SISP – SOCIEDADE INTERBANCÁRIA E SISTEMAS DE PAGAMENTO

Política de Certificação da Entidade Certificadora Subordinada SISPCA01

- PC da SISPCA01 -

Cód.	PLRC004
Versão:	3.0
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
31/07/2018	1.0	SISP	Criação do documento
03/09/2018	1.1	SISP	Alteração de Perfis
30/06/2019	2.0	SISP	Introdução Perfil Certificado de Autenticação Web
10/05/2021	3.0	SISP	Introdução do perfil da Fatura Eletrónica e alteração dos perfis de Certificado Qualificado de Assinatura Individual e Autenticação Web
17/06/2022	3.0	SISP	Revisão do documento

Documentos relacionados

Declaração de Praticas de Certificação da SISP CA

Índice

1. INTRODUÇÃO

1.1. OBJECTIVOS

O objectivo deste documento é definir as políticas utilizadas na emissão dos certificados da Entidade de Certificação SISPCA01

1.2. PÚBLICO-ALVO

Este documento é público e destina-se a todos quantos se relacionam com a Entidade de Certificação SISPCA01 doravante designada de SISP 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 SISP CA, 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 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, conforme disposto no DL-nº33/2007, de 24 de Setembro	Dados sob forma electrónica 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 electrónica 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 electrónica qualificada, conforme disposto no DL-nº33/2007, de 24 de Setembro.	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.
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 electrónico 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	Acto 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 dos mesmos. 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 Certification Authority (SISPCA01).

Todos os certificados emitidos pela SISPCA01 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.
c) ETSI TS 102 042 V2.4.1
d) CABForum BR

Os certificados emitidos pela SISPCA01 contêm uma referência à presente Politica de Certificados, codigo de documento nr. PLRC004, 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 SISPCA01.

3. 3. IDENTIFICAÇÃO DO DOCUMENTO

Este documento é a Politica de Certificados da Entidade Certificadora, SISPCA01. A PC é representada num certificado através de um número único designado de "identificador de objecto" (OID), sendo o valor do OID associado a este documento o 2.16.132.1.2.2.3.2.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 3.0
Estado do Documento	Aprovado
OID	2.16.132.1.2.2.3.2
Data de Emissão	10/05/2021
Localização	https://pki.sisp.cv/

3.4. CONTACTO

A gestão desta PC 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:	https://pki.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 SISPCA01.

4.1.1 TIPOS DE NOMES

Os certificados emitidos pela SISPCA01 são identificados por nome único (DN – Distinguished Name) de acordo com a norma X.509. O nome único do certificado da SISPCA01 é identificado pelos seguintes componentes:

4.1.1.1 Certificado Qualificado de Assinatura Pessoa Singular

Atributo	Codigo	Valor
Country	C	<País da nacionalidade do titular do certificado>
Organization	O (opcional)	<Organização à qual o titular do certificado pertence>
Organization Unit	OU	Certificado para pessoa singular – Assinatura Qualificada
Organization Unit	OU (opcional)	<Área/Departamento da Organização à qual o titular do certificado pertence>
Locality	L(opcional)	<Local de residência do titular>
State or Province	ST (opcional)	<Distrito, estado, ilha de residência do titular>
Title	T (opcional)	<Qualidade do titular do certificado, no ambito da sua utilização para assinatura digital qualificada>
Serial Number	serialNumber	<NIC ou PAS>[1] <codigo pais>- <nº identificação>
Tax Id Number	taxIDNumber	<NIF do titular>
Common Name	CN	<Nome do titular do certificado>
Surname	SN	<Nomes de familia do titular do certificado>
GivenName	givenName	<Nomes próprio do titular do certificado>
Email	eMail	<Email do titular associado ao certificado>

4.1.1.2 Certificado Qualificado de Selo Electronico

[1] NIC – Nº Identificação Civil; PAS – Passaporte

Atributo	Codigo	Valor
Country	C	<Pais da nacionalidade da Organização>
Organization	O	<Nome da Organização tal como registada pelas autoridades oficais competentes>
Organization Unit	OU	Selo Electronico – Assinatura Qualificada
Organization Unit	OU (opcional)	<Area/Departamento da Organização>
Organization Identifier	OI	<VAT>[2] <codigo pais>- <nº identificação fiscal>
Common Name	CN	<Nome da organização pela qual é conhecida>
Email	eMail	<Email do titular>

4.1.1.3 Certificado de Autenticação Pessoa Singular

Atributo	Codigo	Valor
Country	C	<País da nacionalidade do titular do certificado>
Organization	O (opcional)	<Organização à qual o titular do certificado pertence>
Organization Unit	OU	<Certificado para pessoa singular – Autenticação>
Organization Unit	OU (opcional)	<Área/Departamento da Organização à qual o titular do certificado pertence>
Common Name	CN	<Nome do titular do certificado>
Surname	SN	<Nomes de familia do titular do certificado>
GivenName	givenName	<Nomes próprios do titular do certificado>
Email	eMail	<Email do titular>
Serial Number	serialNumber	<Corresponde ao NIF do titular>

