NOSi, EPE – Núcleo Operacional da Sociedade de Informação

Política de Certificação da Entidade Certificadora NOSICA – G2

Versão	Data	Autor
2.0	01/10/2021	Direção de Segurança & Compliance

Controlo de Documentação

Versão	Data da Versão	Criado por	Aprovado por	Classificação
2.0	01/10/2021	Direção de Segurança & Compliance		Público

Histórico de Alterações

Versão	Data	Alterado por	Descrição
1.0	27/07/2021		Criação do Documento
2.0	01/10/2021	Liane Gonçalves	

Implementado	Revisto	Aprovado

Informações de Contacto

Nome	Endereço	Email
Direção de Segurança & Compliance	Praia-Santiago	dsc@nosi.cv

Índice

1. Introdução

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

Este documento descreve a política de certificados para a emissão e gestão dos Certificados Qualificados de Assinatura Digital e Selo Eletrónico, emitido pela Entidade de Certificação Subordinada NOSI CA – G2, doravante NOSI CA.
Os certificados emitidos pelo NOSI CA contêm uma referência ao PC de modo a permitir que Partes confiantes e outras pessoas interessadas possam encontrar informação sobre o certificado e sobre as políticas seguidas pela entidade que o emitiu.

1.1 Visão Geral

Este documento satisfaz e complementa os requisitos impostos pela Declaração de Prática de Certificação (DPC) do NOSI CA.

1.1.1. Público Alvo

Este documento é público e destina-se a todos quantos se relacionam com o NOSI CA.

1.2. Nome e Identificação do Documento

Este documento é a Política de Certificados de assinatura Digital Qualificada. A PC é representada num certificado através de um número único designado de “identificador de objeto” (OID).

Este documento é identificado pelos dados constantes na seguinte tabela:

Informação do documento	
Versão do Documento	Versão 1.0
Estado do Documento	
OID	
Data de Emissão	14/07/2021
Validade	1 ano
Localização	https://nosi.cv

1.3. Participantes PKI

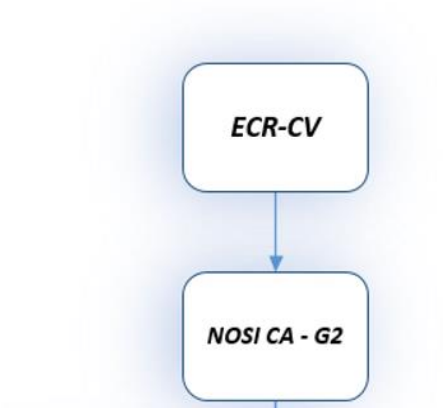
1.3.1. Entidades Certificadoras

O NOSI CA é uma entidade de certificação credenciada pela Autoridade Credenciadora, conforme previsto na legislação Cabo-verdiana, estando deste modo habilitada legalmente a emitir certificados digitais, incluindo os Certificados Digitais Qualificados para Pessoa Singular e Selo Eletrónico. Insere-se em duas hierarquias de confiança:

- Entidade Certificadora de Raiz de Cabo Verde (ECR-CV);
- NOSI Certificate Authority (NOSI CA);

Deste modo, o NOSI CA é reconhecido na maioria dos sistemas operativos sendo a sua função principal providenciar a gestão de serviços de certificação: emissão, operação, suspensão, revogação para os seus subscritores.

Esquematicamente:



O NOSI CA emite certificados:

- Certificados Qualificados:
  - **Assinatura Qualificada para pessoa singular:**
    - **Individual**
      - ✓ Particular - Certificado emitido que inclui o nome do seu titular, que será utilizado para assinar documentos
      - ✓ Assinatura Qualificada de Qualidade (ordens Profissionais) Certificado com as mesmas características do Particular, no entanto acrescido de um atributo de qualidade, associado a uma entidade/organização (ex. Médico, Engenheiro, etc).
      - ✓ Assinatura Qualificada para Representação de pessoa Coletiva Certificado com as mesmas características do Particular, no entanto acrescido de um atributo no qual é conferido os efeitos de representação de uma Organização ao seu titular. Estes poderes de representação são delegados ou conferidos pelos representantes legais da organização.

- **Assinatura Qualificada para pessoa coletiva:**
  - ✓ **Selo Eletrónico** – Certificado emitido para a Organização, ou seja, o titular do certificado é uma pessoa coletiva. Este Certificado pode ser utilizado, a título de exemplo, para assinatura de faturas eletrónicas (emissão de grandes volumes com segurança acrescida), extratos de conta eletrónicos, declarações eletrónicas, certidões e outros tipos de documentos emitidos online por entidades públicas.

- **Assinatura Eletrónica Avançada:**
  - ✓ **Assinatura Avançada Singular** - Certificados emitidos para particulares e profissionais, permitindo a assinatura eletrónica de documentos (sem valor probatório) e a identificação eletrónica segura e unívoca de uma pessoa.

1.3.2. Entidades Registo

Entidade de Registo (ER) é a entidade que aprova os nomes distintos (DN) dos titulares dos certificados e mediante avaliação do pedido, aceita ou rejeita a solicitação do mesmo. Para além disso, a ER também tem autoridade para aprovar a revogação ou suspensão de certificados.

São ER's da PKI do NOSI:

- ER Interna - Operacionalizada Pelos serviços Internos do PKI do NOSI, detentora da EC.

As Entidades de Registo do PKI NOSI, cumprem os requisitos estabelecidos neste documento e estão sujeitas a Auditorias Externas, assim como Auditorias Internas.

As auditorias externas são efetuadas por auditores credenciados pela Autoridade Credenciadora Nacional.

1.3.2.1. ER Interna

No âmbito da Entidade de Certificação NOSI, a entidade de registo materializa-se pelos serviços internos da mesma que procedem ao registo e validação dos dados necessários, conforme explicitado na Política de Certificado de cada tipo de certificados emitidos.

1.3.3. Titulares dos Certificados

No contexto deste documento o termo subscritor/titular aplica-se a todos os utilizadores finais a quem tenham sido atribuídos certificados pela PKI do NOSI.
São considerados titulares de certificados emitidos pela PKI do NOSI, aquele 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 singular;
- Pessoas Coletivas (Organizações).

Em alguns casos, os certificados são emitidos diretamente a pessoas singulares 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/comércio eletrónico. 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, que confiam na validade dos mecanismos e procedimentos utilizados no processo de associação do nome do titular com a sua chave pública, ou seja, confiam que o certificado corresponde na realidade a quem diz pertencer.

Neste documento, considera-se uma parte confiante, aquela que confia no teor, validade e aplicabilidade do certificado emitido pela PKI do NOSI.

1.3.5. Outros Participantes

1.3.5.1. Entidade Credenciadora

A Entidade Credenciadora é a entidade competente para a credenciação e fiscalização das entidades certificadoras.

De uma forma geral o papel da Entidade Credenciadora, exercida em Cabo Verde pela Entidade Certificadora Raiz Cabo Verde (ECRCV), está relacionado com a auditoria/inspeção de conformidade, no sentido de aferir se os processos utilizados pelas EC, nas suas atividades de certificação, estão conformes, de acordo com os requisitos mínimos estabelecidos na legislação Cabo-Verdiana, assim como com o estabelecido nesta PC.

