SOCIEDADE INTERBANCÁRIA E SISTEMAS DE PAGAMENTOS

SISP ROOT CA02 - PC

Código:	PLRC012
Versão:	01
Data da versão:	14/06/2022
Criado por:	SISP
Aprovado por:	Diretor Geral - Jair Silva
Nível de confidencialidade:	Publico

Histórico das alterações

Data	Versão	Criado por	Descrição da alteração
14/06/2022	01	Ruben Veiga	Criação do documento

Índice

ÍNDICE TABELAS

1. Introdução

- **Âmbito**

O presente documento é uma Politica de Certificado e tem como objetivo informar as práticas gerais de emissão e gestão de certificados, seguidas pela Entidade de Certificação Raíz SISPRootCA02 , enquanto prestador de serviços de confiança qualificados no âmbito do *CAB Forum "Baseline for Issuance and Mangement of Publicly-Trusted Certificates" e eIDAS Regulation No. 910/2014*, no suporte à sua atividade de certificação digital

Este documento pode sofrer atualizações regulares.

- **Público-alvo**

Este documento é público e destina-se a todos quantos se relacionam com a Entidades de Certificação Entidade de Certificação Raíz SISPROOTCA02 doravante designada de SISPROOTCA02.

Os certificados emitidos pela SISPROOTCA02 contêm uma referência à presente PC, Código de documento nºPLRC00X.01, de modo a permitir que Partes confiantes e outras pessoas interessadas, possam encontrar informação sobre o certificado e sobre a entidade que o emitiu.

- **Estrutura do Documento**

Este documento segue a estrutura definida e proposta pelo grupo de trabalho PKIX do IETF, no documento RFC 3647. Assume-se que o leitor está familiarizado com os conceitos de criptografia, infraestruturas de chaves publicas e assinaturas eletrónicas. Não sendo o caso recomenda-se o estudo prévio dos referidos tópicos para melhor compreensão do conteúdo. O documento está estruturado em 9 capítulos sendo os 7 primeiros reservados aos procedimentos e praticas de certificação utilizadas pela PKI da SISP e os restantes dois dedicados à Auditoria/*Compliance* e questões legais, respetivamente.

1.1.Contexto Geral

Esta PC especifica os requisitos de segurança, políticas e praticas utilizadas pela SISPROOTCA02 na sua atividade de certificação digital e está de acordo 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) *eIDAS Regulation No.910/2014*
d) *CA –Browser-Forum Baseline Requirements 1.8.4*
e) *ETSI TS 119 312 - Electronic Signatures and Infrastructures (ESI): Cryptographic Suites*

1.2.Designação e Identificação do Documento

Este documento é uma PC que é representada num certificado através de um número único designado de "identificador de objeto" (OID), sendo o valor do OID associado a este documento, 1.3.6.1.4.1.4146.1.60.

Este documento é identificado pelos dados constantes na seguinte tabela:

Tabela 1: Informação do documento

INFORMAÇÃO DO DOCUMENTO	
Nome do Documento	Política de Certificado da SISPROOTCA02
Versão do Documento	Versão 1.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.4146.1.60
Data de Emissão	14/06/2022
Validade	13/06/2023
Localização	http://pki.sisp.cv/

São efetuadas atualizações ao documento, sempre que se justificar.

1.2.1. Revisões

Versão	Criação	Aprovação	Motivo da Revisão
1.0	14/06/2022	15/06/22	Criação
	Administrador de Segurança	Grupo de Gestão	
	Ruben Veiga	Jair Silva	

1.2.2. Histórico do documento

Tabela 2: Histórico do documento

Data	Versão	Criado por	Descrição da alteração
14/06/2022	1.0	Ruben Veiga	Criação do documento

1.3.Participantes na Infraestrutura de Chave Pública

A SISP, enquanto Entidade Gestora da PKI da SISP, cumpre as disposições previstas nas normas e legislação aplicável, assumindo as competências aí descritas sendo responsável por fornecer serviços e assegurar os procedimentos que possam garantir as funcionalidades a seguir indicadas:

1. Geração dos pares de chaves criptográficas associadas a cada uma das Entidades Certificadoras;

2. Receção e validação dos pedidos de emissão de certificados realizados pelas Entidades de Certificação (EC`s) Subordinadas bem como os demais subscritores;

3. Emissão de certificados, relativos a pedidos de certificados que estejam de acordo com o formato requerido pelas Entidades de Certificação da SISP;

4. Receção e validação dos pedidos de suspensão e revogação de certificados;

5. Publicação dos certificados (quando, onde e se apropriado) e de informação acerca do seu estado;

6. Assegurar a contínua disponibilidade da informação pública, para todos os seus utilizadores;

A PKI da SISP é composta pelas seguintes EC's:

- SISP *Root Certification Authority 02 (SISP Root CA02)*
- SISP QWAC Certification Authority (SISP QWAC)

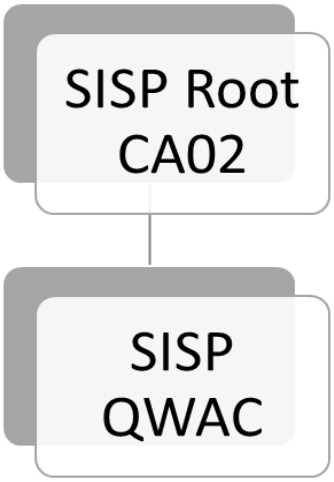

Figura 1: Composição PKI da SISP

1.3.1. Entidades de Certificação

- **SISP Root Certification Authority 02 (SISP Root CA02)**

É uma entidade certificadora de raiz auto-assinada, estando habilitada a emitir certificados para assinatura de entidades certificadoras subordinadas, podendo estas emitir certificados de autenticação web TLS/SSL qualificadas e não qualificadas, e de *code sign*.