[2] VAT – Numero de identificação fiscal da pessoa colectiva

4.1.1.4 Certificado Qualificado de Autenticação Web

Atributo	Codigo	Valor
Country	C	<País >
Organization	O	<Nome da Organização >
Organization Unit	OU (opcional)	<Area/Departamento da organização a qual o CN pertence>
Common Name	CN	<Fully Qualified Domain Name do Servidor Web>
Street		<Morada Postal da Organização)
Locality	L	<Local de residencia da Oragnização>
State or Province	ST	<Distrito, estado, ilha >
PostalCode	(opcional)	<Codigo Postal>
Serial Number	serialNumber	<Corresponde ao NIF do titular>
Subject Business Category Field	subjectBCField	<Setor de atividade da organização. Valores possíveis são: "Private" “Government Entity” “Business Entity” “Non-Commercial Entity”>

4.1.2 USO DO CERTIFICADO E PAR DE CHAVES PELO TITULAR

O Commom Name define o titular do certificado, sendo que para o Certificado Qualificado de Assinatura Digital, este assume a identificação de uma pessoa singular e para o Certificado Qualificado de Selo Eletrónico, o nome de uma pessoa coletiva.

Os certificados de assinatura qualificada associam os dados de validação da assinatura eletróncia a uma pessoa singular enquanto os certificados, qualificado de selo eletrónico e autenticação Web fazem esta associação a uma pessoa coletiva, garantindo a origem, a integridade e confidencialidade dos dados bem assim a titularidade do dominio.

Os certificados emitidos segundo esta política são equivalentes a certificados digitais qualificados, nos termos, do definido na Legislação Caboverdiana e normativos internacionais, aplicável para o efeito.

4.2 VALIDAÇÃO DA IDENTIDADE NO REGISTO INICIAL

A SISPCA01 é responsavel por validar a identidade das entidades candidatas à obtenção de um certificado.

Os Certificados Qualificado de Assinatura Digital e Autenticação são emitidos para pessoas singulares (pessoa natural), sendo estes os responsáveis pela sua utilização. Os Certificados Qualificados de Selo Eletrónico e de Autenticação Web são emitidos para uma Organização (pessoa legal), tendo associado, mas não representado no certificado, uma pessoa singular identificada como "responsável técnico", que terá a responsabilidade de manusear e utilizar o certificado em nome da organização.

4.2.1 MÉTODO DE COMPROVAÇÃO DA POSSE DE CHAVE PRIVADA

O par de chaves e certificado é fornecido em token criptográfico (SmartCard ou token USB) com chip criptográfico, personalizado fisicamente para o titular. A posse da chave privada é garantida pelo processo de emissão e personalização do token criptográfico, garantindo que:

- O par de chaves é gerado no HSM criptográfico e inserido no token criptográfico, por comunicação direta segura e sem ficar registado em qualquer dispositivo,
- O token criptográfico é personalizado para o titular do mesmo,
- A chave pública é enviada à SISP para emissão do certificado digital correspondente, sendo este também inserido no token criptográfico.
- O token criptográfico, é entregue presencialmente.

No caso de emissão de certificados qualificado de Selo Eletrónico e Autenticação Web existe ainda a opção da chave ser gerada pelo Responsável indicado pela pessoa coletiva (Organização) num HSM próprio. Neste caso:

- O responsável e respetiva organização assume a responsabilidade pela chave gerada e pelo HSM utilizado para o efeito;
- Faz chegar à SISP toda a documentação necessária acompanhada de um CSR SHA256;
- O certificado, após validação da documentação entregue, é devolvido ao responsável.

4.2.2 VALIDAÇÃO DA IDENTIDADE DE UMA PESSOA SINGULAR

O processo de autenticação da identidade de uma pessoa singular deve obrigatoriamente garantir que a pessoa para quem vai ser emitido o certificado é quem na realidade diz ser.

Entre as operações a realizar para atingir este objetivo contam-se:

1. Verificar em documentos oficialmente reconhecidos pelo Estado e que contenha uma fotografia:
    a. O nome completo do subscitor;
    b. O número de identificação único legal;
    c. Os dados de contato, incluindo o endereço caso esteja presente;
2. Garantir a presença física do subscritor no momento da realização do registo, a não ser que já exista uma relação de confiança previamente baseada nessa presença física do subscritor;
3. Verificar, em caso de certificados de qualidade, que o candidato tem direito a tais atributos ou privilégios.

4.2.3 VALIDAÇÃO DA IDENTIDADE DE UMA PESSOA COLECTIVA

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 ou legalmente, representam essa pessoa colectiva.
Da documentação que serve de base à emissão do certificado qualificado de selo electronico, deve conter entre outros os seguintes elementos:

a) Documentos, para efeitos de identificação da pessoa colectiva e sua denominação legal, p.e. certidão comercial;

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 comprovados notarialmente;

d) Nome completo, NIF, número de bilhete de identidade ou qualquer outro documento que permita a identificação inequívoca do responsável técnico designado pelo responsável legal da organização e comprovados notarialmente.

Endereço e outras formas de contacto. Não são aceites endereços de emails de serviços gratuitos tais como gmail, hotmail ou outro semelhante.

A validação dos requerentes é efectuada utilizadando os mesmos documentos constantes das alíneas a) b) e c) atrás mencionados.

Adicionalmente é feita a confirmação do pedido de emissão do certificado através de uma chamada para o número do responsável técnico indicado no formulário.

