1.2.3	2.16.840.113549.1.1.11	m	Valor TEM que ser igual ao OID no signatureAlgorithm (abaixo)
	Issuer	4.1.2.4		m	
	Country (C)		"CV"		
	Organization (O)		"ICP-CV"		Designação Oficial da ECR Cabo Verde
	Organization Unit (OU)		"ANAC-Agencia Nacional das Comunicacoes"		
	Common Name (CN)		"Entidade de Certificacao Raiz de Cabo Verde 01"		
	Validity	4.1.2.5		m	For the purposes of this profile, GeneralizedTime values MUST be expressed in Greenwich Mean Time (Zulu) and MUST include seconds (i.e., times are YYYYMMDDHHMMSSZ), even where the number of seconds is zero. GeneralizedTime values MUST NOT include fractional seconds
	Not Before		<data de emissão>		
	Not After		<data de emissão + 12 anos>		Validade de 12 anos com renovação a cada 6 anos.
tbsCertificate	**Subject**	4.1.2.6	<SISP Root CA>	m	
	Country (C)		"CV"		
	Organization (O)		"ICP-CV"		
	Organization Unit (OU)		"SISP-Sociedade Interbancaria e Sistemas de Pagamentos"		
	Common Name (CN)		"Entidade de Certificacao Raiz da SISP 01"		

	Subject Public Key Info Algorithm subjectPublicKey	4.1.2.7	 1.2.840.113549.1.1.1 <Chave Pública com modulus n de 4096 bits>	m	Utilizado para conter a chave pública e identificar o algoritmo com o qual a chave é utilizada (e.g., RSA, DSA ou Diffie-Hellman). O OID rsaEncryption identifica chaves públicas RSA. pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 } rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1} O OID rsaEncryption deve ser utilizado no campo algorithm com um valor do tipo AlgorithmIdentifier. Os parâmetros do campo TÊM que ter o tipo ASN.1 a NULL para o identificador deste algoritmo.24

	Unique Identifiers				
	X509v3 Extensions	4.1.2.8		m	O "unique identifiers" está presente para permitir a possibilidade de reutilizar os nomes do subject e/ou issuer 20
	Authority Key Identifier KeyIdentifier	4.2.1.1	< O key Identifier é composto pela hash de 160-bit SHA-I do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>	m	
	Subject Key Identifier	4.2.1.2	< O key Identifier é composto pela hash de 160-bit SHA-I do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>	m	
	Key Usage Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement Key Certificate Signature CRL Signature Encipher Only Decipher Only	4.2.1.3	"0" seleccionado "0" seleccionado "0" seleccionado "0" seleccionado "0" seleccionado "1" seleccionado "1" seleccionado "0" seleccionado "0" seleccionado	mc	Esta extensão é marcada CRÍTICA
	Cerificate Policies	4.2.1.4		o	
	Basic Constrains CA PathLenConstraint	4.2.1.9	TRUE	o m o	Indica o tipo de Entidade a quem se destina o certificado; restrição básica, se o CA =true o certificado pode assinar uma EC
	CRLDistributionPoints distributionPoint	4.2.1.13	http://crl.sisp.cv/sisprootca.crl	o m	
	Signature Algorithm	4.1.1.2	2.16.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 20
	Signature Value	4.1.1.3	<contém a assinatura digital emitida pela EC>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (subject) do certificado.

5.1.4 OID DO ALGORITMO

O campo "*signatureAlgorithm*" do certificado contém o OID do algoritmo criptográfico utilizado pela EC para assinar o certificado: 2.16.840.113549.1.1.11 (sha256WithRSAEncryption12).

5.1.5 FORMATO DE NOMES

Tal como definido na secção 4.1.

5.1.6 CONDICIONAMENTO NOS NOMES

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

5.1.7 OID DA POLÍTICA DE CERTIFICADOS

A extensão "*certificate policies"* não se encontra ativa no certificado da SISP Root CA.

5.1.8 UTILIZAÇÃO DA EXTENSÃO POLICY CONSTRAINTS

Nada a assinalar.

5.1.9 SINTAXE E SEMÂNTICA DO QUALIFICADOR DE POLÍTICA

Nada a assinalar.

5.1.10 SEMÂNTICA DE PROCESSAMENTO PARA A EXTENSÃO CRÍTICA CERTIFICATE POLICIES

Nada a assinalar.