Tabela 3: Informação do Certificado (SISP Root CA02)

INFORMAÇÃO DO CERTIFICADO	
Nome Distinto	C = CV, O = SISP, OU = SISP-Sociedade Interbancária e Sistemas de Pagamentos, CN = Entidade de Certificação Raiz da SISP 02
Algoritmo de Assinatura	sha512WithRSAEncryption
Serial Number	6f1566a98112c3fffd6a7b9c0c9bc9d062cf2293
Validade	28 de junho de 2034 06:45:00
Thumbprint	9C:D8:8D:03:09:AB:9F:63:60:73:A3:AA:28:E6:4E:F8:94:CC:A3:E6:D9:37:08:74:BA:ED:C7:1F:C9:3A:2D:1E:DB:80:B3:C8:80:9E:0A:D5:B8:F9:47:2A:A0:51:6C:9B:1E:78:AF:D8:F7:74:97:E9:D7:64:2E:5E:C2:0A:02:62
Emissor	C = CV, O = SISP, OU = SISP-Sociedade Interbancária e Sistemas de Pagamentos, CN = Entidade de Certificação Raiz da SISP 02

- **SISP QWAC *Certification Authority***

É uma entidade certificadora subordinada, assinada pela *SISP Root CA 02*, estando habilitada a emitir certificados para utilizadores finais, de acordo com a *CA/Browser Forum "Baseline for Issuance and Mangement of Publicly-Trusted Certificates" e eIDAS Regulation No. 910/2014*.

A SISP QWAC emite certificados qualificados de Autenticação *Web TLS/SSL Extended Validation(EV*) em conformidade com o *Guidelines for the issuance and management of Extended Validation Certificates da CA/Browser Forum.*

Tabela 4: Informação do certificado (SISP QWAC *Certification Authority*)

INFORMAÇÃO DO CERTIFICADO	
Nome Distinto	C = CV, O = SISP, OU = SISP-Sociedade Interbancária e Sistemas de Pagamentos, CN= SISP QWAC
Algoritmo de Assinatura	sha512WithRSAEncryption
Serial Number	77a5aacfb1eb23c603e9f429b724826dbc78add6
Validade	29 de junho de 2028 07:22:55
Thumbprint	35:6F:2C:CF:BE:F4:CE:4C:FB:17:21:B8:9D:DB:43:B1:03:F6:AC:18:00:AA:42:49:06:8F:64:3B:1B:EA:AE:9B:F5:DA:7E:10:2C:16:9B:9E:52:CD:8E:31:7D:79:DA:AC:EC:C3:4A:8A:D7:DB:B5:5C:55:15:F3:03:24:FA:7D:5D
Emissor	C = CV, O = SISP, OU = SISP-Sociedade Interbancária e Sistemas de Pagamentos, CN = Entidade de Certificação Raiz da SISP 02

1.3.2. Entidades ou Unidades de Registo

Entidades ou Unidades de Registo são entidades às quais as EC's delegam a prestação de serviços de identificação, registo de utilizadores de certificados, bem como a gestão de pedidos de renovação e revogação de certificados. A SISP poderá atuar como Unidade de Registo e/ou estabelecer acordos com entidades terceiras para que estas desempenham este papel.

- **Entidade de Registo Interna**

No âmbito da Entidade de Certificação SISPROOTCA02, a entidade de registo materializa-se pelos serviços internos da PKI da SISP que procedem ao registo e validação dos dados necessários, conforme explicitado na Política de Certificado de cada tipo de certificado emitido.

- **Entidades de Registo Externa**

A hierarquia de confiança da SISPROOTCA02, não dispõe de entidades externas de registo.

1.3.3. Titulares de Certificados

No contexto deste documento o termo subscritor/titular aplica-se a todos os utilizadores finais a quem tenham sido atribuídos certificados pela PKI da SISP.

São considerados titulares de certificados emitidos pela PKI da SISP, aqueles cujo nome está inscrito no campo "Assunto" (*Subject*) do certificado e utilizam o certificado e respetiva chave privada de acordo com o estabelecido nas diversas políticas de certificado descritas neste documento, sendo emitidos certificados para as seguintes categorias titulares:

- Pessoa física ou jurídica;
- Pessoa coletivas (Organizações);
- Serviços (computadores, servidores, domínios, etc.)
- Membros dos grupos de trabalho.

Em alguns casos, os certificados são emitidos diretamente a pessoas física ou jurídica para uso pessoal; no entanto, existem situações em que quem solicita o certificado é diferente do titular do mesmo, por exemplo, uma organização pode solicitar certificados para os seus colaboradores para que estes representem a organização em transações eletrónicas. Nestas situações a entidade que solicita a emissão do certificado é diferente do titular do mesmo.

1.3.4. Partes Confiantes

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

Nesta PC, considera-se uma parte confiante, aquela que confia no teor, validade e aplicabilidade do certificado emitido na hierarquia de confiança da PKI da SISP.

1.3.5. Outros Participantes

- **Autoridade Supervisora**

A Autoridade Supervisora assume o papel de entidade que disponibiliza serviços de auditoria/inspeção de conformidade, no sentido de aferir se os processos utilizados pela EC nas suas atividades de certificação, estão conformes, de acordo com os requisitos mínimos estabelecidos na legislação e nomas vigentes. Consideram-se como suas principais atribuições as seguintes:

a) Acreditar as entidades de certificação;

b) Auditar as entidades de certificação;

c) Avaliar as atividades desenvolvidas pelas entidades de certificação autorizadas conforme os requisitos técnicos definidos nos termos da alínea anterior;

d) Zelar pelo adequado funcionamento e eficiente prestação de serviço por parte de entidades de certificação em conformidade com as disposições legais e regulamentares da atividade.

- **Entidades Externas de Prestação de Serviços**

As Entidades que prestam serviços de suporte à PKI da SISP, têm as suas responsabilidades devidamente definidas através de contratos estabelecidos com as mesmas.

- **Auditor de Segurança**

Figura independente do círculo de influência da Entidade de Certificação, exigida pela Autoridade Supervisora. A sua missão é auditar a infraestrutura da Entidade de Certificação, no que respeita a equipamentos, recursos humanos, processos, políticas e regras, tendo que submeter um relatório anual, à Autoridade Supervisora.

1.4.Utilização do Certificado

Os certificados emitidos pela SISPROOTCA02 destinam-se em exclusivo para a assinatura de certificados das Entidades Certificadoras de nível imediatamente subsequente ao seu, de sua CRL (Lista de Certificados Revogados) e da sua OCSP, com o objetivo de garantir os seguintes serviços:

- Autenticação;
- Confidencialidade;
- Integridade;
- Privacidade;
- Autenticidade e
- Não-repudio.

Estes serviços são obtidos com recurso à utilização de criptografia de chave pública, através da sua utilização na estrutura de confiança que a PKI da SISP proporciona. Assim, os serviços de identificação e autenticação, integridade e não-repúdio são obtidos mediante a utilização de assinaturas digitais. A confidencialidade é garantida através dos recursos a algoritmos de cifra, quando conjugados com mecanismos de estabelecimento e distribuição de chaves, geridos por equipamentos criptográficos certificados. As partes confiantes podem validar a cadeia de confiança e assim garantir a autenticidade e a identidade do titular.