4.2.4 INFORMAÇÃO DE SUBSCRITOR/TITULAR NÃO VERIFICADA

A SISP reserva o direito de rejeitar o pedido de emissão de certificado se o processo de validação descrito nos pontos 4.2.2 e 4.2.3 não estiverem conformes.

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

Qualquer entidade pode solicitar a revogação de um determinado certificado, havendo conhecimento ou suspeita de compromisso da chave privada do titular ou qualquer outro ato que recomende esta ação, designadamente

- O titular do certificado no caso de certificados de pessoa singular
- O(s) representante(s) legal(ais) da entidade que possa atestar a qualidade do titular do certificado, aposta no certificado digital, sempre que essa qualidade deixe de ser válida
- Parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferentes dos

previstos.

Para o efeito deve-se proceder ao preenchimento do formulário próprio do qual deve constar os seguintes elementos:

- Nome ou designação legal do titular;
- Número de pessoa coletiva, sede, objeto social, nome dos titulares dos corpos sociais e de outras pessoas com poderes para a obrigarem e número de matrícula na conservatória do registo comercial ou/e nome completo, número do bilhete de identidade ou qualquer outro elemento que permita a identificação inequívoca da entidade (ou seu representante) que inicia o pedido de revogação
- Endereço e outras formas de contacto
- Indicação do motivo para revogação do certificado

O processo de identificação e autenticação para pedido de revogação de certificado de pessoa singular ou pessoa coletiva, é efetuado através de um dos seguintes métodos:

- Assinatura digital qualificada do formulário,
- Assinatura manuscrita do formulário com entrega do mesmo, pelo subscritor, nas instalações da SISP S.A, sitas na Praia ou das ER's por esta designada.
- Assinatura manuscrita do formulário com reconhecimento notarial da assinatura.

As ERs da SISPCA01 guardam toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efetua o pedido de revogação do certificado de assinatura digital qualificada.

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.

Os perfis de certificados da SISPCA01 estão 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) ETSI TS 102 042 V2.4.1
d) CAB Forum Baseline Requirements
e)
f) 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 DE CERTIFICADO QUALIFICADO DE ASSINATURA PESSOA SINGULAR

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 Interbancaria e Sistemas de Pagamentos"		
	Common Name (CN)		"Entidade Certificadora da SISP <nn>"		
	Validity	4.1.2.5		m	
	Not Before		<data de emissão>		
	Not After		<data de emissão + n anos>		Validade Maxima = 2 anos.
	Subject	4.1.2.6		m	
	Country (C)		"CV"	m	
	Organization (O)		<Organização a qual o titular do certificado pertence>	o	
	Organization Unit (OU)		"Certificado para pessoa singular - Assinatura Qualificada"	m	
	Organization Unit (OU)		<Area/Departamento da organização a qual o titular do certificado pertence>	o	
	Locality (L)		<Localidade de residência de Titular>	o	
	State or Province (ST)		<Distrito, estado, ilha de residência do titular>	o	
	Title (title)		<Qualidade do titular do certificado, no âmbito da sua utilização para assinatura digital qualificada>	o	Opcional. Somente em caso de qualidade profissional
	TaxID Number (taxIDNumber)		<Número de Identificação Fiscal do Titular>	m	
	Serial Number (serialNumber)		<NIC ou PAS>[1] <codigo pais>- <nº identificação>	m	
	Common Name (CN)		<nome do titular do certificado>	m	
	Surname (SN)		<Nomes de familia do titular do certificado>	m	
	Given Name (givenName)		<Nomes próprio do titular do certificado>	m	
	e-mail		<email do titular>	m	

	Select Public Key Info Algorithm subjectPublicKey	4.1.2.7	 1.2.840.113549.1.1.1 <Chave Pública com modulus n de 4096bits>	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	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-l	m	 O key Identifier é composto pela hash de 160-bit SHA-l do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>
	Subject Key Identifier	4.2.1.2	O key Identifier é composto pela hash de 160-bit SHA-l	m	O key Identifier é composto pela hash de 160-bit SHA-l do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>
	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 "1" seleccionado "1" seleccionado "0" seleccionado "0" seleccionado "0" seleccionado "0" seleccionado "0" seleccionado "0" seleccionado	mc	Esta extensão é marcada CRÍTICA
	Cerificate Policies policyIdentifier	4.2.1.4	 2.16.132.1.2.2.3.2	o m	 Identificador da Politica de Certificado da SISP CA

	policyQualifiers		<policyQualifierID> cPSuri: https://pki.sisp.cv	o	Descrição do OID: "O atributo cPSuri contém um apontador para a Politica de Certificados publicada pela SISP CA. O apontador está na forma de um URL."
	policyIdentifier policyQualifiers		2.16.132.1.3.2.3.2 <policyQualifierID> cPSuri: https://pki.sisp.cv	o o	Identificador da Declaração de Praticas de Certificação O atributo cPSuri contém um apontador para Declaração de Praticas de Certificação publicada pela SISP CA. O apontador está na forma de um URL.
	Extended Ket Usage KeyPurposeId	4.2.1.12	id-kp-emailProtection	o	OID: 1.3.6.1.5.5.7.3.4
	CRLDistributionPoints distributionPoint	4.2.1.13	http://crl.sisp.cv/sispca.crl	o o	URL para aceder a CRL
	Qualified Certificate Statement id-qcs-pkixQCSyntax-v2 id-qcs-pkixQCSyntax-v2 id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcCompliance="0.4.0.1862.1.1" id-etsi-qcs-QcSSCD="0.4.0.1862.1.4" id-etsi-qcs-QcType="0.4.0.1862.1.6.1"		Declaração efectuada pela EC da PKI da SISP, indicando que este certificado é emitido de acordo com o ETSI TS 101 862 Declaração efectuada pela EC da PKI da SISP, indicando que este certificado é emitido de acordo com a politica SSCD, conforme ETSI TS 101 862 Declaração efectuada pela EC da PKI da SISP, indicando que este certificado é de assinatura qualificada
	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 o o	Valor do OID: (id-ad-ocsp) URL para aceder ao OCSP
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha256WithRSAEncryption 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 PERFIL DE CERTIFICADO QUALIFICADO DE SELO ELECTRONICO