5.2 PERFIL DA LISTA DE REVOGAÇÃO (CRL)

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

O protocolo X.509 define um método de revogação do certificado, que envolve a emissão periódica, pela EC, de uma estrutura de dados assinada, a que se dá o nome de Lista de Revogação de Certificados (CRL).

A CRL é uma lista com identificação temporal dos certificados revogados, assinada pela EC e disponibilizada livremente num repositório público. Cada certificado revogado é identificado na CRL pelo seu número de série.

Quando uma aplicação utiliza um certificado (por exemplo, para verificar a assinatura digital de um utilizador remoto), a aplicação verifica a assinatura e validade do certificado, assim como obtém a CRL mais recente e verifica se o número de série do certificado não faz parte da mesma. Note-se que uma EC emite uma nova

CRL numa base regular periódica.

O perfil da CRL está de acordo com:

a) Recomendação ITU.T X.509;
b) RFC 5280 e,
c) Legislação cabo-verdiana.

5.2.1 NÚMERO DE VERSÃO

O campo “version” da CRL descreve a versão utilizada na codificação da CRL. Neste perfil, a versão utilizada é 2 (dois).

5.2.2 PERFIL DA CRL DA SISP ROOT CA

Componente da CRL	Componente do Certificado	Secção no RFC5280	Valor	Tipo	Comentários
tbsCertList	**Version**	5.1.2.1	1	m	O valor 1 identifica a utilização da Versão 2 do padrão ITU X.509
	Signature	5.1.2.2	2.16.840.113549.1.1.11	m	Contém o identificador do algoritmo utilizado para assinar a LCR. O valor TEM que ser igual ao OID no campo signatureAlgorithm (abaixo)
	Issuer	5.1.2.3		m	
	Country (C)		"CV"		
	Organization (O)		"IPC-CV"		
	Common Name (CN)		"Entidade de Certificacao Raiz da SISP "		
	thisUpdate	5.1.2.4	<data de emissão da CRL>	m	For the purposes of this profile, GeneralizedTime values MUST be expressed in Greenwich Mean Time (Zulu) and MUST include seconds (i.e., times are YYYYMMDDHHMMSSZ), even where the number of seconds is zero. GeneralizedTime values MUST NOT include fractional seconds
	nextUpdate	5.1.2.5	<data da próxima emissão da LCR = thisUpdate + N>	m	Este campo indica a data em que a próxima LCR vai ser emitida. A próxima LCR pode ser emitida antes da data indicada, mas não será emitida depois dessa data. Os emissores da LCR DEVEM emitir LCR com o tempo de nextUpdate maior ou igual a todas as LCR anteriores. Implementações TÊM que utilizar o tempo UTC até 2049, e a partir dessa data devem utilizar o GeneralisedTime. N será no máximo 90 dias.
	revokedCertificates	5.1.2.6	<lista de certificados revogados>	m	
	CRL Extensions	5.1.2.7		m	
	Authority Key Identifier	5.2.1		o	

	KeyIdentifier		O key Identifier é composto pela hash de 160-bit SHA-256 do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>		
	CRL Number	5.2.3	<número sequencial único e incrementado>	m	
	Issuing Distribuition Point DistributionPointName	5.2.5	http://crl.sisp.cv/sisprootca.crl	c	
	CRL Entry Extensions	5.3			

	Reason Code				Valor tem que ser um dos seguintes: 1 – keyCompromise 2 – cACompromise 3 – affiliationChanged 4 – superseded 5 – cessationOfOperation 6 – certificateHold 8 – removeFromCRL 9 – privilegeWithdrawn 10 - Compromise
	Signature Algorithm	5.3.1 5.1.1.2	 2.16.840.113549.1.1.11	o m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member- body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 20
	Signature Value	5.1.1.3	<contém a assinatura digital emitida pela EC>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (subject) do certificado.