1.4.1. Utilização Adequada do Certificado

Os requisitos e regras definidos neste documento aplicam-se a todos os certificados emitidos pela entidade certificadora SISPROOTCA02.

Os certificados emitidos pela SISPROOTCA02 são também utilizados pelas partes confiantes para verificação da cadeia de confiança, assim como para garantir a autenticidade e identidade do emissor de um certificado de transmissão de dados na web através do protocolo TLS/SSL, a titularidade do domínio, a identidade do website/organização, a confidencialidade e a segurança na troca de informação entre o utilizador e o sítio *web*.

1.4.2. Utilização Não Autorizada

Os certificados emitidos pela SISPROOTCA02 não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente.

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

1.5.Gestão das Políticas

1.5.1. Organização e Gestão do Documento

A gestão desta PC é da responsabilidade do Grupo de Trabalho Segurança.

1.5.2. Contactos da Entidade

Tabela 5: Contatos da entidade

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

1.5.3. Entidade que garante a adequação da CPS às políticas

O Grupo de Trabalho de Segurança, determina a conformidade e aplicação interna desta PC (e/ou respetivas DPCs), submetendo-a de seguida ao Grupo de Gestão para aprovação.

1.5.4. Procedimento para Aprovação da PC

A validação desta PC (e/ou respetivas DPCs) e correções (ou atualizações) deverão ser levadas a cabo pelo Grupo de Trabalho de Segurança. Correções (ou atualizações) deverão ser publicadas sob a forma de novas versões desta PC (e/ou respetivas DPCs), substituindo qualquer PC (e/ou respetivas DPCs) anteriormente definida.

O Grupo de Trabalho de Segurança deverá ainda determinar quando é que as alterações na PC (e/ou respetivas DPCs) levam a uma alteração nos identificadores dos objetos (OID) da PC (e/ou respetivas DPCs).

Após a fase de validação, a PC (e/ou respetivas DPCs) é submetida ao Grupo de Gestão, que é a entidade responsável pela aprovação e autorização de modificações neste tipo de documentos.

1.6.Definições e Acrónimos

1.6.1. Definições

Tabela 6: Definições

Definições	
Termo	**Definição**
Assinatura Eletrónica	Dados sob forma eletrónica anexos ou logicamente associados a uma mensagem de dados e que sirvam de método de autenticação.
Assinatura Eletrónica Avançada	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 detetar toda e qualquer alteração superveniente do conteúdo deste.
Assinatura Eletrónica Qualificada	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 Supervisora	Entidade competente para a credenciação e fiscalização das Entidades de Certificação.
Certificado	Documento eletrónico que liga os dados de verificação de assinatura ao seu titular e confirma a identidade desse titular.
Certificado qualificado	Certificado de assinatura eletrónica, emitido por um prestador de serviços de confiança qualificado, nos termos da legislação de uma determinada jurisdição.
Chave Privada	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no

	documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a Correspondente chave pública.
Chave Pública	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves.
Credenciação	Ato pelo qual é reconhecido a uma entidade, que o solicite o direito ao exercício de atividade de entidade de certificação credenciada.
Dados de Criação de Assinatura	Um conjunto único de dados, como códigos ou chaves criptográficas privadas, usado pelo signatário para a criação de uma assinatura eletrónica.
Dados Verificação de Assinatura	Um conjunto de dados, como códigos ou chaves criptográficas públicas, usado para verificar a assinatura eletrónica.
Dispositivo de Criação de Assinatura	Suporte lógico ou dispositivo de equipamento utilizado para possibilitar o tratamento dos dados de criação de assinatura.
Dispositivo Seguro de Criação de Assinatura	Dispositivo de criação de assinatura que assegure, através de meios técnicos e processuais adequados, que, i) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura só possam ocorrer uma única vez e que a confidencialidade desses dados se encontre assegurada; ii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura não possam, com um grau razoável de segurança, ser deduzidos de outros dados e que a assinatura esteja protegida contra falsificações realizadas através das tecnologias disponíveis; iii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura possam ser eficazmente protegidos pelo titular contra a utilização ilegítima por terceiros; iv) Os dados que careçam de assinatura não sejam modificados e possam ser apresentados ao titular antes do processo de assinatura.
Documento Eletrónico,	Documento elaborado mediante processamento eletrónico de dados.
Endereço Eletrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos.

1.6.2. Acrónimos

Tabela 7: Acrónimos

Acrónimos	
C	*Country*
CN	*Common Name*
CA	*Certification Authority (o mesmo que EC)*
CRL	*Certificate Revocation List (o mesmo que LCR)*
DN	*Distinguished Name*
DPC	Declaração de Prática de Certificação
EC	*Entidade Certificadora*
HSM	*Hardware Security Module*
O	*Organization*
OU	*Organization Unit*
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
LCR	*Lista de Certificados Revogados*
PC	Política de Certificados
PKI	*Public Key Infrastructure*
PKCS	*Public Key Cryptography Standards*
SHA	*Secure Hash Algorithm*
SSl/TLS	*Secure Sockets Layer / Transport Layer Security*
SSCD	*Secure Signature Creation Device*

1.6.3. Referencias bibliográficas

- *RFC 5280: Internet X.509 Public key Infrastructure Certificate and Certificate Revocation List*
  Profile, 2008;
- *RFC 3647 - Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, 2003;*
  CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.8.4;
- *Regulation (EU) No 910/2014;*
- *ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.*

2. Responsabilidade de Publicação e Repositório

2.1.Repositórios

A SISP é responsável pelas funções de repositório da SISPROOTCA02, publicando entre outras, informação relativa às práticas adotadas e o estado dos certificados emitidos (CRL).

O acesso à informação disponibilizada pelo repositório é efetuado através do protocolo *HTTPS e HTTP*, estando implementado os seguintes mecanismos de segurança:

- A *CRL* e *PC* só podem ser alterados através de processos e procedimentos bem definidos,
- A plataforma tecnológica do repositório encontra-se devidamente protegida pelas técnicas mais atuais de segurança física e lógica,

- Os recursos humanos que gerem a plataforma têm formação e treino adequado para o serviço em questão.