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 Interbancaria e Sistemas de Pagamentos"		
	Common Name (CN)		"Entidade Certificadora da SISP <nn>"		
	Validity	4.1.2.5		m	
	Not Before		<data de emissão>		
	Not After		<data de emissão + nanos>		Validade Maxima = 2 anos.
	Subject	4.1.2.6		m	
	Country (C)		"CV"	m	
	Organization (O)		<Nome da Organização tal como registada nas entidades competentes"	m	
	Organization Unit (OU)		"Selo Electrónico Qualificado"	m	Designação do tipo de certificado
	Organization Unit (OU)		<Area/Departamento da organização >	o	
	Organization Identifier (OI)		<numero de identificação fiscal do titular do certificado>	m	
	Common Name (CN)		<Nome da organização pela qual é conhecida>	m	
	e-mail		<email do titular>	m	Email utilizado para envio de mensagens em bulk
	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 4096bits>		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
	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-l 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-l 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 “1” seleccionado “1” seleccionado “0” seleccionado “0” seleccionado “0” seleccionado “0” seleccionado “0” seleccionado “0” seleccionado	mc	Esta extensão é marcada CRÍTICA
	Cerificate Policies policyIdentifier policyQualifiers	4.2.1.4	 2.16.132.1.2.2.3.2 <policyQualifierID> cPSuri: https://pki.sisp.cv	o m o	 Identificador da Politica de Certificado da SISP CA Descrição do OID: "O atributo cPSuri contém um apontador para a Politica de Certificados publicada pela SISP CA. O apontador está na forma de um URL."

	policyIdentifier policyIdentifier		2.16.132.1.3.2.3.2 <policyQualiflierID> cPSuri: https://pki.sisp.cv	o o	Identificador da Declaração de Praticas de Certificação O atributo cPSuri contém um apontador para Declaração de Praticas de Certificação publicada pela SISP CA. O apontador está na forma de um URL.
	Extended Ket Usage KeyPurposeId	4.2.1.12	id-kp-emailProtection		OID: 1.3.6.1.5.5.7.3.4
	CRLDistributionPoints distributionPoint	4.2.1.13	http://crl.sisp.cv/sispca.crl	o o	URL para aceder a CRL
	Qualified Certificate Statement id-qcs-pkixQCSyntax-v2 id-qcs-pkixQCSyntax-v2 id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcCompliance="0.4.0.1862.1.1" id-etsi-qcs-QcSSCD="0.4.0.1862.1.4" id-etsi-QcType="0.4.0.1862.1.6.2"		Declaração efectuada pela EC da PKI da SISP, indicando que este certificado qualificado e emitido de acordo com o ETSI TS 101 862 Declaração efectuada pela EC da PKI da SISP, indicando que este certificado é emitido de acordo com a politica SSCD, conforme ETSI TS 101 862 Declaração efectuada pela EC da PKI da SISP, indicando que este certificado é um Selo Electronico
	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 o o	Valor do OID: (id-ad-ocsp) URL para aceder ao OCSP
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha256WithRSAEncryption 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.

5.1.5 PERFIL DE CERTIFICADO AVANÇADO DE AUTENTICAÇÃO PESSOA SINGULAR

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 Interbancaria e Sistemas de Pagamentos"		
	Common Name (CN)		"Entidade Certificadora da SISP <nn>"		
	Validity	4.1.2.5		m	
	Not Before		<data de emissão>		
	Not After		<data de emissão + n anos>		Validade Maxima = 2 anos.
	Subject	4.1.2.6		m	
	Country (C)		"CV"	m	
	Organization (O)		<Nome da Organização tal como registada nas entidades competentes"	o	
	Organization Unit (OU)		"Certificado para pessoa singular - Autenticação"	m	Designação do tipo de certificado
	Title (title)		<Qualidade do titular do certificado, no âmbito da sua utilização para autenticação>	o	
	Common Name (CN)		<nome do titular do certificado>	m	
	Surname (SN)		<Nomes de familia do titular do certificado>	m	
	Given Name (givenName)		<Nomes próprio do titular do certificado>	m	
	Serial Number (serialNumber)		<Identificador único do titular do certificado>	m	Corresponde ao NIF do titular.
	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				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
	subjectPublicKey		1.2.840.113549.1.1.1 <Chave Pública com modulus n de 4096 bits>		
	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-l 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-l 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	 “1” seleccionado “0” seleccionado “0” seleccionado “0” seleccionado “0” seleccionado “0” seleccionado “0” seleccionado “0” seleccionado “0” seleccionado	mc	Esta extensão é marcada CRÍTICA
	Cerificate Policies policyIdentifier policyQualifiers	4.2.1.4	 2.16.132.1.2.2.3.2 <policyQualifierID> cPSuri: https://pki.sisp.cv	o m o	 Identificador da Politica de Certificado da SISP CA Descrição do OID: "O atributo cPSuri contém um apontador para a Politica de Certificados publicada pela SISP CA. O apontador está na forma de um URL."
	policyIdentifier		2.16.132.1.3.2.3.2	o	Identificador da Declaração de Praticas de Certificação