A Entidade Credenciadora é uma das "peças" que contribui para a confiabilidade dos Certificados Qualificados, pelas competências que exerce sobre as EC que os emitem. No âmbito das suas funções, exerce os seguintes papéis relativamente às EC:

a) Credenciação: procedimento de aprovação da EC para exercer a sua atividade, com base numa avaliação feita a parâmetros tão diversificados como a segurança física, e lógica, procedimentos de acesso e de operação, recursos humanos;
b) Registo: procedimento sem o qual a EC não poderá emitir os Certificados Qualificados;
c) Fiscalização: procedimento assente em inspeções efetuadas às EC, com vista a regularmente verificar parâmetros de conformidade;

1.3.5.2. Entidade Registo

Descrito na secção 1.3.2

1.3.5.3. Entidades de Validação OCSP

As Entidades de Validação OCSP, têm como função comprovar o estado dos certificados emitidos, através da utilização do protocolo Online Certificate Status Protocol (OCSP),

de forma a determinar o estado atual do certificado, a pedido de uma entidade, sem necessidade de recorrer à verificação do estado através da consulta das Listas de Certificados Revogados (CRL-Certificate Revogation List).
O serviço de Entidade de Validação OCSP é disponibilizado pela PKI da NOSI.

1.3.5.4. Auditor de Segurança

Figura independente do círculo de influência da Entidade de Certificação, devidamente acreditado pela Autoridade Credenciadora de Cabo Verde (ARME – Agência Regulamentação Multissectorial de Economia). A sua missão é auditar a infraestrutura da Entidade de Certificação, no que respeita a equipamentos, recursos humanos, processos, políticas e regras para avaliação de conformidade dos serviços de confiança ao abrigo do Decreto Lei nº 33/2007 de 24 de Setembro e do Decreto Regulamentar nº 18/2007 de 24 de Dezembro.

As Auditorias de conformidade deverão ocorrer, pelo menos, a cada 12 meses, com intuito de confirmar que a NOSI CA, como prestadora qualificada de serviços de confiança e os serviços de confiança que disponibiliza, cumprem os requisitos estabelecidos pelo Decreto Lei nº 33/2007 de 24 de Setembro e Decreto Regulamentar nº 18/2007 de 24 de Dezembro.

1.4. Utilização do Certificado

Os certificados emitidos no domínio da PKI NOSI são utilizados, pelos diversos titulares, com o objetivo de garantir os seguintes serviços de segurança:

a) Controlo de acessos;
b) Confidencialidade;
c) Integridade;
d) Autenticação e,
e) Não repúdio.

Estes serviços são obtidos com recurso à utilização de criptografia de chave pública, através da sua utilização na estrutura de confiança que a PKI do NOSI 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.

1.4.1. Utilização Adequada

Os requisitos e regras definidos neste documento aplicam-se a todos os certificados emitidos pela PKI do NOSI.

Os certificados emitidos pela PKI do NOSI são também utilizados pelas Partes Confiantes para verificação da cadeia de confiança de um certificado emitido sob o NOSI CA, assim como para garantir a autenticidade e identidade do emissor de uma assinatura digital gerada pela chave privada correspondente à chave pública contida num certificado emitido sob o NOSI CA.

1.4.1.1. Certificados Emitidos para Pessoas Singulares

Os certificados emitidos para pessoas singulares, de acordo com o tipo de certificado adquirido, podem ser utilizados para:

- Assinar documentos
- Assinar correio eletrónico

1.4.1.2. Certificados Emitidos para Organizações

Os certificados para as organizações são emitidos para garantia de Identificação da Organização.

1.4.2. Utilização Não Autorizada

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

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

Os serviços de certificação oferecidos pela PKI do NOSI, não foram desenhados nem estão autorizados a ser utilizados 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. Entidade Responsável pela gestão do documento

A gestão desta política de certificados é da responsabilidade do Grupo de Trabalho de Administração de Segurança da PKI do NOSI.

1.5.2. Contacto

Nome:	*PKI do NOSI*
Morada:	*Data Center Estado Cabo Verde, Av. António Mascarenhas – Achada Grande Frente – Santiago, Cabo Verde*
Correio Eletrónico:	*pki@nosi.cv*
Site:	https://nosi.cv/
Telefone:	(+238) 260 79 73

1.5.3. Entidade Responsável pela determinação da conformidade da PC

O Grupo de Trabalho da PKI do NOSI determina a conformidade e aplicação interna desta PC, submetendo-o de seguida ao Grupo de Gestão para aprovação.

1.5.4. Procedimentos para aprovação da PC

A validação desta PC e seguintes correções (ou atualizações) deverão ser levadas a cabo pelo Grupo de Trabalho da PKI do NOSI. As correções (ou atualizações) deverão ser publicadas sob a forma de novas versões desta PC, substituindo qualquer PC anteriormente definida. O Grupo de Trabalho da PKI do NOSI deverá ainda determinar quando é que as alterações na PC levam a uma alteração nos identificadores dos objetos (OID) da PC.

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

1.6. Acrónimos e Definições

1.6.1. 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*
ICP-CV	*Infraestrutura de chaves públicas de Cabo Verde*
CRL	*Certificate Revogation List*
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*

1.6.2. DEFINIÇÕES

Assinatura digital, conforme disposto no Modalidade DL- nº33/2007, de 24 de setembro	Modalidade de assinatura eletrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento eletrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento eletrónico foi alterado depois de aposta a assinatura.
Assinatura eletrónica, conforme disposto no DL-nº33/2007, de 24 de setembro	Dados sob forma eletrónica anexos ou logicamente associados a uma mensagem de dados e que sirvam de método de autenticação.
Assinatura eletrónica avançada, conforme disposto no DL-nº33/2007, de 24 de setembro.	Assinatura eletrónica que preenche os seguintes requisitos: i) Identifica de forma unívoca o titular como autor do documento; ii) A sua aposição ao documento depende apenas da vontade do titular; iii) É criada com meios que o titular pode manter sob seu controlo exclusivo; iv) A sua conexão com o documento permite detetar toda e qualquer alteração superveniente do conteúdo deste.
Assinatura eletrónica qualificada, conforme disposto no DL-nº33/2007, de 24 de setembro.	Assinatura digital ou outra modalidade de assinatura eletrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura.
Autoridade credenciadora, conforme disposto no DL-nº33/2007, de 24 de setembro.	Entidade competente para a credenciação e fiscalização das Entidades de Certificação
Certificado, conforme disposto no DL- nº33/2007, de 24 de setembro	Documento eletrónico que liga os dados de verificação de assinatura ao seu titular e confirma a identidade desse titular.
Certificado qualificado, conforme disposto no DL-nº33/2007, de 24 de setembro	Certificado que contém os elementos referidos no artigo 67.º do DL 33/2007 [6] e é emitido por entidade de certificação que reúne os requisitos definidos no artigo 45.º do DL 33/2007.
Chave privada, conforme disposto no DL- nº33/2007, de 24 de setembro	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico 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 eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves.
Credenciação, conforme disposto no DL- nº33/2007, de 24 de setembro	Ato pelo qual é reconhecido a uma entidade, que o solicite e que exerça a atividade 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 eletrónica.
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	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, conforme disposto no DL-nº33/2007, de 24 de setembro.	Documento elaborado mediante processamento eletrónico de dados.
Endereço eletrónico, conforme disposto no DL- nº33/2007, de 24 de Setembro.	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos.

2. Responsabilidade de Publicação e Repositório

2.1. Repositório

O NOSI CA é responsável pelas funções de repositório do NOSI CA, 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:

- CRL e PC só podem ser alterados através de processos e procedimentos bem definidos,
- 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 de Informação de Certificação

O NOSI disponibiliza sempre a seguinte informação pública on-line no URL https://pki.nosi.cv:

a) Seu próprio Certificado;
b) Uma cópia eletrónica atualizada da DPC do NOSI CA;
c) Uma cópia eletrónica atualizada das PC´s do NOSI CA;
d) Lista de Certificados Revogados do NOSI CA (CRL);
e) Uma relação das Entidades de Registos vinculadas e seus respetivos endereços de instalações técnicas em funcionamento;
f) Formulário para solicitação de emissão de certificado;
g) Formulário para solicitação de revogação/suspensão de certificado.