2.2.Publicação da Informação de Certificação

A SISP mantém um repositório em ambiente Web, permitindo que as Partes Confiantes efetuem pesquisas on-line relativas à revogação e outra informação referente ao estado dos Certificados, durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

A SISP disponibiliza para as todas as suas Entidades Certificadoras a seguinte informação pública *on-line* no *URL http://pki.sisp.cv*:

- Certificados das EC's;
- Uma cópia atualizada da DPC das EC's;
- Uma cópia eletrónica atualizada das PC's das EC's;
- Uma relação das EC's vinculadas à cada EC de Raiz;
- Lista de Certificados Revogados das EC's (LCR);
- Uma relação das Entidades de Registos vinculadas e seus respetivos endereços de instalações técnicas em funcionamento;

Adicionalmente serão conservadas todas as versões anteriores das PC's das EC's Subordinadas, disponibilizando-as a quem as solicite (desde que justificado), ficando, no entanto, fora do repositório público de acesso livre.

A SISP disponibiliza ainda publicamente e no seu sitio web uma ferramenta que permite aos titulares de certificados web testarem e validarem a cadeia de confiança dos certificados nos estados, validos, revogados e expirados.

2.3.Periodicidade de Publicação

A SISP garante que as atualizações a esta PC e respetivas políticas serão publicadas sempre que houver necessidade de se proceder a uma alteração. Uma nova CRL da SISPROOTCA02, será publicada, no mínimo, de três em três mês.

2.4.Controlos de Acesso aos Repositórios

A informação publicada pela SISP estará disponível na Internet, sendo sujeita a mecanismos de controlo de acesso (acesso somente para leitura). A SISP implementou medidas de segurança lógica e física para impedir que pessoas não autorizadas possam adicionar, apagar ou modificar registos do repositório.

3. Identificação e Autenticação

3.1.Atribuição de Nomes

Esta secção descreve os procedimentos usados para autenticar as entidades antes de lhe serem emitidos certificados, bem como questões relativas a disputas de nomes.

3.1.1. Tipos de Nomes

A SISP garante a emissão de certificados contendo um *Distinguished Name (DN) X.509*, definido conforme RFC 5280 e emite certificados para os requerentes que submetem documentação contendo um nome verificável.

A SISP assegurará, dentro da sua infraestrutura de confiança, a não existência de certificados que, contendo o mesmo DN, possam identificar entidades distintas.

O nome único destes certificados está identificado nas respetivas Políticas de Certificados

3.1.2. Necessidade de Nomes Significativos

A SISP assegurará, que os nomes usados nos certificados por ela emitidos, identificam de uma forma significativa os seus utilizadores. Isto é, será assegurado que o DN usado é apropriado para o utilizador em questão e que a componente *Common Name* do DN representa o utilizador de uma forma facilmente compreensível pelas pessoas. A SISPROOTCA02 garante que o campo *Common Name* constante do *Suject DN* do certificado é igual a um dos *Subject Alternative Names,* e que foi validado usando pelo menos um dos métodos indicados na secção 3.2.2.4 da *Baseline Requirements CA/B Forum*.

3.1.3. Anonimato ou Pseudónimo de Titulares

Nada a assinalar.

3.1.4. Interpretação de Formato de Nomes

As regras utilizadas pela SISP para interpretar o formato dos nomes seguem o estabelecido no RFC 5280, assegurando que todos os atributos *DirectoryString* dos campos *issuer* e *subject* do certificado são codificados numa *UTF8String*, com exceção dos atributos *country* e *serial number* que são codificados numa *PrintableString.*

3.1.5. Unicidade de Nomes

A SISP controlará os nomes existentes, de forma a garantir que um certificado contém um DN único, relativo apenas a uma entidade e que não é ambíguo.

3.1.6. Reconhecimento, Autenticação e Papeis das Marcas Registadas

Os nomes, emitidos pela SISP, respeitarão o máximo possível as marcas registadas. A SISP não permitirá deliberadamente a utilização de nomes registados cuja propriedade não possa ser comprovada pelo requerente. Contudo poderá recusar a emissão de certificados com nomes de marcas registadas se entender que outra identificação é mais conveniente.

3.2.Validação de Identidade no Registo Inicial

A SISPROOTCA02 é responsável por autenticar a identidade das entidades candidatas à obtenção de um certificado.

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, os poderes bastantes do representante nomeado pela entidade para a referida emissão.

A emissão de certificados qualificados dentro da hierarquia de confiança da SISP, obriga a que SISPROOTCA02 proceda a um processo rigoroso de verificação da identidade do titular e dos dados a ele associados.

3.2.1. Método de Prova de Posse da Chave Privada

Nos casos em que a SISPROOTCA02 não é a responsável pela geração do par de chaves a ser atribuído ao titular, antes da emissão, deve garantir que o titular está na posse da chave privada correspondente à chave publica incluída no pedido de certificado (CSR).
O método de prova deve ser tanto mais rigoroso quanto maior for a importância e o tipo de certificado solicitado, devendo estar devidamente especificado na Política de Certificado em questão.

3.2.2. Autenticação de Identidade da Organização e Domínio

Os DNs emitidos pela SISPROOTCA02 têm em consideração as marcas registadas, não permitindo a utilização deliberada de nomes registados cuja propriedade não possa ser provada, podendo recusar a emissão do certificado se concluir que outra identificação é mais apropriada.

A SISPROOTCA02 verifica a autenticidade dos dados através de uma das seguintes formas:

a) Por meio de documentos oficiais emitidos por entidades governamentais, designadamente, Certidão Comercial;
b) Autenticação do formulário de pedido de certificado contendo os dados da organização, por uma entidade com poderes para tal (Cartório Notarial, Conservatória, ou outro equivalente);
c) De uma base de dados de terceiros confiável e que seja atualizada periodicamente (D&B, por exemplo);
d) De uma visita ao local, pelo próprio CA ou de um Agente em sua representação;
e) Da prova de controlo do endereço de email sempre que este é incluído no Distinguished Name ou Subject Alternative Name;
f) Da validação do direito de uso e controlo do nome de domínio/endereço constantes do Common Name e Subject Alternative Name do certificado. A SISPROOTCA02 efectua esta validação, utilizando pelo menos um dos métodos descritos na secção 3.2.2.4 da CAB Forum Baseline Requirements.

3.2.2.1. Identidade

Nada a assinalar.

3.2.2.2. Marcas Registadas

Nada a assinalar.

3.2.2.3. Verificação do País

Nada a assinalar.

3.2.2.4. Validação de Autorização ou Controlo de Domínio

Nada a assinalar.

3.2.2.5. Autenticação de um endereço IP

Nada a assinalar.

3.2.2.6. Validação do domínio Wildcard

Nada a assinalar.