	policyIdentifier		<policyQualiflierID> cPSuri: https://pki.sisp.cv	o	O atributo cPSuri contém um apontador para Declaração de Praticas de Certificação publicada pela SISP CA. O apontador está na forma de um URL.
	Extended Ket Usage Client Authentication	4.2.1.12	1.3.6.1.5.5.7.3.2		
	CRLDistributionPoints distributionPoint	4.2.1.13	http://crl.sisp.cv/sispca.crl	o o	URL para aceder a CRL
	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 o o	Valor do OID: (id-ad-ocsp) URL para aceder ao OCSP
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha256WithRSAEncryption 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.

5.1.5 PERFIL DE CERTIFICADO QUALIFICADO DE AUTENTICAÇÃO WEB

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	1.2.840.113549.1.1.11	m	Valor TEM que ser igual ao OID no signatureAlgorithm (abaixo)
	Issuer	4.1.2.4		m	
	Country (C)		"CV"		
	Organization (O)		"ICP-CV"		
	Organization Unit (OU)		"SISP-Sociedade Interbancaria e Sistemas de Pagamentos"		
	Common Name (CN)		"Entidade Certificadora da SISP <nn> "		Designação Oficial da SISPCA da SISP
	Validity	4.1.2.5		m	TEM que utilizar tempo UTC até 2049, passando a partir daí a utilizar *GeneralisedTime*
	Not Before		<data de emissão>		
	Not After		<data de emissão + 1 anos>		Validade maxima de 1 ano.
	Subject	4.1.2.6		m	
	Country (C)		<País>	m	
	Organization (O)		<Nome da Organização >	m	
	Common Name (CN)		<Fully Qualified Domain Name do Servidor Web>	m	
	Organization Unit (OU)		<Area/Departamento da organização a qual o CN pertence>	o	
	Street		<Morada da Organização>	m	
	Locality (L)		<Localidade >	m	
	State or Province (ST)		<Distrito, estado, ilha >	m	
	PostalCode		<Codigo Postal>	o	
	Serial Number (serialNumber)		<Identificador único da organização>	m	De acordo com o documento Guidelines for the Issuance and Management Of Extended Validation Certificates capítulo 9.2.6: Subject:serialNumber

	Subject Business Category Field		<Setor de atividade da organização. Valores possíveis são: Private" "Government Entity" "Business Entity" "Non-Commercial Entity">	m	De acordo com o documento Guidelines for the Issuance and Management Of Extended Validation Certificates capítulo 9.2.4: subject:businessCategory
	Select 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	4.1.2.8		m	
	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	 "1" seleccionado "0" seleccionado "1" seleccionado "1" seleccionado "0" seleccionado "0" seleccionado "0" seleccionado "0" seleccionado "0" seleccionado	mc	Esta extensão é marcada CRÍTICA

	Cerificate Policies policyIdentifier policyQualifiers	4.2.1.4	 2.16.132.1.3.2.3.2 <policyQualifierID> cPSuri: https://pki.sisp.cv	m m m	 Identificador da Declaração de Praticas de Certificação O atributo cPSuri contém um apontador para Declaração de Praticas de Certificação publicada pela SISP CA. O apontador está na forma de um URL.
	policyIdentifier policyQualifiers		2.16.132.1.2.2.3.2 <policyQualifierID> cPSuri: https://pki.sisp.cv	m m	Identificador da Politica de Certificado da SISP CA Descrição do OID: "O atributo cPSuri contém um apontador para a Politica de Certificados publicada pela SISP CA. O apontador está na forma de um URL."
	policyIdentifier		<2.23.140.1.1>	m	Identificador da Politica de Certificados do CA/B Forum para os cetificados Extended Validation
	CRLDistributionPoints distributionPoint	4.2.1.13	 http://crl.sisp.cv/sispca.crl	m m	 URL para aceder a CRL
	Extended Key Usage Server Authentication Client Authentication	4.2.1.12	 1.3.6.1.5.5.7.3.1 1.3.6.1.5.5.7.3.2	 mc mc	 Server Autentication Client Autentication
	Qualified Certificate Statement id-qcs-pkixQCSyntax-v2 id-qcs-pkixQCSyntax-v2		 id-etsi-qcs-QcCompliance="0.4.0.1862.1.1" id-etsi-qcs-QcType="0.4.0.1862.1.6.3"	 m m	 Certificado para Autenticação WEB
	Internet Certificate Extensions				.
	Authority Information Access accessMethod accessLocation	4.2.2.1	 1.3.6.1.5.5.7.48.1 http://ocsp.sisp.cv/	m	 Valor do OID: (id-ad-ocsp) URL para aceder ao OCSP
	Signature Algorithm 4.1.1.2		 1.2.840.113549.1.1.11	 m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha256WithRSAEncryption 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.