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

2.3. Periodicidade de Publicação

O NOSI CA 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 do NOSI CA, será publicada, no mínimo, uma vez por dia.

2.4. Controlo de Acesso aos Repositórios

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

3. Identificação e Autenticação

3.1. Atribuição de Nomes

A atribuição de nomes segue a convenção determinada pela DPC do NOSI CA.

3.1.1. Tipos de Nomes

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

3.1.1.1. Certificado Qualificado de Assinatura Digital

Atributo	Código	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>
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 âmbito da sua utilização para assinatura digital qualificada>
Serial Number	serialNumber	< tipo doc identificação ><código país>-<NIC ou PAS>
Common Name	CN	<Nome do titular do certificado>
Surname	SN	<Nomes de família do titular do certificado>
GivenName	givenName	<Nomes próprio do titular do certificado>

A constituição do DN do certificado qualificado de assinatura digital, pode variar conforme especificações das Entidade de Registo NOSI CA (ver 7.1.3).

3.1.1.2. Certificado Qualificado de Selo Eletrónico

Atributo	Código	Valor
Country	C	<País de nacionalidade da Organização>
Organization	O	<Nome da Organização tal como registada nas entidades competentes>
Organization Unit	OU	Qualified Certificate for Electronic Seal
Organization Unit	OU (opcional)	<Área/Departamento da Organização>
Organization Identifier	OI	VAT1<código país>-<Número do de identificação Fiscal>
Common Name	CN	<Nome da organização pela qual é conhecida>

3.1.1.3. Perfil de Certificado de Autenticação

Atributo	Código	Valor
Country	C	<País da nacionalidade do titular do certificado>
Organization	O (opcional)	<Organização à qual o titular do certificado pertence>
Organization Unit	OU	<Área/Departamento da Organização à qual o titular do certificado pertence>
Organization Unit	OU (opcional)	Certificado para pessoa singular – Autenticação
Common Name	CN	<Nome do titular do certificado>
Title	T (opcional)	<Qualidade do titular do certificado, no âmbito da sua utilização para assinatura digital qualificada>
Surname	SN	<Nomes de família do titular do certificado>
GivenName	givenName	<Nomes próprio do titular do certificado>
Serial Number	serialNumber	< tipo doc identificação ><código país>-<NIC ou PAS>

[1] **VAT** – Identificação com base num número nacional de identificação do imposto sobre o valor acrescentado.

3.1.2. Necessidade de Nomes Significativos

O NOSI CA irá assegurar, dentro da sua hierarquia de confiança:

- A não existência de certificados que, tendo o mesmo nome único, identifiquem entidades distintas,
- A relação entre o titular e a organização a que pertence é a mesma que consta no certificado e é facilmente percetível e identificável pelos Humanos (com exceção dos certificados com pseudónimos).

3.1.3. Anonimato ou pseudónimo de titulares

A NOSI CA emite certificados com pseudónimo de titulares, garantindo para o efeito que:

- O certificado contém o pseudónimo do titular, claramente identificado como tal, sendo conservados os elementos que comprovam a verdadeira identidade dos requerentes titulares de certificados com pseudónimo,

- Comunicará à autoridade judiciária, sempre que esta o ordenar nos termos legalmente previstos, os dados relativos à identidade dos titulares de certificados que sejam emitidos com pseudónimo seguindo-se, no aplicável, a legislação vigente.

3.1.4. Interpretação de formato de nomes

As regras utilizadas pela NOSI CA 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 excepção dos atributos country e serial number que são codificados numa PrintableString.

3.1.5. Unicidade dos Nomes

De acordo com os seus processos de emissão, o NOSI CA rejeita a emissão de certificados com o mesmo DN para titulares distintos. Para cada tipo de certificado emitido, a respetiva Política de Certificados indica o conteúdo do serial number que

deverá ser escolhido de modo a assegurar a unicidade do campo e a não induzir uma parte confiante em ambiguidade.

3.1.6. Reconhecimento, autenticação, e função das marcas registadas

Os nomes, emitidos pelo NOSI CA, respeitarão o máximo possível as marcas registadas. O NOSI CA 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.

3.1.7. 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 NOSI CA 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, 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 á NOSI CA toda a documentação necessária acompanhada de um CSR SHA256;

O certificado, após validação da documentação entregue, é devolvido ao responsável.

3.2. Validação de identidade no registo inicial

O NOSI CA é responsável por autenticar a identidade das entidades candidatas à obtenção de um certificado. Um certificado qualificado de assinatura digital é emitido para pessoa singular, sendo este o responsável pela sua utilização. Um Certificado Qualificado de Selo Eletrónico é emitido 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.

3.2.1. Certificado Qualificados

3.2.1.1. Autenticação de 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:

a) Verificar em documentos oficialmente reconhecidos pelo Estado e que contenha uma fotografia:
   i. O nome completo do subscritor;
   ii. O número documento de identificação;
   iii. Os dados de contato, incluindo o endereço caso esteja presente;

b) 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.

3.2.1.2. Autenticação da Identidade de uma Pessoa Colectiva (Selo Eletrónica)

Os Certificados Qualificados emitidos para pessoas coletivas denominam-se de Certificados Qualificados de Selos Eletrónicos, neste caso o Common Name identifica a pessoa coletiva como titular o certificado.

A validação dos dados da pessoa coletiva é efetuada através de documentos emitidos por entidades legais, definidas para o efeito (exemplo Registo Comercial ou Certidão Permanente). Os dados do responsável técnico e do(s) representante(s) da organização são validados mediante cópia do documento de Identificação ou, caso não seja disponibilizado, deverá o contrato de emissão (formulário) ser devidamente autenticado por entidade com poderes para o ato (notário ou advogado).

A autenticação é efetuada aquando a receção do certificado, pelo responsável técnico designado pelos representantes legais da pessoa coletiva. Esta autenticação poderá ser efetuada através de uma das seguintes formas:

1. Entrega presencial:

    a) Ao próprio:
        i. O responsável técnico efetua o levantamento do certificado nas instalações da NOSI EPE, no escritório (Achada Grande Frente) acompanhado de documentos de identificação.
    b) A terceiro:

O responsável técnico pode delegar os poderes de levantamento do certificado a terceiro, mediante declaração com assinatura autenticada e reconhecida por entidade com poderes legais para o ato. A pessoa a quem foram delegados poderes de levantamento, deve apresentar a declaração e respetivo documento de identificação, aquando o levantamento do certificado.

3.2.2. Certificados Avançados

A validação inicial da identidade do requerente de um certificado avançado, emitido pelo NOSI CA, é efetuada através de documentação que é solicitada e enviada pelo

requerente juntamente com o formulário de pedido de emissão de certificado avançado, através da qual valida os dados que constam no pedido, nomeadamente dados do titular, da Entidade Responsável que requer o certificado. As assinaturas constantes no formulário são verificadas de forma comparativa com as cópias dos documentos de identificação solicitadas.

3.2.3. Informação do Subscritor/Titular não verificada

Toda informação descritas nas secções 2.1 e 2.2.

3.2.4. Validação de Autoridade

Nada a assinalar.

3.2.5. Critérios para Interoperabilidade

Nada a assinalar.

3.3. Identificação e Autenticação para Pedidos de Renovação de Chaves

3.3.1. Identificação e Autenticação para Renovação de Chaves, de Rotina

Não existe renovação de chaves, de rotina.

3.3.2. Renovação Após 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 pedido 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
- 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 disponível no (https://pki.nosi.cv) do qual deve constar os seguintes elementos:

- Nome;
- Endereço e outras formas de contacto;
- Indicação do motivo para revogação do certificado.