3.2.2.7. Exatidão de fontes de dados

Nada a assinalar

3.2.2.8. Registos CAA

Nada a assinalar.

3.2.3. Autenticação de Identidade do Indivíduo

A verificação de identidade dos titulares e/ou subscritores é feita elo grupo de trabalho de registos e pode ser feita de uma das seguintes vias:

- Mediante a presença física da pessoa singular ou de um representante autorizado da pessoa coletiva, e na presença de dois operadores de registos;
- À distância, utilizando meios de identificação eletrónica, para os quais tenha sido assegurada, antes da emissão do certificado qualificado, a presença física da pessoa singular ou de um representante autorizado da pessoa coletiva e que cumprem os requisitos estabelecidos no artigo 8.o relativamente aos níveis de garantia «substancial» ou «elevado» conforme descrito no Regulamento eIDAS No.910/2024; ou

- Por meio de um certificado de assinatura eletrónica qualificada ou de selo eletrónico qualificado emitidos sob a Infraestrutura de Chave Publica de Cabo Verde (apenas para cidadãos e residentes em Cabo Verde).

3.2.3.1 Identificação de Pessoa Singular

Se o titular é uma pessoa singular, a identidade pode ser verificada através do:

- Nome completo do subscritor
- Data e local de nascimento
- Documento de identificação oficialmente reconhecido pelas autoridades do país
- Documento equivalente á presença física com valor probatório legal.

Se o titular é uma pessoa física em representação de uma pessoa coletiva:

- Nome completo do subscritor
- Data e local de nascimento
- Documento de identificação oficialmente reconhecido pelas autoridades do país
- Documento equivalente à presença física com valor probatório legal
- Designação legal e número de identificação da pessoa coletiva
- Evidencia legal que comprove o poder de representação

Se o titular é uma pessoa singular e é possuidor de uma qualidade profissional:

- Nome completo do subscritor
- Data e local de nascimento
- Documento de identificação oficialmente reconhecido pelas autoridades do país
- Documento equivalente à presença física com valor probatório legal
- Evidencia da profissão exercida
- Número da Licença emitida pela Ordem Profissional
- Área/Departamento a que se encontra afeto

3.2.3.2 Identificação de Pessoa Coletiva

Se o subscritor é uma pessoa coletiva, a identidade pode ser verificada através de:

- Documentos e dados de identificação como sejam:
  - Denominação legal e completa da entidade, p.e, certidão comercial
  - Endereço
  - Número de Identificação Fiscal
  - Número de Registo Comercial

3.2.3.3 Identificação de Dispositivo ou Aplicação

A identificação deve ser autenticada utilizando uma das seguintes provisões:

- Ser oficialmente reconhecido na jurisdição em que o subscritor/titular se encontra registado;
- Pelo nome completo e endereço do subscritor/titular;
- Possuir pelo menos um documento de identificação que contenha fotografia ou

- Número de identificação legal único reconhecido pela jurisdição onde foi emitido.

A SISPROOTCA02 verificará se o candidato tem direito a obter o certificado em questão. Em se tratando de certificados qualificados de autenticação web, a SISPROOTCA02 é obrigada a efetuar a verificação do nome e endereço do representante legal e que a morada da entidade é a que conste dos documentos oficiais ou onde desenvolve a sua atividade.

3.2.4. Informação de Subscritor/Titular Não Verificada

Toda a informação constante do certificado é validada.

3.2.5. Validação de Autoridade

Ver secções 3.2.2 e 3.2.3.

3.2.6. Critérios para Interoperabilidade ou Certificação

Os certificados emitidos pela SISPROOTCA02 são feitos numa hierarquia de confiança. De modo a garantir a total interoperabilidade entre aplicações que usam certificados digitais, recomenda-se o uso exclusivo de caracteres alfanuméricos, sem acentos, espaços, sublinhados, sinal menos, ponto final *([a-z], [A-Z], [0-9], " ", "_", "-", ".")* nas entradas da diretoria X.509.

3.3.Identificação e Autenticação para Renovação de Chaves

3.3.1. Identificação e Autenticação para Renovação de Chaves de Rotina

Não existe renovação de chaves, de rotina. A renovação de certificados utiliza os procedimentos para a autenticação e identificação inicial, onde são gerados novos pares de chaves.

3.3.2. Identificação e Autenticação para Renovação apos Revogação

Se um certificado é revogado, o indivíduo/organização será sujeito a todo o processo inicial de registo, de forma a obter um novo certificado.

3.4.Identificação e Autenticação para Solicitação de Revogação

O pedido de revogação deve obedecer às condições descritas em pormenor na secção 4.9.

4. Requisitos Operacionais do Ciclo de Vida do Certificado

4.1.Pedido de Certificado

O pedido de certificado deve ser formulado, mediante o preenchimento e assinatura do formulário próprio, disponibilizado pela SISP. A assinatura do formulário pode ser manuscrita ou digital, com recurso a uma assinatura qualificada.

4.1.1. Quem Pode Submeter um Pedido de Certificado

O pedido de certificado pode ser efetuado:

- Pelo representante legal do titular, devidamente mandatado para o efeito, quando o titular é uma pessoa coletiva ou
- Por um representante da SISP.

4.1.2. Processo de Registo e Responsabilidades

Após a receção da documentação inicia-se o processo de validação da autenticidade da documentação e da identidade do titular. Este processo é realizado por dois administradores de registo. Todos os pedidos aceites ou rejeitados serão retidos e preservados pelo período de 7 anos de acordo com a secção 5.5.2 do *CA Browser* Fórum.
A SISPROOTCA02 não dispõe de entidade de registo externa.

4.2.Processamento do Pedido de Certificado

4.2.1. Desempenho de Funções de Identificação e Autenticação

A SISPROOTCA02, assim que rececione o formulário de pedido de emissão de certificado, assim como a informação necessária à emissão do pedido, procederá à validação de toda a informação disponibilizada a fim de verificar a autenticidade dos dados constantes (cf. secção 3.2).

4.2.2. Aprovação ou Rejeição de Pedidos de Certificados

A SISPROOTCA02 apenas aceita o pedido de certificado para emissão se todos os dados constantes no pedido forem autênticos, neste caso sucede-se a aprovação do pedido.

No caso das informações constantes não forem verdadeiras ou forem incompletas, a EC rejeita o pedido de emissão de certificado sendo assim informado ao responsável pelo pedido.

A SISPROOTCA02 não emite certificados para domínios internos.