5.1.6 PERFIL DE CERTIFICADO QUALIFICADO DE FATURA ELETRONICA

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 Interbancaria e Sistemas de Pagamentos"		
	Common Name (CN)		"Entidade Certificadora da SISP <nn>"		
	Validity	4.1.2.5		m	
	Not Before		<data de emissão>		
	Not After		<data de emissão + n anos>		Validade Maxima = 2 anos.
	Subject	4.1.2.6		m	
	Country (C)		"CV"	m	
	Organization (O)		<Nome da Organização tal como registada nas entidades competentes"	m	
	Organization Unit (OU)		"Fatura Eletronica"	m	Designação do tipo de certificado
	Organization Unit (OU)		<Area/Departamento da organização >	o	
	Organization Identifier (OI)		<número de identificação fiscal do titular do certificado>	m	
	Common Name (CN)		<Nome da organização pela qual é conhecida>	m	
	e-mail		<email do titular>	m	Email utilizado para envio de mensagens em bulk
	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				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
	subjectPublicKey		1.2.840.113549.1.1.1 <Chave Pública com modulus n de 4096bits>		
	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-l 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-l 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 “1” seleccionado “1” seleccionado “0” seleccionado “0” seleccionado “0” seleccionado “0” seleccionado “0” seleccionado “0” seleccionado	mc	Esta extensão é marcada CRÍTICA
	Cerificate Policies policyIdentifier	4.2.1.4	 2.16.132.1.2.2.3.2	o m	 Identificador da Politica de Certificado da SISP CA

	policyQualifiers		<policyQualifierID> cPSuri: https://pki.sisp.cv	o	Descrição do OID: "O atributo cPSuri contém um apontador para a Politica de Certificados publicada pela SISP CA. O apontador está na forma de um URL."
	policyIdentifier policyIdentifier		2.16.132.1.3.2.3.2 <policyQualifierID> cPSuri: https://pki.sisp.cv	o o	Identificador da Declaração de Praticas de Certificação O atributo cPSuri contém um apontador para Declaração de Praticas de Certificação publicada pela SISP CA. O apontador está na forma de um URL.
	Extended Ket Usage KeyPurposeId	4.2.1.12	id-kp-emailProtection		OID: 1.3.6.1.5.5.7.3.4
	CRLDistributionPoints distributionPoint	4.2.1.13	http://crl.sisp.cv/sispca.crl	o o	URL para aceder a CRL
	Qualified Certificate Statement id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcCompliance="0.4.0.1862.1.1"		Declaração efectuada pela EC da PKI da SISP, indicando que este certificado qualificado e emitido de acordo com o ETSI TS 101 862
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcSSCD="0.4.0.1862.1.4"		Declaração efectuada pela EC da PKI da SISP, indicando que este certificado é emitido de acordo com a politica SSCD, conforme ETSI TS 101 862
	id-qcs-pkixQCSyntax-v2		id-etsi-QcType="0.4.0.1862.1.6.2"		Declaração efectuada pela EC da PKI da SISP, indicando que este certificado é um Selo Electronico
	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 o o	 Valor do OID: (id-ad-ocsp) URL para aceder ao OCSP
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha256WithRSAEncryption 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.

5.1.6 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 (sha256WithRSAEncryption).

5.1.7 FORMATO DE NOMES

Tal como definido na secção 4.1.

5.1.8 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.

5.1.9 OID DA POLÍTICA DE CERTIFICADOS

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

5.1.10 UTILIZAÇÃO DA EXTENSÃO POLICY CONSTRAINTS

Nada a assinalar.

5.1.11 SINTAXE E SEMÂNTICA DO QUALIFICADOR DE POLÍTICA

A extensão "certificate policies" contém um tipo de qualificador de política a ser utilizado pelos emissores dos certificados e pelos escritores da política de certificados. O tipo de qualificador é o "cPSuri" que contém um apontador, na forma de URL, para a Declaração de Práticas de Certificação publicada pela EC e, um apontador, na forma de URL, para a Politica de Certificados.

5.1.12 SEMÂNTICA DE PROCESSAMENTO PARA A EXTENSÃO CRÍTICA CERTIFICATE POLICIES

Nada a assinalar.

5.2 CERTIFICADO "ESPÉCIMEN"

Os certificados "espécimen" poderão ser emitidos sempre que seja necessário validar o perfil, o processo de emissão e/ou a sua utilização. O certificado de "espécimen" pode ser emitido para efeito de testes tendo por base um contrato de responsabilidade a celebrar entre a SISP e a Entidade requerente.
Este certificado difere dos certificados usuais, considerados finais no seguinte:

- Perfil de certificado: é adicionado o prefixo "(espécimen)" ao CommonName (CN);
- Emissão do certificado: de acordo com formulário específico para usos internos;

È obrigatoria a presença de Auditor e do Administrador de Segurança na emissão de certificados "espécimen".

5.3 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 caboverdiana.