A ER do NOSI CA guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efetua o pedido de revogação num período não inferior a 20 anos, do certificado de assinatura digital qualificada.

4. Requisitos Operacionais do Ciclo de Vida do Certificado

4.1. Pedido de Certificado

O pedido de certificado deve ser formulado, mediante o preenchimento do Formulário próprio, disponível na loja on-line (www.store.nosi.cv) ou aos balcões das ER.

4.1.1. Quem pode subscrever um Pedido Certificado?

No âmbito geral da ER do NOSI CA, que emite certificados para público em geral.

Os Certificados Qualificados e Avançados de assinatura digital podem ser subscritos:

- Pelo Titular do certificado, quando o certificado é emitido para pessoa singular,
- Pelo Titular e Representantes legais da entidade, quando o certificado é emitido

para pessoa singular associada a uma entidade (na qualidade ou em representação).

O Certificado Qualificado de Selo Eletrónico pode ser subscrito:

- 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”.

Para as Entidades de Registo, a emissão é restrita ao âmbito das mesmas, nomeadamente a Ordem profissional, apenas são emitidos certificados qualificados de assinatura digital.

O pedido de certificado será subscrito pelo titular na qualidade ou função atestada pelos representantes legais da Entidade.

4.1.2. Processo de Registo e Responsabilidades

O pedido de certificado 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, pelo NOSI CA ou ER designada.

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

4.2. Processamento do Pedido de Certificado

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

a) Pedido do Certificado;
b) Receção e verificação de toda a documentação e autorizações exigidas;

c) Validação da exatidão e integridade do pedido de certificado;
d) Processo de emissão de certificado.

As secções 3.2, 4.2.1 e 4.3 descrevem detalhadamente todo o processo.

4.2.1. Processos para a Identificação e Funções de Identificação

4.2.1.1. Certificado de Pessoa Singular

Conforme indicado na secção 3.2

4.2.1.2. Certificado de Pessoa Coletiva

Conforme indicado na secção 3.2

4.2.1.3. Aprovação ou Recusa de Pedidos de Certificado

A aprovação de certificado passa pelo cumprimento dos requisitos exigidos no ponto 4.2 e 4.2.1.1.
Quando tal não se verifique, é recusada a emissão do certificado.

4.2.1.4. Prazo para processar o pedido do certificado

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

4.3. Emissão do certificado

Os certificados emitidos pelo NOSI CA, são emitidos através da plataforma disponibilizada pelo NOSI CA, de forma automática, após o registo e aprovação do pedido de Certificado. Após a aprovação, o request é enviado diretamente para a Entidade de Certificação a qual procede com a emissão do certificado.

Qualquer certificado emitido na PKI do NOSI CA é sujeito a uma aprovação. Esta

aprovação depende do tipo de certificado e da Entidade de Certificação em causa. Para aprovação de certificado de utilizador final, o Grupo de Trabalho de Administração de Registo é responsável pela gestão e aprovação dos pedidos de certificados.

4.3.1. Emissão do Certificados Digitais Qualificados

No caso de Certificados Qualificados de Assinatura e de Selo Eletrónico, o certificado será armazenado em dispositivo de armazenamento seguro, que dependendo da opção escolhida, poderá ser um SmartCard (cartão com chip criptográfico), token USB, ou disponibilizado ao cliente.

4.3.2. Emissão de Certificados Avançados

Os Certificados avançados poderão ser disponibilizados em dispositivo de armazenamento seguro, tal como os certificados digitais qualificados, podendo, no entanto, também, ser disponibilizados através de Download ou em dispositivo magnético (CD, Pen Drive, etc) ou via email.

4.3.3. Notificação da Emissão do Certificados

O titular do certificado é notificado da emissão do certificado através de chamada telefónica ou via email antes da receção do mesmo.

4.4. Aceitação do certificado

4.4.1. Procedimento para Aceitação do Certificado

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

Note-se que antes de ser disponibilizado o certificado ao titular, e consequentemente lhe ser 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;

4.4.2. Publicação do Certificado

O NOSI CA não publica os certificados por ele emitidos, disponibilizando integralmente ao titular.

As condições para este efeito encontram-se definidas na secção 4.4.1. da PC.

4.4.3. Notificação da emissão de certificado a outras entidades

O NOSI CA não notifica outras entidades sobre a emissão de certificados exceto em acordo previamente estabelecidos.

4.5. Uso de Certificado e Par de Chaves

4.5.1. 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 4.5 da Declaração de Práticas de Certificação (DPC);
c) Enquanto o certificado se mantiver válido e não estiver na CRL do NOSI CA.

4.5.2. Uso do Certificado e par de Chaves Públicas 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.

4.6. Renovação do Certificado

Esta prática não é suportada pela PKI do NOSI CA.

A renovação de um certificado é o processo, em que a emissão de um novo certificado utiliza os dados anteriores do certificado, não havendo alteração das chaves ou qualquer outra informação, com exceção do período de validade do certificado.

4.6.1. Motivos para Renovação de Certificado

Nada a assinalar.

4.6.2. Quem pode submeter o Pedido de Renovação de Certificado

Nada a assinalar.

4.6.3. Processamento do Pedido de Renovação de Certificado

Nada a assinalar.

4.6.4. Notificação de Emissão de novo Certificado ao Titular

Nada a assinalar.

4.6.5. Procedimentos para Aceitação de Certificado

Nada a assinalar.

4.6.6. Publicação de Certificado após Renovação

Nada a assinalar.

4.6.7. Notificação da Emissão do Certificado a Outras Entidades

Nada a assinalar.

4.7. Renovação do Certificado com Geração de novo par de Chaves

O NOSI CA assume a renovação de certificado com geração de novo par de chaves, sendo considerada sempre uma nova emissão.

4.7.1. Motivo para 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.

4.7.2. Quem pode submete o pedido de Certificado de uma nova chave Pública

Tal como na secção 4.1.1.

4.7.3. Processamento do pedido de Renovação do Certificado com Geração de novo par de Chave

Tal como na secção 4.1.2 e 4.2.

4.7.4. Notificação da Emissão de novo Certificado ao Titular

Tal como na secção 4.3.2.

4.7.5. Procedimentos para aceitação de um Certificado com Geração de novo par de Chaves

Tal como secção 4.4.1.

4.7.6. Publicação de Certificado Renovado com Geração de novo par de Chaves

Tal como secção 4.4.2.

4.7.7. Notificação da Emissão de Certificado Renovado a outras Entidades

Tal como secção 4.4.

4.8. Modificação de Certificado

Esta prática não é suportada pela PKI do NOSI CA.

A alteração de certificados é o processo em que é emitido um certificado para um titular, mantendo as respetivas chaves publicas, havendo apenas alterações na informação do certificado.

4.8.1. Motivos para Alteração do Certificado

Nada a assinalar.

4.8.2. Quem pode submeter o pedido de Alteração de Certificado

Nada a assinalar.

4.8.3. Processamento do pedido de Alteração de Certificado

Nada a assinalar.

4.8.4. Notificação da Emissão de Certificado Alterado ao Titular

Nada a assinalar.

4.8.5. Procedimentos para Aceitação de Certificado Alterado

Nada a assinalar.

4.8.6. Publicação do Certificado Alterado

Nada a assinalar.

4.8.7. Notificação da Emissão de Certificado alterado a outras Entidades

Nada a assinalar.

4.9. 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.