5.3 PERFIL DE CERTIFICADO DE OCSP

Nada a assinalar

5.4 PERFIL DE CERTIFICADO ENTIDADES CERTIFICADORAS SUBORDINADAS

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

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

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

O perfil do certificado das Entidades Certificadoras Subordinadas está de acordo com os requisitos da ICP-CV e com os seguintes standards:

a) *RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework;*
b) RFC 5280 - Internet X.509 PKI - Certificate and CRL Profile;
c) Legislação cabo-verdiana

5.4.1 NÚMERO DA VERSÃO

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

5.4.2 EXTENSÕES DE CERTIFICADO

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

5.4.3 PERFIL DO CERTIFICADO

Componente do Certificado	Componente do Certificado	Secção no RFC5280	Valor	Tipo	Comentários
tbsCertificate	**Version**	4.1.2.1	3	m	O valor 3 identifica a utilização de certificados ITU-T X.509 versão 3
	Serial Number	4.1.2.2	<atribuído pela EC a cada certificado>	m	
	Signature	4.1.2.3	2.16.840.113549.1.1.11	m	Valor TEM que ser igual ao OID no signatureAlgorithm (abaixo)
	Issuer	4.1.2.4		m	
	Country (C)		"CV"		
	Organization (O)		"ICP-CV"		
	Organization Unit (OU)		"SISP-Sociedade Interbancária e Sistemas de Pagamentos"		Designação Oficial da EC da SISP
	Common Name (CN)		"Entidade de Certificação Raiz da SISP <nn> "		nn - sequencia da EC
	Validity	4.1.2.5		m	
	Not Before		<data de emissão>		
	Not After		<data de emissão + 6 anos>		Validade de 6 anos com renovação a cada 3 anos.
	Subject	4.1.2.6		m	
	Country (C)		"CV"		
	Organization (O)		"ICP-CV"		
	Organization Unit (OU)		"SISP-Sociedade Interbancaria e Sistemas de Pagamentos"		
	Common Name (CN)		<nome da subca>		
	Select Public Key Info	4.1.2.7		m	Utilizado para conter a chave pública e identificar o algoritmo com o qual a chave é utilizada (e.g., RSA, DSA ou Diffie-Hellman).

	Algorithm subjectPublicKey		1.2.840.113549.1.1.1 <Chave Pública com modulus n de 4096 bits>		O OID rsaEncryption identifica chaves públicas RSA. pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 } rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1} O OID rsaEncryption deve ser utilizado no campo algorithm com um valor do tipo AlgorithmIdentifier. Os parâmetros do campo TÊM que ter o tipo ASN.1 a NULL para o identificador deste algoritmo.24
	Unique Identifiers	4.1.2.8		m	O "unique identifiers" está presente para permitir a possibilidade de reutilizar os nomes do subject e/ou issuer 20

	X509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier KeyIdentifier	4.2.1.1	 O key Identifier é composto pela hash de 160-bit SHA-256 do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>	m	
	Subject Key Identifier	4.2.1.2	O key Identifier é composto pela hash de 160-bit SHA-256 m do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>	m	
	Key Usage Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement Key Certificate Signature CRL Signature Encipher Only Decipher Only	4.2.1.3	 "0" seleccionado "0" seleccionado "0" seleccionado "0" seleccionado "0" seleccionado "1" seleccionado "1" seleccionado "0" seleccionado "0" seleccionado	mc	Esta extensão é marcada CRÍTICA
	Cerificate Policies policyIdentifier policyQualifiers	4.2.1.4	 2.16.132.1.1.2.3 <policyQualifierID> cPSuri: https://pki.sisp.cv	o m o	Identificador da Declaração de Práticas de Certificação da EC Raiz da SISP (id-qt-cps PKIX CPS Pointer Qualifier) Descrição do OID: "O atributo cPSuri contém um apontador para a Declaração de Práticas de Certificação publicada pela SISP ROOT CA. O apontador está na forma de um URL."
	policyIdentifier policyQualifiers		2.16.132.1.2.2.3 <policyQualifierID> cPSuri: https://pki.sisp.cv	m o	Identificador da Declaração de Práticas de Certificação da EC Raiz da SISP (id-qt-cps PKIX CPS Pointer Qualifier) Descrição do OID: "O atributo cPSuri contém um apontador para a Politica de Certificados publicada pela SISP ROOT CA. O apontador está na forma de um URL."
	Basic Constrains CA PathLenConstraint	4.2.1.9	 TRUE 0	o m o	Indica o tipo de Entidade a quem se destina o certificado; restrição básica, se o CA =true o certificado pode assinar uma EC
	CRLDistributionPoints distributionPoint	4.2.1.13	 http://crl.sisp.cv/sisprootca.crl	o m	

	Internet Certificate Extensions				
	Authority Information Access accessMethod accessLocation	4.2.2.1	 1.3.6.1.5.5.7.48.2 http://ocsp.sisp.cv	o m m	Valor do OID: (id-ad-ocsp)
	Signature Algorithm	4.1.1.2	2.16.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 20
	Signature Value	4.1.1.3	<contém a assinatura digital emitida pela EC>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (subject) do certificado.

6. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

6.1 PEDIDO DE CERTIFICADO

6.1.1 QUEM PODE SUBSCREVER UM PEDIDO DE CERTIFICADO

O certificado da EC SISP Root apenas pode ser pedido pelo Conselho de Administração da SISP – Sociedade Interbancária e Sistemas de Pagamentos, S.A.

O certificado da EC Subordinada pode ser solicitado pelo(s) representante(s) da pessoa coletiva que legal e estatutariamente a obrigam.

6.1.2 PROCESSO DE REGISTO E RESPONSABILIDADES

O processo de registo do certificado de EC é constituído pelos seguintes passos, a serem efetuados pelos Grupos de Trabalho relevantes:

- Geração do par de chaves (chave pública e privada) em ambiente criptográfico apropriado;
- Geração do PKCS#10 correspondente, em ambiente criptográfico apropriado.

6.2 PROCESSAMENTO DO PEDIDO DE CERTIFICADO

O pedido de certificado é processado do seguinte modo:

a) Criação do par de chaves e assinatura do certificado em ambiente criptográfico apropriado, de acordo com o perfil indicado nesta política;
b) Disponibilização do certificado.

As secções 6.2.1 e 6.3 descrevem detalhadamente todo o processo.

6.2.1 PROCESSOS PARA A IDENTIFICAÇÃO E FUNÇÕES DE AUTENTICAÇÃO

Os Grupos de trabalho relevantes executam a identificação e a autenticação de toda a informação necessária de acordo com o estipulado na secção 6 deste documento.

1. Os Grupos de trabalho relevantes aprovam a candidatura para emissão do Certificado SISP Root CA:
    a. Existe consentimento expresso do Grupo de Gestão da PKI da SISP.
2. Certificado para Entidade de Certificação Subordinada:
    a. Identificação e autenticação bem-sucedida de toda a informação necessária nos termos da secção 4 – toda a documentação, utilizada para verificação da identidade e de poderes de representação, é guardada;
    b. PKCS#10 válido.

Em qualquer outra situação, o pedido de emissão de certificado não será aceite.

Após a emissão do certificado, os Grupos de trabalho relevantes disponibilizam o certificado ao Grupo de

Gestão da PKI da SISP e, se for o caso, aos representantes legais da Entidade de Certificação Subordinada.

6.2.2 APROVAÇÃO OU RECUSA DE PEDIDOS DE CERTIFICADO

A aprovação de certificado passa pelo cumprimento dos requisitos exigidos no ponto 6.2 e 6.2.1.

Quando tal não se verifique, é recusada a emissão do certificado.

6.2.3 PRAZO PARA PROCESSAR O PEDIDO DE CERTIFICADO

Após a aprovação do pedido de certificado, o certificado deverá ser emitido em não mais do que cinco (5) dias úteis.

6.3 EMISSÃO DE CERTIFICADO

6.3.1 PROCEDIMENTOS PARA A EMISSÃO DE CERTIFICADO

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

- Os representantes legais da SISP S.A., seus procuradores ou das entidades subordinadas nomeado (s) para esta cerimónia;
- Pelo menos três (3) membros dos Grupos de Trabalhos;
- Um Auditor da ANAC na geração do par de chaves da SISP Root CA e o Auditor SISP no caso das Sub CA's .;
- Quaisquer observadores, aceites pelo Grupo de Gestão da PKI da SISP.