4.2.3. Prazo para Emissão do Certificado

Nada a assinalar.

4.3.Emissão de Certificados

4.3.1. Ações da CA durante a Emissão do Certificado

A emissão do certificado é efetuada na presença do auditor, por dois membros dos grupos de trabalho, mediante autenticação (cartão+ PIN), sendo um responsável pela inserção dos dados e outro pela validação e aprovação do pedido.

A emissão do certificado resulta da interação com o modulo criptográfico (HSM), seguindo um procedimento específico e de acordo com a política de certificado respetiva. O certificado emitido e

assinado pela Entidade Certificadora hierarquicamente superior, é importado na Sub CA correspondente e é gerado a primeira CRL.

A vigência do certificado inicia no momento da sua emissão.

4.3.2. Notificação ao Subscritor/Titular pela CA Emissora do Certificado

Nada a assinalar.

4.4.Aceitação do Certificado

4.4.1. Conduta que Constitui a Aceitação do Certificado

O certificado considera-se aceite após a assinatura do formulário de emissão e aceitação de certificado pelo(s) representante(s) da entidade subordinada.

Note-se que antes de ser disponibilizado o certificado aos representantes, e consequentemente lhe serem disponibilizadas todas as funcionalidades na utilização da chave privada e certificado, é garantido que:

- É tomado conhecimento dos direitos e responsabilidades;
- É tomado conhecimento das funcionalidades e conteúdo do certificado;
- É aceite formalmente o certificado e as suas condições de utilização assinando para o efeito o Formulário de Receção de certificado.

4.4.2. Publicitação do Certificado pela CA

A SISPROOTCA02 não publicita a lista de certificados emitidos.

4.4.3. Notificação da Emissão de Certificados a Outras Entidades

A SISPROOTCA02 não notifica entidades outras, sobre a sua atividade de emissão de certificados.

4.5.Utilização do Certificado e Par de Chaves

4.5.1. Utilização do Certificado e Par de Chaves pelo Subscritor/Titular

O titular deve utilizar sua chave privada e garantir a proteção dessa chave conforme o previsto nesta PC.
A sua utilização apenas é permitida:

- A quem for designado como responsável ou representante da entidade requerente no formulário de adesão;
- Após aceitação dos termos e condições de utilização, conforme definido na **secção 4.4.1;**
- Enquanto o certificado se mantiver válido e não estiver na CRL da SISPROOTCA02.

4.5.2. Utilização do Certificado e Chave Pública por Partes Confiantes

As partes confiantes devem usar aplicações/software que estejam em conformidade com o padrão x.509 e devem confiar no certificado apenas se este estiver valido. A SISPROOTCA02 disponibiliza serviços que permitem validar o status do certificado a todo momento e em real time, a saber: OCSP e CRL.

4.6.Renovação de Certificado

A renovação de um certificado é o processo de emissão de um novo certificado com uma nova par de chaves. Pode-se fazer uso dos dados e funções do pedido anterior, desde que estes tenham-se mantido inalterados.

4.6.1. Circunstâncias para a Renovação do Certificado

Nada a assinalar.

4.6.2. Quem pode Solicitar a Renovação de Certificado

Nada a assinalar.

4.6.3. Processamento do Pedido de Renovação de Certificado

Nada a assinalar.

4.6.4. Notificação de Nova Emissão de Renovação de Certificado ao Subscritor/Titular

Nada a assinalar.

4.6.5. Conduta que Constitui a Aceitação de Renovação de Certificado

Nada a assinalar.

4.6.6. Publicitação da Renovação de Certificados pela CA

Nada a assinalar.

4.6.7. Notificação da Renovação de Certificados pela CA a Outras Entidades

Nada a assinalar.

4.7.Re-Key do Certificado

4.7.1. Circunstâncias para o Re-Key de Certificado

A SISPROOTCA02 não suporta o processo Re-Key de certificados

4.7.2. Quem pode Solicitar a Certificação de Uma Nova Chave Publica

Nada a assinalar.

4.7.3. Processamento do Pedido de re-keying

Nada a assinalar.

4.7.4. Notificação de Emissão de Novo Certificado ao Subscritor

Nada a assinalar.

4.7.5. Conduta que Constitui a Aceitação do Certificado Re-Keyed

Nada a assinalar.

4.7.6. Publicitação do Certificado Re-Keyed pela CA

Nada a assinalar.

4.7.7. Notificação do Certificado Re-Keyed pela CA a Outras Entidades

Nada a assinalar.

4.8.Modificação do Certificado

A modificação do certificado é um processo pelo qual o certificado é emitido para um subscritor/titular ou patrocinador mantendo as mesmas chaves, com alterações apenas nas informações do certificado. A modificação de certificados não é suportada pela SISPROOTCA02.

4.8.1. Circunstâncias para Modificação de Certificado

Nada a assinalar.

4.8.2. Quem Pode Solicitar a Modificação de Certificado

Nada a assinalar.

4.8.3. Processamento do Pedido de Modificação de Certificado

Nada a assinalar.

4.8.4. Notificação de Emissão de Novo Certificado ao Subscritor

Nada a assinalar.

4.8.5. Conduta que Constitui a Aceitação do Certificado Modificado

Nada a assinalar.

4.8.6. Publicitação do Certificado Modificado pela CA

Nada a assinalar.

4.8.7. Notificação do Certificado Modificado pela CA a Outras Entidades

Nada a assinalar.

4.9.Revogação e Suspensão do Certificado

A revogação 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, deixam de ser válidos.
A suspensão de certificados não é suportada pela SISPROOTCA02 CA.

4.9.1. Motivos para Revogação

A SISPROOTCA02 deve revogar o certificado no período máximo de 7 dias se ocorrer uma ou mais das seguintes situações:

- A SubCA solicita por escrito a revogação do certificado;
- A SubCA notifica a SISP Root CA2 (Issuing CA) que o pedido inicial de certificado não foi autorizado e não garante autorização retroativamente;
- A Issuing CA obtém evidencia de que a Chave Privada da SubCA correspondente à Chave Publica no certificado foi comprometida ou não cumpre mais os requisitos da Secção 6.1.5 e da Secção 6.1.6;
- A Issuing CA obteve evidencias de que o Certificado foi incorretamente utilizado;
- A Issuing CA é informada de que o Certificado não foi emitido em conformidade ou a SubCA não cumpriu com este documento ou com a Política de Certificados aplicável;
- A Issuing CA determina que uma ou mais informações que aparecem no Certificado é impreciso ou não é verídico;
- A Issuing CA ou a SubCA cessou as operações e não criou condições para que outra CA fornecesse suporte de revogação para o Certificado;
- A revogação é exigida nos termos da Política de Certificação da Issuing CA.