4.9.1. Motivos para a Suspensão

O NOSICA, suspende os certificados nas circunstâncias seguintes:

a) A Pedido do próprio titular, devidamente identificado para o efeito
b) Suspeita de comprometimento da chave privada;
c) Suspeita de perda da chave privada;
d) Suspeita de perda, destruição ou deterioração do dispositivo de suporte da chave privada (por exemplo, suporte/token criptográfico);

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

4.9.2. Quem pode Submeter o Pedido de Suspensão

O pedido de suspensão só pode ser submetido pelo titular do certificado, devidamente identificado e sempre que se verifiquem alguma das condições descritas no ponto 4.9.1.

4.9.3. Procedimentos para Pedido de Suspensão

A suspensão poderá ser solicitada através de contacto direto com a NOSI CA (em dias úteis) a qual fornecerá todas as indicações necessárias para proceder a suspensão do certificado.

4.9.4. Limite do Período de Suspensão

O Certificado é suspenso pelo período de tempo definido no plano de segurança da NOSI CA, que em todo o caso não poderá ser superior a 3 (três) dias úteis.

4.9.5. Motivos para Revogação

Um certificado pode ser revogado por uma das seguintes razões:

a) Comprometimento da chave privada;
b) Perda ou roubo do cartão/token;
c) Atualização/alteração de dados;
d) Deterioração do cartão/token;
e) Utilização do certificado para atividades abusivas;

f) Falha na utilização do cartão/token;

g) 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

h) Cessação de funções do NOSI CA sem ter transmitido a sua documentação a outra entidade certificadora;

i) Se após pedido de suspensão pelo titular ultrapassar os 3 dias sem que este efetue o pedido de renovação;

j) Quando o NOSI CA tomar conhecimento do falecimento, interdição ou inabilitação do titular do certificado.

Após revogação de Certificado o NOSI CA não irá emitir certificado referente aos mesmos dados de criação de assinatura.

4.9.6. 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 4.9.5, as seguintes entidades:

- O próprio titular do certificado, devidamente identificado para o efeito;
- Uma parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos.

O NOSI CA, guarda toda a documentação utilizada para verificação da identidade e autenticidade da pessoa que efetua o pedido de revogação, garantindo a verificação da identidade do titular, por meio legalmente reconhecido, não aceitando poderes de representação para o pedido de revogação de certificados.

4.9.7. Procedimentos para Pedido de Revogação

De acordo com a secção 4.9.7. da DPC do NOSI CA.

4.9.8. Prazo para Processar o Pedido de Revogação

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

4.9.9. 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. A revogação do certificado não tem efeitos retroativos.

4.9.10. 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).

4.9.11. Periodicidade da Emissão da Lista de Certificados Revogados (CRL)

O NOSI CA disponibiliza uma nova CRL Base diariamente.

4.9.12. 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.

4.9.13. Disponibilidade de Verificação Online do Estado / Revogação de Certificado

O NOSI CA dispõe de serviços de validação OCSP do estado dos certificados online. Esse serviço poderá ser acedido em (https://ocsp.nosi.cv/ejbca/publicweb/status/ocsp).

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

4.9.14. Requisitos de Verificação Online

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

4.9.15. Outras formas Disponíveis de Notificação da Revogação

O titular do certificado é notificado via e-mail, sempre que o certificado for revogado.

4.9.16. Requisitos Especiais em caso de Comprometimento de Chave Privada

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

As respostas a esse incidente podem incluir:

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

Renovação de todos os certificados emitidos no “ramo” da hierarquia de confiança do NOSI CA.

4.10. 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.

4.10.1. Motivos para a Suspensão

O NOSICA, suspende os certificados nas circunstâncias seguintes:

g) A Pedido do próprio titular, devidamente identificado para o efeito

h) Suspeita de comprometimento da chave privada;
i) Suspeita de perda da chave privada;
j) Suspeita de perda, destruição ou deterioração do dispositivo de suporte da chave privada (por exemplo, suporte/token criptográfico);
k) Sempre que haja razões credíveis que induzam a suspeita que o serviços de certificação possam ter sido comprometidos, de tal forma que coloquem em causa a fiabilidade dos certificados;
l) 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

4.10.2. Quem pode Submeter o Pedido de Suspensão

O pedido de suspensão só pode ser submetido pelo titular do certificado, devidamente identificado e sempre que se verifiquem alguma das condições descritas no ponto 4.9.1.

4.10.3. Procedimentos para Pedido de Suspensão

A suspensão poderá ser solicitada através de contacto direto com a NOSI CA (em dias úteis) a qual fornecerá todas as indicações necessárias para proceder a suspensão do certificado.

4.10.4. Limite do Período de Suspensão

O Certificado é suspenso pelo período de tempo definido no plano de segurança da NOSI CA, que em todo o caso não poderá ser superior a 3 (três) dias úteis.

4.10.5. Motivos para Revogação

Um certificado pode ser revogado por uma das seguintes razões:

k) Comprometimento da chave privada;

l) Perda ou roubo do cartão/token;
m) Atualização/alteração de dados;
n) Deterioração do cartão/token;
o) Utilização do certificado para atividades abusivas;
p) Falha na utilização do cartão/token;
q) 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
r) Cessação de funções do NOSI CA sem ter transmitido a sua documentação a outra entidade certificadora;
s) Se após pedido de suspensão pelo titular ultrapassar os 3 dias sem que este efetue o pedido de renovação;
t) Quando o NOSI CA tomar conhecimento do falecimento, interdição ou inabilitação do titular do certificado.

Após revogação de Certificado o NOSI CA não irá emitir certificado referente aos mesmos dados de criação de assinatura.

4.10.6. 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 4.9.5, as seguintes entidades:

- O próprio titular do certificado, devidamente identificado para o efeito;
- Uma parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos.

O NOSI CA, guarda toda a documentação utilizada para verificação da identidade e autenticidade da pessoa que efetua o pedido de revogação por um período n\ao inferior a 20 anos, garantindo a verificação da identidade do titular, por meio legalmente reconhecido, não aceitando poderes de representação para o pedido de

revogação de certificados.

4.10.7. Procedimentos para Pedido de Revogação

De acordo com a secção 4.9.7. da DPC do NOSI CA.

4.10.8. Prazo para Processar o Pedido de Revogação

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

4.10.9. 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. A revogação do certificado não tem efeitos retroativos.

4.10.10. 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).

4.10.11. Periodicidade da Emissão da Lista de Certificados Revogados (CRL)

O NOSI CA disponibiliza uma nova CRL Base diariamente.

4.10.12. 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.

4.10.13. Disponibilidade de Verificação Online do Estado / Revogação de Certificado

O NOSI CA dispõe de serviços de validação OCSP do estado dos certificados online. Esse serviço poderá ser acedido em

(https://ocsp.nosi.cv/ejbca/publicweb/status/ocsp).

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

4.10.14. Requisitos de Verificação Online

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

4.10.15. Outras formas Disponíveis de Notificação da Revogação

O titular do certificado é notificado via e-mail, sempre que o certificado for revogado.

4.10.16. Requisitos Especiais em caso de Comprometimento de Chave Privada

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

As respostas a esse incidente podem incluir:

- Revogação do certificado do NOSI CA e de todos os certificados emitidos no "ramo" da hierarquia de confiança do NOSI CA;
- Notificação da Autoridade Credenciadora e todos os titulares de certificados emitidos no "ramo" da hierarquia de confiança do NOSI CA;
- Geração de novo par de chaves para o NOSI CA;

Renovação de todos os certificados emitidos no "ramo" da hierarquia de confiança do NOSI CA.

4.11. Fim Subscrição

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

a) Revogação do certificado;
b) Por ter caducado o prazo de validade do certificado.

4.12. Retenção e recuperação de chaves

A PKI do NOSI só efetua a retenção da sua chave privada.

5. Medidas de segurança física de gestão e operacionais

Descrito no capítulo 5 da Declaração de Prática de Certificação do NOSI CA disponível https://pki.nosi.cv.