A cerimónia de emissão de certificado é constituída pelos seguintes passos:

- Identificação e autenticação de todas as pessoas presentes na cerimónia, garantindo que o(s) representante(s) e os membros do Grupo de Trabalho têm os poderes necessários para os atos a praticar;
- Os membros do Grupo de Trabalho efetuam o procedimento de arranque de processamento do certificado e emitem o Pedido de Assinatura de Certificado (CSR) (correspondente ao PKCS#10 gerado no HSM), que é arquivado num suporte tecnológico (não regravável);
- O certificado emitido e assinado pela Entidade Certificadora hierarquicamente superior, é importado na EC correspondente;
- Procede-se á geração da primeira CRL;
- A cerimónia de emissão fica concluída com a execução do procedimento de finalização de processamento do certificado, pelos membros do Grupo de Trabalho;

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

6.3.2 NOTIFICAÇÃO DA EMISSÃO DO CERTIFICADO AO TITULAR

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

6.4 ACEITAÇÃO DO CERTIFICADO

6.4.1 PROCEDIMENTOS PARA A ACEITAÇÃO DO CERTIFICADO

O certificado considera-se aceite após a assinatura do formulário de emissão e aceitação de certificado pelo(s) representante(s) de acordo com cerimónia de emissão (conforme secção 6.3.1).

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

a) Titular toma conhecimento dos seus direitos e responsabilidades;
b) Titular toma conhecimento das funcionalidades e conteúdo do certificado;
c) Titular aceita formalmente o certificado e as suas condições de utilização assinando para o efeito o formulário de receção e aceitação de certificado.

Os procedimentos necessários em caso de expiração, revogação e renovação do certificado, bem como os termos, condições e âmbito de utilização do mesmo estão definidos nesta Política de Certificados e na respetiva Declaração de Práticas de Certificação.

6.4.2 PUBLICAÇÃO DO CERTIFICADO

A SISP Root CA não publica certificados emitidos para Entidades de Certificação Subordinadas disponibilizandos-o integralmente ao titular, nas condições definidas no ponto 6.4.1.

6.4.3 NOTIFICAÇÃO DA EMISSÃO DE CERTIFICADO A OUTRAS ENTIDADES

A Autoridade Credenciadora será convidada para a cerimónia de emissão do certificado da SISP Root CA. Será igualmente notificada cada vez que for emitido um certificado de uma EC subordinada.

6.5 USO DO CERTIFICADO E PAR DE CHAVES

6.5.1 USO DO CERTIFICADO E DA CHAVE PRIVADA PELO TITULAR

Os titulares de certificados utilizarão a sua chave privada apenas e só para o fim a que estas se destinam (conforme estabelecido no campo do certificado "keyUsage") e sempre com propósitos legais.

A sua utilização apenas é permitida:

a) A quem estiver designado no campo "Subject" do certificado;
b) De acordo com as condições definidas na secção 3.5 da Declaração de Práticas de Certificação (DPC);
c) Enquanto o certificado se mantiver válido e não estiver na CRL da SISP Root CA.

6.5.2 USO DO CERTIFICADO E DA CHAVE PÚBLICA PELAS PARTES CONFIANTES

Na utilização do certificado e da chave pública, as partes confiantes apenas podem confiar nos certificados, tendo em conta apenas o que é estabelecido nesta Política de Certificado e na respetiva DPC.

Para isso devem, entre outras, garantir o cumprimento das seguintes condições:

a) Ter conhecimento e perceber a utilização e funcionalidades proporcionadas pela criptografia de chave

pública e certificados;
b) Ser responsável pela sua correta utilização;
c) Ler e entender os termos e condições descritos nas políticas e práticas de certificação;
d) Verificar os certificados (validação de cadeias de confiança) e CRL, tendo especial atenção às suas extensões marcadas como críticas e propósito das chaves;
e) Confiar nos certificados, utilizando-os sempre que estes estejam válidos.

6.6 RENOVAÇÃO DO CERTIFICADO COM GERAÇÃO DE NOVO PAR DE CHAVES

A renovação de chaves do certificado (certificate re-key) é o processo em que um titular (ou patrocinador) gera um novo par de chaves e submete o pedido para emissão de novo certificado que certifica a nova chave pública. Este processo, no âmbito desta Política de Certificado, é designado por renovação de certificado com geração de novo par de chaves.

A renovação de certificado com geração de novo par de chaves é feita de acordo com o estabelecido na secção 6.3.

6.6.1 MOTIVO PARA A RENOVAÇÃO DO CERTIFICADO COM GERAÇÃO DE NOVO PAR DE CHAVES

É motivo válido para a renovação de certificado com geração de novo par de chaves, sempre e quando se verifique que:

a) Certificado está a expirar;
b) Suporte do certificado está a expirar;
c) A informação constante no certificado sofre alterações.