5.3.1 NÚMERO DE VERSÃO

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

5.3.2 PERFIL DA CRL DA SISPCA01

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	1.2.840.113549.1.1.11	m	Contém o identificador do algoritmo utilizado para assinar a CRL. O valor TEM que ser igual ao OID no campo signatureAlgorithm (abaixo)
	Issuer Country (C) Organization (O) Organization Unit (OU) Common Name (CN)	5.1.2.3	"CV" "ICP-CV" "SISP-Sociedade Interbancaria e Sistemas de Pagamentos" "Entidade Certificadora da SISP <nn> "	m	<nn > - Número de SubCA
	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 CLR = 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 24 horas.
	revokedCertificates	5.1.2.6	<lista de certificados revogados>	m	
	CRL Extensions	5.1.2.7		m	
	Authority Key Identifier KeyIdentifier	5.2.1	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)>	o	
	CRL Number	5.2.3	<número sequencial único e incrementado>	m	
	CRL Distribuition Point DistributionPointName	5.2.5	http://crl.sisp.cv/sispca.crl	c	
	CRL Entry Extensions	5.3			

	Reason Code	5.3.1		o	Valor tem que ser um dos seguintes: 1 – keyCompromise 2 – cACompromise 3 – affiliationChanged 4 – superseded 5 – cessationOfOperation 6 – certificateHold 8 – removeFromCRL 9 – privilegeWithdrawn 10 - Compromise
	Signature Algorithm	5.1.1.2	1.2.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha256WithRSAEncryption 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.

5.4 PERFIL DE CERTIFICADO DE OCSP

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. Essa confiança é dada através do uso de certificados digitais X.509 v3, que são estrutura de dados que fazem a ligação entre a chave pública e o seu titular. Esta ligação é garantida através da assinatura digital de cada certificado por uma EC de confiança. A EC pode basear esta afirmação em meios técnicos (por exemplo, prova de posse da chave privada através de um protocolo desafio-resposta), na apresentação da chave privada, ou no registo efetuado pelo titular.

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

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

O perfil dos Certificados de Validação on-line OCSP está de acordo com:

a) Recomendação ITU.T X.509;
b) RFC 5280 e
c) Outras normas e legislação aplicável.

5.4.1 NÚMERO DE VERSÃO

O campo “version” do certificado descreve a versão utilizada na codificação do certificado. Neste perfil, a versão utilizada é a 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 OCSP DA SISPCA01

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 Country (C) Organization (O) Organization Unit (OU) Common Name (CN)	4.1.2.4	 "CV" "ICP-CV" "SISP-Sociedade Interbancaria e Sistemas de Pagamentos" <nome>	m	 nome da subCA da SISP
	Validity Not Before Not After	4.1.2.5	 <data de emissão> <data de emissão + 5,4 anos>	m	TEM que utilizar tempo UTC até 2049, passando a partir daí a utilizar *GeneralisedTime* Validade de 5 anos e 4 meses
	Subject Country (C) Organization (O) Organization Unit (OU) Organization Unit (OU) Common Name (CN)	4.1.2.6	 "CV" "ICP-CV" "Validação Online" "SISP-Sociedade Interbancaria e Sistemas de Pagamentos" "Serviço de Validação Online da SISPCA01 <nnnn>"	m	 <nnn> - sequencia do certificado
	Select 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
	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-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 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	 "1" seleccionado "1" seleccionado "0" seleccionado "0" seleccionado "0" seleccionado "0" seleccionado "0" seleccionado "0" seleccionado "0" seleccionado	mc	Esta extensão é marcada CRÍTICA
	Cerificate Policies policyIdentifier policyQualifiers	4.2.1.4	 2.16.132.1.2.2.3.2 <policyQualifierID> cPSuri: https://pki.sisp.cv	o m o	 Identificador da Politica de Certificado da SISP CA Descrição do OID: "O atributo cPSuri contém um apontador para a Politica de Certificados publicada pela SISP CA. O apontador está na forma de um URL."
	policyIdentifier policyIdentifier		2.16.132.1.3.2.3.2 <policyQualifierID> cPSuri: https://pki.sisp.cv	o o	Identificador da Declaração de Praticas de Certificação O atributo cPSuri contém um apontador para Declaração de Praticas de Certificação publicada pela SISP CA. O apontador está na forma de um URL.
	Extended Ket Usage OCSPSigner	4.2.1.12	 1.3.6.1.5.5.7.3.9	 c	 Descrição do OID: Indica que a chave privada correspondente ao certificado X.509 pode ser utilizada para assinar respostas OCSP.

	OCSPNocheck		NULL	o	Não é uma extensão definida no RFC 3280. Definida em http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.48.1.5 html., esta extensão deve ser incluída num certificado de assinatura OCSP. Esta extensão indica ao cliente OCSP que este certificado de assinatura pode ser confiável, mesmo sem validar junto do servidor OCSP (já que a resposta seria assinada pelo servidor OCSP e o cliente teria que novamente validar o estado do certificado de assinatura).
	Internet Certificate Extensions				.
	Authority Information Access	4.2.2.1		o	Esta extensão TEM de ser crítica1.
	accessMethod		1.3.6.1.5.5.7.48.1.2	o	Valor do OID: (id-ad-ocsp)
	accessLocation		http://ocsp.sisp.cv	o	URL para aceder ao OCSP
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha256WithRSAEncryption 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 pedido de certificado deve ser formulado, mediante o preenchimento do Formulario proprio, disponivel no sítio da internet sa SISP ou aos balcões das ER's.