4.9.2. Quem pode solicitar a revogação

Está legitimado para submeter o pedido de revogação, as seguintes entidades:

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

4.9.3. Procedimento para o Pedido de Revogação

Todos os pedidos de revogação devem ser endereçados à SISP S.A. por escrito, através do portal web disponível em https://pki.sisp.cv/ ou por mensagem eletrónica assinada digitalmente, em formulário próprio de pedido de revogação disponibilizado para o efeito.
O pedido é processado nas 24horas seguintes à receção do pedido. Antes de processar o pedido a SISPROOTCA02 obriga-se a verificar a identidade e autenticidade da entidade requerente bem com a manter um registo do pedido após a sua execução.

4.9.4. Período de Carência do Pedido de Revogação

O titular pode solicitar a revogação do certificado a qualquer momento. Contudo recomenda-se em caso de suspeita de comprometimento da chave privada, que o pedido seja feito nas 24 horas seguintes à deteção.

4.9.5. Tempo de Processamento do Pedido de Revogação pela CA

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

4.9.6. Requisito de Verificação da Revogação pelas Partes Confiantes

Antes de utilizarem um certificado, as partes confiantes têm a responsabilidade de verificar o estado do certificado, através da CRL ou num servidor de verificação do estado online (OCSP).

4.9.7. Frequência de Emissão de CRL

A SISPROOTCA02 publica uma nova CRL no repositório, sempre que haja uma revogação. Quando não existam alterações ao estado de validade dos certificados, ou seja, se nenhuma revogação se tiver produzido, a SISPROOTCA02 disponibiliza uma nova CRL a cada **3 meses**.

A CRL pode ser consultada no seguinte repositório: http://crl.sisp.cv/sisprootca02.crl

4.9.8. Latência Máxima para CRL

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

4.9.9. Disponibilidade de Verificação de Estado/Revogação *Online*

A SISPROOTCA02 funciona offline e não dispõe de um serviço de validação de estado de certificado online, OCSP.

4.9.10. Requisitos de Verificação de Revogação *Online*

Antes de fazer uso de um certificado as partes confiantes têm a responsabilidade de verificar o estado de todos os certificados, através da CRL.

A CRL pode ser acedida em https://pki.sisp.cv/document_repository que se encontra disponível 24 horas por dia, 7 dias por semana, excepto durante os períodos de paragem programada para manutenção em que as partes confiantes serão notificadas.

O término de um certificado ocorre quando o prazo de validade expira ou é revogado.

4.9.11. Outras Formas Disponíveis de Anunciar a Revogação

Nada a assinalar.

4.9.12. Requisitos Especiais Relacionados com o Comprometimento de Chave

Complementarmente às razões mencionadas na secção 4.9.1 desta PC (Politica de Certificado), as partes podem utilizar o email pki@sisp.cv para reportar o comprometimento ou suspeita de comprometimento da chave privada dos certificados adquiridos.

4.9.13. Circunstâncias para Suspensão

Nada a assinalar.

4.9.14. Quem Pode Solicitar a Suspensão

Nada a assinalar.

4.9.15. Procedimento Para Solicitação de Suspensão

Nada a assinalar.

4.9.16. Limites do Período de Suspensão

Nada a assinalar.

4.10. Serviços de Estado do Certificado

4.10.1. Caraterísticas Operacionais

O *status* dos certificados emitidos encontra-se publicamente disponível através CRL e do serviço OCSP.

4.10.2. Disponibilidade de Serviço

O serviço de *status* do certificado está disponível 24 horas por dia, 7 dias por semana. Se um certificado for revogado, não permanece na CRL após a data de expiração.

4.10.3. Recursos Opcionais

Não estipulado.

4.11. Fim de Subscrição

O término de uma assinatura de certificado ocorre quando o período de validade expira ou o certificado é revogada, de acordo com RFC 3647.

4.12. Custodia e Recuperação de Chaves

4.12.1. Políticas e Praticas de Custodia e Recuperação de Chaves

A SISP retém a chave privada da SISP QWAC e da SISPROOTCA02 e armazena-as em ambiente seguro.

As chaves são encriptadas e armazenadas num HSM e não é possível a sua transferência para outro dispositivo. A SISP dispõe de uma copia de backup das chaves que são armazenadas em local seguro com o mesmo nível de segurança que as originais.

4.12.2. Políticas e Praticas de Encapsulamento e Recuperação de Chave de Sessão

Ver secção 4.12.1

5. Controlos de Segurança Física, Gestão e Operacionais

Os controlos de segurança física, gestão e operacionais encontram-se descritos na Declaração de Práticas de Certificação da SISPROOTCA02.

6. Controlos de Segurança Técnica

Os controlos de segurança técnica encontram-se descritos na Declaração de Práticas de Certificação da SISPROOTCA02.

7. Perfis de Certificado, CRL e OCSP

Os perfis de certificados emitidos pela SISPROOTCA02 estão de acordo com a recomendação da ITU.T X.509 versão 3 e atendem aos seguintes standards:

- ETSI EN 319 401 – *General Policy Requirements for Trust Service Providers* e outros relacionados com a prestação de serviços de confiança qualificados;
- *CAB Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*
- ETSI 319 412-5 v2.2.3: Electronic Signatures and Infrastructures (ESI); Certificate Profile-QCStatements;
- *EU Regulation No.910/2014*
- Legislação nacional

7.1.Perfil do Certificado

7.1.1.1. Perfil de Certificado da SISPROOTCA

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	1.2.840.113549.1.1.13	m	Valor TEM que ser igual ao OID no signatureAlgorithm (abaixo)
	Issuer	4.1.2.4		m	
	Country (C)		"CV"		
	Organization (O)		"SISP"		
	Organization Unit (OU)		"SISP-Sociedade Interbancaria e Sistemas de Pagamentos"		

	Common Name (CN)		"Entidade de Certificacao Raiz da SISP 02"		
	Validity Not Before Not After	4.1.2.5	<data de emissão> <data de emissão + 12 anos>	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 Validade de 12 anos com renovação a cada 6 anos.
	Subject Country (C) Organization (O) Organization Unit (OU) Common Name (CN)	4.1.2.6	<SISP Root CA2> "CV" "SISP" "SISP-Sociedade Interbancaria e Sistemas de Pagamentos" "Entidade de Certificacao Raiz da SISP 02"	m	EC auto-assinada
	Subject Public Key Info Algorithm subjectPublicKey	4.1.2.7	1.2.840.113549.1.1.13 <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 3} 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-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 512-bit SHA 512 do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>	m	
	Key Usage Digital Signature	4.2.1.3	"0" seleccionado	mc	Esta extensão é marcada CRÍTICA

	Non Repudiation Key Encipherment Data Encipherment Key Agreement Key Certificate Signature CRL Signature Encipher Only Decipher Only		“0” seleccionado “0” seleccionado “0” seleccionado “0” seleccionado “1” seleccionado “1” seleccionado “0” seleccionado “0” seleccionado		
	Cerificate Policies	4.2.1.4		o	
	Basic Constrains CA PathLen Constraint	4.2.1.9	TRUE	m c 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/sisprootca2.crl	o m	
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.13	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha512WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member- body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13
	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.