6.6.2 QUEM PODE SUBMETER O PEDIDO DE CERTIFICADO DE UMA NOVA CHAVE PÚBLICA

Tal como na secção 6.1.1.

6.6.3 PROCESSAMENTO DO PEDIDO DE RENOVAÇÃO DO CERTIFICADO COM GERAÇÃO DE NOVO PAR DE CHAVES

Tal como na secção 6.1.2 e 6.2.

6.6.4 NOTIFICAÇÃO DA EMISSÃO DE NOVO CERTIFICADO AO TITULAR

Tal como na secção 6.3.2.

6.6.5 PROCEDIMENTOS PARA ACEITAÇÃO DE UM CERTIFICADO RENOVADO COM GERAÇÃO DE NOVO PAR DE CHAVES

Tal como na secção 6.4.1.

6.6.6 PUBLICAÇÃO DE CERTIFICADO RENOVADO COM GERAÇÃO DE NOVO PAR DE CHAVES

Tal como na secção 6.4.2.

6.6.7 NOTIFICAÇÃO DA EMISSÃO DE CERTIFICADO RENOVADO A OUTRAS ENTIDADES

Tal como na secção 6.4.3.

6.7 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

Na prática, a revogação e suspensão de certificados é uma ação através da qual o certificado deixa de estar válido antes do fim do seu período de validade, perdendo a sua operacionalidade.

Os certificados depois de revogados não podem voltar a ser válidos, enquanto que, os certificados suspensos podem recuperar a sua validade.

6.7.1 MOTIVOS PARA A SUSPENSÃO

A SISP Root CA não suspende certificados.

7.7.2 QUEM PODE SUBMETER O PEDIDO DE SUSPENSÃO

Nada a assinalar.

6.7.3 PROCEDIMENTOS PARA PEDIDO DE SUSPENSÃO

Nada a assinalar.

6.7.4 LIMITE DO PERÍODO DE SUSPENSÃO

Nada a assinalar.

6.7.5 MOTIVOS PARA A REVOGAÇÃO

Um certificado pode ser revogado por uma das seguintes razões:

- Comprometimento da chave privada;
- Comprometimento da chave privada da SISP Root CA;
- Perda da chave privada;
- Inexatidões, graves nos dados fornecidos;
- Equipamento tecnológico deixa de ser utilizado no âmbito da SISP Root CA;
- Comprometimento ou suspeita de comprometimento da senha e acesso à chave privada (exemplo: PIN);
- Perda, destruição ou deterioração do dispositivo de suporte da chave privada (por exemplo, suporte/token criptográfico);
- Incumprimento por parte da SISP Root CA ou titular das responsabilidades previstas na presente Política de Certificado e/ou correspondente DPC;
- 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;
- Por ordem judicial ou, desde que devidamente fundamentada, pelas entidades integrantes da ICP-CV a saber:
    - Conselho Gestor da ICP-CV
    - Autoridade Credenciadora
    - ECR-CV
- Cessação de funções.

O certificado é revogado no prazo máximo de 24 horas.

6.7.6 QUEM PODE SUBMETER O PEDIDO DE REVOGAÇÃO

Está legitimado para submeter o pedido de revogação, sempre que se verifiquem alguma das condições descritas no ponto 6.7.5, as seguintes entidades:

- Os responsáveis legais da Entidade de Certificação Subordinada;

- A SISP S.A.;
- Uma parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos.

A SISP Root CA guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efetua o pedido de revogação, garantindo a verificação da identidade dos seus representantes legais, por meio legalmente reconhecido, não aceitando poderes de representação para o pedido de revogação do certificado da SISP Root CA e nem das Entidades Certificadoras Subordinadas.