6. Medidas de Segurança Técnicas

Descrito no capítulo 6 da Declaração de Prática de Certificação disponível https://pki.nosi.cv.

7. Perfis de Certificado, CRL e OCSP

7.1. 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 os certificados das EC´s que assinaram este e assim consecutivamente até chegar à EC Raiz.

O perfil do certificado do NOSICA – G2, está de acordo com os requisitos da ICP-CV e com os seguintes standards:

a. RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework;
b. RFC 5280 - Internet X.509 PKI - Certificate and CRL Profile;
c. ETSI EN 319 412
d. Legislação Cabo-verdiana.

7.1.1. Número Versão

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

7.1.2. Extensões do Certificado

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

7.1.3. OID do Algoritmo

O campo “signature Algorithm” do certificado contém o OID do algoritmo criptográfico utilizado pela EC para assinar o certificado: x.x.x.x.x.x.xx (sha256WithRSA).

7.1.4. Formato de Nomes

Tal como definido em 3.1.

7.1.5. Condicionantes 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 do NOSI CA.

7.1.6. OID da Política de certificados

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

7.1.7. Utilização da Extensão Policy Contraints

Nada a assinalar.

7.1.8. Sixtaxe e Semântica 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.

7.1.9. Semântica de Processamento para a Extensão Crítica Certificate Policies

Nada a assinalar.

7.1.10. PERFIL DE CERTIFICADO DE ASSINATURA DIGITAL QUALIFICADO DE QUALIDADE (ORDEM PROFISSIONAL)

Componente do Certificado		Secção no RFC 5280	Valor	Tipos	Comentários
tbsCertificate	**Version**	4.1.2.1	2	m	O valor 2 identifica a utilização do certificado 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"		País do titular
	Organization (O)		"ICP-CV"		
	Organization Unit (OU)		"NOSI – Nucleo Operacional da Sociedade de Informacao"		
	Common Name (CN)		"NOSICA - G2"		Nome da EC
	Validity	4.1.2.5		m	Validade do Certificado
	Not Before		<data de emissão>		Validade máxima de 5 anos e 2 meses
	Not After		<data de emissão + máximo de 5 anos>		Validade máxima de 5 anos e 2 meses.
	Subject	4.1.2.6		m	
	Country (C)		<CV>		

	Organization (O)		<Organização à qual o titular do certificado pertence>	o	
	Organization Unit (OU)		<Área/Departamento da Organização à qual o titular do certificado pertence>	o	
	Organization Unit (OU)		Certificado para pessoa singular Assinatura Qualificada		Designação do tipo de certificado.
	Locality (L)		<Localidade de residência do titular>	o	<Localidade><Município><Ilha>
	Common Name (CN)		<nome do titular do certificado>		Nome completo do titular
	Title (title)		<Qualidade do titular do certificado, no âmbito da sua utilização para assinatura digital qualificada> - Informação confirmada pela Entidade de Certificação apenas na data de emissão e que não foi confirmada posteriormente a essa data, ou informação similar.	o	Opcional. Somente em caso de qualidade profissional Nas Entidades de Registo específicas com âmbitos restritos, nomeadamente as ordens profissionais, este campo é constituído por <Nº da cédula profissional>
	Surname (SN)		<Nomes de família do titular do certificado>	o	
	Given Name (givenName)		<Nomes próprio do titular do certificado>	o	
	Serial Number (serialNumber)		<Identificador único do titular do certificado>	o	Num âmbito geral, este campo assume os valores **NIC** ou **PAS** seguido do código do país do nº associado. A estrutura é a seguinte: <doc de identificação><código do país>-<nº de identificação>, (exemplo IDCCV-J12345678)
	Subject Public Key Info	4.1.2.7		m	Utilizado para conter a chave pública e identificar o algoritmo com o qual a chave é utilizada (e.g., RSA, DSA ou Diffie-Hellman).

	algorithm		1.2.840.113549.1.1.1		O OID rsaEncryption identifica chaves públicas RSA. pkcs-1 OBJECT IDENTIFIER ::= { iso(1) memberbody(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.10
	subjectPublicKey		<Chave Pública com *modulus* n de 2048 bits>		
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		o	
	keyIdentifier		O *key Identifier* é composto pela *hash* de 160-bit SHA-1	m	O key Identifier é composto pela hash de 160-bit SHA-1 do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>
	Subject Key Identifier	4.2.1.2	O *key Identifier* é composto pela hash de 160-bit SHA-1	m	O key Identifier é composto pela hash de 160-bit SHA-1 do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>
	Key Usage	4.2.1.3		mc	Esta extensão é marcada CRÍTICA
	Digital Signature		“0” selecionado		
	Non Repudiation		“1” selecionado		
	Key Encipherment		“0” selecionado		
	Data Encipherment		“0” selecionado		
	Key Agreement		“0” selecionado		

	Key Certificate Signature		“0” selecionado		
	CRL Signature		“0” selecionado		
	Encipher Only		“0” selecionado		
	Decipher Only		“0” selecionado		
	Certificate Policies	4.2.1.4		o	
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.1.2_ OID da PC	m	Identificador da Politica de Certificados
	policyQualifiers		https://pki.nosi.cv/pc_nosica-g2.pdf		Contém um apontador para a Politica de Certificados publicada pela NOSI CA. O apontador está na forma de um URI."
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.1.3_ OID da DPC	o	Identificador da Declaração de Práticas de Certificados
	policyQualifiers		https://pki.nosi.cv/dpc_nosica-g2.pdf	o	Contém um apontador para a Declaração de Prática de Certificados publicada pela NOSI CA. O apontador está na forma de um URL."
	Basic Constraints	4.2.1.9		c	Esta extensão é marcada CRÍTICA.
	CA		FALSE		
	Extended Key Usage	4.2.1.12			
	KeyPurposeId		id-kp-emailProtection		OID: 1.3.6.1.5.5.7.3.4
	CRLDistributionPoints	4.2.1.13		o	
	distributionPoint		https://crl.nosi.cv/nosica-g2.crl	o	URL para aceder a CRL

	Subject Alternative name	4.2.1.6			
	Qualified Certificate Statement		id-pe-qcStatements = “1.3.6.1.5.5.7.1.3”[1]		A extensão QCStatements é uma extensão introduzida pelo PKIX Qualified Certificate Profile11 e ETSI .
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcCompliance = "0.4.0.1862.1.1"		Declaração do NOSI CA, representada por um OID, indicando que este certificado é emitido de acordo com o Anexo III do Regulamento (EU) 910/2014).
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcSSCD = " 0.4.0.1862.1.4"		Declaração efetuada pelo NOSI CA, indicando que a chave privada associada à chave pública no certificado está guardada num dispositivo qualificado de criação de selo eletrónico, de acordo com o Anexo III do Regulamento (EU) 910/2014. Esta declaração indica que os certificados são emitidos em conformidade com a política SSCD, conforme ETSI TS 101 456.
	Internet Certificate Extensions				
	Authority Information Access	4.2.2.1		o	
	accessMethod		1.3.6.1.5.5.7.48.1	o	Valor do OID: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp)
	accessLocation		https://ocsp.nosi.cv/ejbca/publicweb/status/ocsp	o	URL para aceder ao OCSP
	Signature Algorithm	4.1.1.2	2.16.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha-256WithRSA OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}

	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.