7.1.1.2. Perfil de Certificado da SISP QWAC CA

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	1.2.840.113549.1.1.13	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" "SISP" "SISP-Sociedade Interbancaria e Sistemas de Pagamentos" "Entidade de Certificacao Raiz da SISP 02 "	m	 Designação Oficial da EC da SISP 02 - sequencia da EC

	Validity Not Before Not After	4.1.2.5	 <data de emissão> <data de emissão + 5 anos e 4 meses>	m	Validade maxima de 6 anos.
	Subject Country (C) Organization (O) Organization Unit (OU) Common Name (CN)	4.1.2.6	 "CV" "SISP" "SISP-Sociedade Interbancaria e Sistemas de Pagamentos" "SISP QWAC"	m	Designação Official da EC da SISP
	Select Public Key Info Algorithm subjectPublicKey	4.1.2.7	 1.2.840.113549.1.1.13 <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 3} 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 512-bit SHA-512do 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 512-bit SHA-512 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	4.2.1.3	 “1” seleccionado “0” seleccionado “1” seleccionado “1” seleccionado “0” seleccionado “1” seleccionado “1” seleccionado	mc	Esta extensão é marcada CRÍTICA

	Encipher Only Decipher Only		"0" seleccionado "0" seleccionado		
	Cerificate Policies policyIdentifier policyQualifiers	4.2.1.4	 1.3.6.1.4.1.4146.1.60 <policyQualifierID> cPSuri: https://pki.sisp.cv/document_repository	o m o	Identificador da Declaração de Práticas de Certificação da SISP ROOT CA 02 (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 02. O apontador está na forma de um URL."
	policyIdentifier policyQualifiers		1.3.6.1.4.1.4146.1.60 <policyQualifierID> cPSuri: https://pki.sisp.cv/document_repository	m o	Identificador da Declaração de Práticas de Certificação da SISP ROOT CA 02 (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 02. O apontador está na forma de um URL."
	Basic Constrains CA PathLen Constraint	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/sisprootca2.crl	o m	
	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	 m m	 Server Autentication Client Autentication
	Internet Certificate Extensions				
	Authority Information Access accessMethod accessLocation accessMethod accessLocation	4.2.2.1	 1.3.6.1.5.5.7.48.1 http://ocsp.sisp.cv/ 1.3.6.1.5.5.7.48.2 https://pki.sisp.cv/document_repository	o	 Valor do OID: (id-ad-ocsp) URL para aceder ao OCSP Valor do OID: (id-ad-ca) URL para aceder ao Certificado da CA
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.13	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha512WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member- body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13
	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.

7.1.2. Número da Versão

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

7.1.3. Extensões do Certificado

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

7.1.4. OID do Algoritmo

O campo "*signatureAlgorithm*" do certificado contém o OID do algoritmo criptográfico utilizado pela EC para assinar o certificado: *1.2.840.113549.1.1.13 (sha512WithRSAEncryption)*.

7.1.5. Formatos de Nome

Tal como definido na secção 3.1.

7.1.6. Condicionamento nos Nomes

A SISP pode incluir condicionamento aos nomes, no campo "*nameConstraints*" sempre que se justificar.

7.1.7. OID da Política de Certificado

Nada a assinalar.

7.1.8. Utilização de Extensão de Restrições de Política

Nada a assinalar.

7.1.9. Sintaxe e Semânticas de Qualificadores de Política

Nada a assinalar.

7.1.10. Semântica de Processamento para a Extensão critica *Certificate Policies*

Nada a assinalar.

7.2. Perfil 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, 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.

Componente da CRL	Componente do Certificado	Secção no RFC5280	Valor	Tipo	Comentários
tbsCertList	**Version**	5.1.2.1	3	m	O valor 3 identifica a utilização da Versão 3 do padrão ITU X.509
	Signature	5.1.2.2	1.2.840.113549.1.1.13	m	Contém o identificador do algoritmo utilizado para assinar a LCR. O valor TEM que ser igual ao OID no campo signatureAlgorithm (abaixo)
	Issuer Country (C) Organization (O) Common Name (CN)	5.1.2.3	 "CV" "SISP" "Entidade de Certificacao Raiz da SISP 02 "	m	
	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 KeyIdentifier	5.2.1	 O key Identifier é composto pela hash de 512-bit SHA-512 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	

	Issuing Distribuition Point DistributionPointName	5.2.5	http://crl.sisp.cv/sisprootca02.crl	c	
	CRL Entry Extensions Reason Code	5.3 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	1.2.840.113549.1.1.13	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha512WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member- body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13
	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.

7.2.1. Número(s) de Versão

O campo "*version*" da *CRL* descreve a versão utilizada na codificação da *CRL*. Neste perfil, a versão utilizada é 3 (três).

7.2.2. *CRL* e Extensões da *CRL*

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.

7.3.Perfil OCSP

7.3.1. Número(s) de Versão

Nada a assinalar.

7.3.2. Extensões OCSP

Nada a assinalar.

Referencias Bibliográficas

- RFC 5280: Internet X.509 Public key Infrastructure Certificate and Certificate Revocation List Profile, 2008;
- RFC 3647 - Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, 2003;
- CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.8.4;
- CA/ Browser Forum-EV-Guidelines –v1.7.6;
- Regulation (EU) No 910/2014;
- ETSI 319 412-4 v1.1.1: Electronic Signatures and Infrastructures (ESI); Certificate Profile for Website;
- ETSI 319 412-5 v2.2.3: Electronic Signatures and Infrastructures (ESI); Certificate Profile-QCStatements;
- ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.