6.7.7 PROCEDIMENTO PARA O PEDIDO DE REVOGAÇÃO

Os procedimentos seguidos no pedido de revogação de certificado são os seguintes:

- Todos os pedidos de revogação devem ser endereçados à SISP S.A. por escrito ou por mensagem eletrónica assinada digitalmente, em formulário próprio de pedido de revogação, indicando o motivo do pedido de revogação;
- Identificação e autenticação da entidade que efetua o pedido de revogação;
- Registo e arquivo do formulário de pedido de revogação;
- Análise do pedido de revogação pelo Grupo de Trabalho de Autenticação da PKI da SISP, que propõe ao Grupo de Trabalho de Gestão a aprovação ou recusa do pedido de revogação;
- Mediante o parecer do Grupo de Trabalho de Autenticação da PKI da SISP, o Grupo de trabalho de Gestão, decide-se a aprovação ou recusa do pedido de revogação do certificado;
- Sempre que se decidir revogar um certificado, a revogação é publicada na respetiva CRL.

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

- Data do pedido de revogação;
- Nome do titular do certificado;
- Exposição pormenorizada dos motivos para o pedido de revogação;
- Nome e funções da pessoa que solicita a revogação;
- Informação de contacto da pessoa que solicita a revogação;
- Assinatura da pessoa que solicita a revogação.

6.7.8 PRODUÇÃO DE EFEITOS DA REVOGAÇÃO

A revogação será feita de forma imediata. Após terem sido efetuados todos os procedimentos e seja verificado que o pedido é válido, o pedido não pode ser anulado.

6.7.9 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.

6.7.10 REQUISITOS DE VERIFICAÇÃO DA REVOGAÇÃO PELAS PARTES CONFIANTES

Antes de utilizarem um certificado, as partes confiantes têm como responsabilidade verificar o estado de todos os certificados, através das CRL ou num servidor de verificação do estado online (via OCSP).

6.7.11 PERIODICIDADE DA EMISSÃO DA LISTA DE CERTIFICADOS REVOGADOS (CRL)

A SISP Root CA disponibiliza uma nova CRL Base a cada 3 (três) meses.

6.7.12 PERÍODO MÁXIMO ENTRE A EMISSÃO E A PUBLICAÇÃO DA CRL

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

6.7.13 DISPONIBILIDADE DE VERIFICAÇÃO ONLINE DO ESTADO / REVOGAÇÃO DE CERTIFICADO

A SISP Root CA não disponibiliza serviços de validação OCSP para os certificados.

6.7.14 REQUISITOS DE VERIFICAÇÃO ONLINE DE REVOGAÇÃO

Nada a assinalar.

6.7.15 OUTRAS FORMAS DISPONÍVEIS PARA DIVULGAÇÃO DE REVOGAÇÃO

Nada a assinalar.

6.7.16 REQUISITOS ESPECIAIS EM CASO DE COMPROMETIMENTO DE CHAVE PRIVADA

No caso da chave privada da SISP Root CA ser comprometida, devem ser tomadas medidas apropriadas de resposta ao incidente.

As respostas a esse incidente podem incluir:

- Revogação do certificado da SISP Root CA e de todos os certificados emitidos no "ramo" da hierarquia de confiança da SISP Root CA;
- Notificação da Autoridade Credenciadora e de todos os titulares de certificados emitidos no "ramo" da hierarquia de confiança da SISP Root CA;
- Geração de novo par de chaves para a SISP Root CA;
- Renovação de todos os certificados emitidos no "ramo" da hierarquia de confiança da SISP Root CA.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] ARME, Declaração de Práticas de Certificação da EC Raiz de Cabo Verde.
[2] ARME, Política de Certificados da ICP-CV e Requisitos mínimos de Segurança.
[3] Portaria nº 2/2008, de 28 de Janeiro;
[4] Decreto-Lei nº44/2009 de 9 de Novembro;

[5] Decreto Regulamentar nº. 18/2007, de 24 de Dezembro;
[6] Decreto-Lei nº 33 /2007, de 24 de Setembro;
[7] Portaria nº 4/2008

[8] FIPS 140-2. 1994, Security Requirements for Cryptographic Modules.

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

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

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

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

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

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

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

[16] RFC 2252. 1997, Lightweight Directory Access Protocol (v3).

[17] RFC 2560. 1999, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.
[18] RFC 2986. 2000, PKCS #10: Certification Request Syntax Specification, version 1.7.
[19] RFC 3161. 2001, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

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

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

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

[23] RFC 4210. 2005, Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP).
[24] Política de Certificado da EC Raiz de Cabo Verde
[25] CABForum Baseline Requirements
[26] CABForum-EV-Guidelines –v1.7.0