7.1.11. PERFIL DE CERTIFICADO QUALIFICADO DE ASSINATURA DIGITAL PARA REPRESENTAÇÂO DE PESSOA COLETIVA

Componente do Certificado		Secção no RFC 5280	Valor	Tipos	Comentários
tbsCertificate	**Version**	4.1.2.1	2	m	O valor 2 identifica a utilização do certificado ITU-T X.509 Versão 3
	Serial Number	4.1.2.2	<atribuido 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"		País do titular
	Organization (O)		"ICP-CV"		
	Organization Unit (OU)		"NOSI – Nucleo Operacional da Sociedade de Informacao"		
	Common Name (CN)		"NOSICA - G2"		Nome da EC
	Validity	4.1.2.5		m	Validade do Certificado
	Not Before		<data de emissão>		Validade máxima de 5 anos e 2 meses
	Not After		<data de emissão + máximo de 5 anos>		Validade máxima de 5 anos e 2 meses.
	Subject	4.1.2.6		m	
	Country (C)		<CV>		

	Organization (O)		<Organização à qual o titular do certificado pertence>	o	
	Organization Unit (OU)		<Área/Departamento da Organização à qual o titular do certificado pertence>	o	
	Organization Unit (OU)		Certificado Qualificado de Representação Pessoa Coletiva		Designação do tipo de certificado.
	Organization Identifier (OI)		**VATCV-(Número de NIF)**	m	**VAT<País>-<Número do de identificação Fiscal>**
	Locality (L)		<Localidade de residência do titular>	o	<Localidade><Município><Ilha>
	Common Name (CN)		<nome do titular do certificado>		Nome completo do titular
	Title (title)		<Qualidade do titular do certificado, no âmbito da sua utilização para assinatura digital qualificada> - Informação confirmada pela Entidade de Certificação apenas na data de emissão e que não foi confirmada posteriormente a essa data, ou informação similar.	o	Opcional. Somente em caso de qualidade profissional Nas Entidades de Registo específicas com âmbitos restritos, nomeadamente as ordens profissionais, este campo é constituído por <Nº da cédula profissional>
	Surname (SN)		<Nomes de família do titular do certificado>	o	
	Given Name (givenName)		<Nomes próprio do titular do certificado>	o	
	Serial Number (serialNumber)		<Identificador único do titular do certificado>	o	Num âmbito geral, este campo assume os valores **NIC** ou **PAS** seguido do código do país do nº associado. A estrutura é a seguinte: <doc de identificação><código do país>-<nº de identificação>, (exemplo IDCCV-J12345678)
	Subject Public Key Info	4.1.2.7		m	Utilizado para conter a chave pública e identificar o algoritmo com o qual a chave é utilizada (e.g., RSA, DSA ou Diffie-Hellman).

	algorithm		1.2.840.113549.1.1.1		O OID rsaEncryption identifica chaves públicas RSA. pkcs-1 OBJECT IDENTIFIER ::= { iso(1) memberbody(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.10
	subjectPublicKey		<Chave Pública com *modulus* n de 2048 bits>		
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		o	
	keyIdentifier		O *key Identifier* é composto pela *hash* de 160-bit SHA-1	m	O key Identifier é composto pela hash de 160-bit SHA-1 do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>
	Subject Key Identifier	4.2.1.2	O *key Identifier* é composto pela hash de 160-bit SHA-1	m	O key Identifier é composto pela hash de 160-bit SHA-1 do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>
	Key Usage	4.2.1.3		mc	Esta extensão é marcada CRÍTICA
	Digital Signature		“0” selecionado		
	Non Repudiation		“1” selecionado		
	Key Encipherment		“0” selecionado		
	Data Encipherment		“0” selecionado		
	Key Agreement		“0” selecionado		

	Key Certificate Signature		“0” selecionado		
	CRL Signature		“0” selecionado		
	Encipher Only		“0” selecionado		
	Decipher Only		“0” selecionado		
	Certificate Policies	4.2.1.4		o	
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.1.2- OID da PC	m	Identificador da Politica de Certificado
	policyQualifiers		https://pki.nosi.cv/pc_nosica-g2.pdf		Contém um apontador para a Politica de Certificados publicada pela NOSI CA. O apontador está na forma de um URI."
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.2 userNotice explicitText: “O certificado emitido segundo esta política é equivalente a um certificado digital qualificado, nos termos definidos na legislação de Cabo Verde aplicável para o efeito.”		Valor do OID: 1.3.6.1.5.5.7.2.2 (id-qt-unotice) Descrição do OID: "User notice é utilizado para apresentar às partes confiantes quando um certificado é utilizado” (http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5. 7.2.2.html)
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.1.3- OID da DPC	o	Identificador da Declaração de Práticas de Certificados
	policyQualifiers		https://pki.nosi.cv/dpc_nosica-g2.pdf	o	Contém um apontador para a Declaração de Prática de Certificados publicada pela NOSI CA. O apontador está na forma de um URL."
	Basic Constraints	4.2.1.9		c	Esta extensão é marcada CRÍTICA.

	CA		FALSE		
	Extended Key Usage	4.2.1.12			
	KeyPurposeId		id-kp-emailProtection		OID: 1.3.6.1.5.5.7.3.4
	CRLDistributionPoints	4.2.1.13		o	
	distributionPoint		https://pki.nosi.cv/crls/nosica-g2.crl	o	URL para aceder a CRL
	Subject Alternative name	4.2.1.6			
	Qualified Certificate Statement		id-pe-qcStatements = “1.3.6.1.5.5.7.1.3”[1]		A extensão QCStatements é uma extensão introduzida pelo PKIX Qualified Certificate Profile11 e ETSI .
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcCompliance = "0.4.0.1862.1.1"		Declaração do NOSI CA, representada por um OID, indicando que este certificado é emitido de acordo com o Anexo III do Regulamento (EU) 910/2014).
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcSSCD = " 0.4.0.1862.1.4"		Declaração efetuada pelo NOSI CA, indicando que a chave privada associada à chave pública no certificado está guardada num dispositivo qualificado de criação de selo eletrónico, de acordo com o Anexo III do Regulamento (EU) 910/2014. Esta declaração indica que os certificados são emitidos em conformidade com a política SSCD, conforme ETSI TS 101 456.
	Internet Certificate Extensions				
	Authority Information Access	4.2.2.1		o	

	accessMethod		1.3.6.1.5.5.7.48.1	o	Valor do OID: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp)
	accessLocation		https://ocsp.nosi.cv/ejbca/publicweb/status/ocsp	o	URL para aceder ao OCSP
	Signature Algorithm	4.1.1.2	2.16.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha-256WithRSA OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}
	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.

7.1.12. PERFIL DE CERTIFICADO QUALIFICADA DE ASSINATURA DIGITAL PARA PESSOA SINGULAR

Componente do Certificado		Secção no RFC 5280	Valor	Tipos	Comentários
tbsCertificate	**Version**	4.1.2.1	2	m	O valor 2 identifica a utilização do certificado ITU-T X.509 Versão 3
	Serial Number	4.1.2.2	<atribuido 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"		País do titular
	Organization (O)		"ICP-CV"		
	Organization Unit (OU)		"NOSI – Nucleo Operacional da Sociedade de Informacao"		
	Common Name (CN)		"NOSICA - G2"		Nome da EC
	Validity	4.1.2.5		m	Validade do Certificado
	Not Before		<data de emissão>		Validade máxima de 5 anos e 2 meses
	Not After		<data de emissão + máximo de 5 anos>		Validade máxima de 5 anos e 2 meses.
	Subject	4.1.2.6		m	
	Country (C)		<CV>		
	Organization (O)		<Organização à qual o titular do certificado pertence>	o	