Os certificados qualificados de assinatura digital ou autenticação podem ser subscritos:

- Pelo Titular do certificado, quando o certificado é emitido para pessoa natural,
- Pelo Titular e Representantes legais da entidade, quando o certificado é emitido para pessoa singular associada a uma entidade (na qualidade ou em representação).

Os Certificados Qualificado de Selo Eletrónico e de Autenticação Web podem ser subscritos:

- Pelos representantes legais da pessoa coletiva com poderes para o ato, sendo designado por estes uma pessoa física, responsável pelo manuseamento e operação do certificado, denominada de "responsável técnico".

6.1.2 PROCESSO DE REGISTO E RESPONSABILIDADES

O pedido de certificado qualificado é da responsabilidade dos intervenientes, identificados na secção anterior, assim como é da sua responsabilidade a veracidade dos dados fornecidos e disponibilização de toda a documentação necessária que a permita verificar.

O processo de registo é considerado efetivo após ser verificada e confirmada toda a informação constante no pedido, pela SISP ou ER designada

O processo de registo inicia-se com o preenchimento do formulário disponível no site da SISP ou aos balcões da ER designada.

6.2 PROCESSAMENTO DO PEDIDO DE CERTIFICADO

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

a) Receção e verificação de toda a documentação e autorizações exigidas;

b) Verificação da identidade do requisitante;

c) Verificação da exatidão e integridade do pedido de certificado;

d) Pedido de emissão de certificado dirigido à SISP CA

As secções 4.2, 6.2.1 e 6.3 descrevem detalhadamente todo o processo.

6.2.1 PROCESSOS PARA A IDENTIFICAÇÃO E FUNÇÕES DE AUTENTICAÇÃO

6.2.1.1 Certificado Pessoa Singular
Conforme indicado na secção 4.2

6.2.1.2 Certificado Pessoa Colectiva
Conforme indicado na secção 4.2

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 realizada automaticamente, pela plataforma da SISP CA, após o registo e validação do pedido de certificado, sendo que a chave privada é gerada no cartão (ou token USB) com chip criptográfico ou pelo titular através do CSR.

6.3.2 NOTIFICAÇÃO DA EMISSÃO DO CERTIFICADO AO TITULAR
O titular do certificado considera-se notificado da emissão do certificado aquando da receção do mesmo.

6.4 ACEITAÇÃO DO CERTIFICADO

6.4.1 PROCEDIMENTOS PARA A ACEITAÇÃO DO CERTIFICADO

O certificado considera-se aceite após a recepção do mesmo.

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.
d) 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 SISPCA01 não publica os certificados emitidos, disponibilizando-o integralmente ao titular, nas condições definidas no ponto 6.4.1.

6.4.3 NOTIFICAÇÃO DA EMISSÃO DE CERTIFICADO A OUTRAS ENTIDADES

Nada a assinalar.

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 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, os certificados suspensos podem recuperar a sua validade.

6.7.1 MOTIVOS PARA A SUSPENSÃO

A SISPCA01não suspende certificados.

6.7.2 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

- Perda ou roubo do cartão/token;
- Actualização/alteração de dados;
- Deterioção do cartão/token;
- Qualidade do titular do certificado, aposta no certificado digital, deixa de ser válida;
- Poderes de representação inscritos no certificado sejam suspensos ou alterados;
- Utilização do certificado para atividades abusivas;
- Falha na utilização do cartão/token;
- 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 SISPCA01guarda 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 de certificados.

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. ou às Entidades de Registo 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 aprova ou recusa o pedido;
- 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 SISPCA01disponibiliza uma nova CRL Base diariamente.

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 60 minutos.

6.7.13 DISPONIBILIDADE DE VERIFICAÇÃO ONLINE DO ESTADO / REVOGAÇÃO DE CERTIFICADO

A SISPCA01dispõe de serviços de validação OCSP do estado dos certificados online. Esse serviço poderá ser acedido em http://ocsp.sisp.cv.

O período máximo entre a revogação e a disponibilização através do serviço de validação OCSP, não deverá ultrapassar os 30 minutos.

6.7.14 REQUISITOS DE VERIFICAÇÃO ONLINE DE REVOGAÇÃO

As partes confiantes deverão dispor de software capaz de operar o protocolo OCSP, de forma a obter a informação sobre o estado do certificado.

6.7.15 OUTRAS FORMAS DISPONÍVEIS PARA DIVULGAÇÃO DE REVOGAÇÃO

O titular do certificado é notificado, sempre que o certificado for revogado.

6.7.16 REQUISITOS ESPECIAIS EM CASO DE COMPROMETIMENTO DE CHAVE PRIVADA

No caso da chave privada da SISPCA01 ser comprometida, devem ser tomadas medidas apropriadas de resposta ao incidente.

As respostas a esse incidente podem incluir:

- Revogação do certificado da SISPCA01e de todos os certificados emitidos no “ramo” da hierarquia de confiança da SISP CA;
- Notificação da Autoridade Credenciadora e todos os titulares de certificados emitidos no “ramo” da hierarquia de confiança da SISP CA;
- Geração de novo par de chaves para a SISP CA;

- Renovação de todos os certificados emitidos no “ramo” da hierarquia de confiança da SISP CA.

7. AUDITORIAS E NORMAS DE SEGURANÇA

Descrito nas secções 7, 8 e 4.3 da Declaração de Práticas de Certificação disponível em https://pki.sisp.cv.

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