	Organization Unit (OU)		<Área/Departamento da Organização à qual o titular do certificado pertence>	o	
	Organization Unit (OU)		Certificado Assinatura Qualificada para Pessoa Singular		Designação do tipo de certificado.
	Locality (L)		<Localidade de residência do titular>	o	<Localidade><Município><Ilha>
	Common Name (CN)		<nome do titular do certificado>		Nome completo do titular
	Title (title)		<Qualidade do titular do certificado, no âmbito da sua utilização para assinatura digital qualificada> - Informação confirmada pela Entidade de Certificação apenas na data de emissão e que não foi confirmada posteriormente a essa data, ou informação similar.	o	Opcional. Somente em caso de qualidade profissional Nas Entidades de Registo específicas com âmbitos restritos, nomeadamente as ordens profissionais, este campo é constituído por <Nº da cédula profissional>
	Surname (SN)		<Nomes de família do titular do certificado>	o	
	Given Name (givenName)		<Nomes próprio do titular do certificado>	o	
	Serial Number (serialNumber)		<Identificador único do titular do certificado>	o	Num âmbito geral, este campo assume os valores **NIC** ou **PAS** seguido do código do país do nº associado. A estrutura é a seguinte: <doc de identificação><código do país>-<nº de identificação>, (exemplo IDCCV-J12345678)
	Subject Public Key Info	4.1.2.7		m	Utilizado para conter a chave pública e identificar o algoritmo com o qual a chave é utilizada (e.g., RSA, DSA ou Diffie-Hellman).
	algorithm		1.2.840.113549.1.1.1		O OID rsaEncryption identifica chaves públicas RSA. pkcs-1 OBJECT IDENTIFIER ::= { iso(1) memberbody(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.10

	subjectPublicKey		<Chave Pública com *modulus* n de 2048 bits>		
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		o	
	keyIdentifier		O *key Identifier* é composto pela *hash* de 160-bit SHA-1	m	O key Identifier é composto pela hash de 160-bit SHA-1 do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>
	Subject Key Identifier	4.2.1.2	O *key Identifier* é composto pela hash de 160-bit SHA-1	m	O key Identifier é composto pela hash de 160-bit SHA-1 do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>
	Key Usage	4.2.1.3		mc	Esta extensão é marcada CRÍTICA
	Digital Signature		"0" selecionado		
	Non Repudiation		"1" selecionado		
	Key Encipherment		"0" selecionado		
	Data Encipherment		"0" selecionado		
	Key Agreement		"0" selecionado		
	Key Certificate Signature		"0" selecionado		
	CRL Signature		"0" selecionado		
	Encipher Only		"0" selecionado		

	Decipher Only		“0” selecionado		
	Certificate Policies	4.2.1.4		o	
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.1.2- OID da PC	m	Identificador da Politica de Certificado de Assinatura Digital Qualificada
	policyQualifiers		https://pki.nosi.cv/pc_nosica-g2.pdf		Contém um apontador para a Politica de Certificados Qualificados publicada pela NOSI CA. O apontador está na forma de um URI."
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.1.2- OID da DPC	o	Identificador da Declaração de Práticas de Certificação
	policyQualifiers		https://pki.nosi.cv/dpc_nosica-g2.pdf	o	Contém um apontador para a Declaração de Prática de Certificados publicada pela NOSI CA. O apontador está na forma de um URL."
	Basic Constraints	4.2.1.9		c	Esta extensão é marcada CRÍTICA.
	CA		FALSE		
	Extended Key Usage	4.2.1.12			
	KeyPurposeId		id-kp-emailProtection		OID: 1.3.6.1.5.5.7.3.4
	CRLDistributionPoints	4.2.1.13		o	
	distributionPoint		https://pki.nosi.cv/crls/nosica-g2.crl	o	URL para aceder a CRL
	Subject Alternative name	4.2.1.6			

	Qualified Certificate Statement		id-pe-qcStatements = “1.3.6.1.5.5.7.1.3”[1]		A extensão QCStatements é uma extensão introduzida pelo PKIX Qualified Certificate Profile11 e ETSI .
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcCompliance = "0.4.0.1862.1.1"		Declaração do NOSI CA, representada por um OID, indicando que este certificado é emitido de acordo com o Anexo III do Regulamento (EU) 910/2014).
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcSSCD = " 0.4.0.1862.1.4"		Declaração efetuada pelo NOSI CA, indicando que a chave privada associada à chave pública no certificado está guardada num dispositivo qualificado de criação de selo eletrónico, de acordo com o Anexo III do Regulamento (EU) 910/2014. Esta declaração indica que os certificados são emitidos em conformidade com a política SSCD, conforme ETSI TS 101 456.
	Internet Certificate Extensions				
	Authority Information Access	4.2.2.1		o	
	accessMethod		1.3.6.1.5.5.7.48.1	o	Valor do OID: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp)
	accessLocation		https://ocsp.nosi.cv/ejbca/publicweb/status/ocsp	o	URL para aceder ao OCSP
	Signature Algorithm	4.1.1.2	2.16.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha-256WithRSA OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}
	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.

7.1.13. PERFIL DE CERTIFICADO QUALIFICADO DE SELO ELETRÓNICO

Componente do Certificado		Secção no RFC 5280	Valor	Tipos	Comentários
tbsCertificate	**Version**	4.1.2.1	2	m	O valor 2 identifica a utilização do certificado 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"		País do titular
	Organization (O)		"ICP-CV"		
	Organization Unit (OU)		"NOSI – Nucleo Operacional da Sociedade de Informacao"		
	Common Name (CN)		"NOSICA - G2"		Nome da EC
	Validity	4.1.2.5		m	Validade do Certificado TEM que utilizar tempo UTC até 2049, passando a partir daí a utilizar GeneralisedTime
	Not Before		<data de emissão>		
	Not After		<data de emissão + máximo de 5 anos>		Validade máxima de 5 anos e 2 meses.
	Subject	4.1.2.6		m	
	Country (C)		<CV>		

	Organization Unit (OU)		<Área/Departamento da Organização>	m	
	Organization Unit (OU)		**Certificado Qualificado de Selo Eletrónico**	m	Designação do tipo de certificado.
	Organization Identifier (OI)		**VATCV-(Número de NIF)**	m	**VAT<País>-<Número do de identificação Fiscal>**
	Organization (O)		<Nome da Organização tal como registada nas entidades competentes>	m	
	Common Name (CN)		<Nome da organização pela qual é conhecida>	m	
	Subject Public Key Info	4.1.2.7		m	Utilizado para conter a chave pública e identificar o algoritmo com o qual a chave é utilizada (e.g., RSA, DSA ou Diffie-Hellman).
	algorithm		1.2.840.113549.1.1.1		O OID rsaEncryption identifica chaves públicas RSA. pkcs-1 OBJECT IDENTIFIER ::= { iso(1) memberbody(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.10
	subjectPublicKey		<Chave Pública com *modulus* n de 2048 bits>		
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		o	
	keyIdentifier		O *key Identifier* é composto pela *hash* de 160-bit SHA-1	m	O key Identifier é composto pela hash de 160-bit SHA-1 do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>

	Subject Key Identifier	4.2.1.2	O key Identifier é composto pela hash de 160-bit SHA-1 do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>	m	
	Key Usage	4.2.1.3		mc	Esta extensão é marcada CRÍTICA
	Digital Signature		“0” selecionado		
	Non Repudiation		“1” selecionado		certKeyUsage KeyUsage ::= {nonRepudiation}
	Key Encipherment		“1” selecionado		
	Data Encipherment		“0” selecionado		
	Key Agreement		“0” selecionado		
	Key Certificate Signature		“0” selecionado		
	CRL Signature		“0” selecionado		
	Encipher Only		“0” selecionado		
	Decipher Only		“0” selecionado		
	Certificate Policies	4.2.1.4		o	
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.1.3_ OID da PC	m	Identificador da Politica de Certificado
	policyQualifiers		https://pki.nosi.cv/pc_nosica-g2.pdf		Contém um apontador para a Politica de Certificados publicada pela NOSI CA. O apontador está na forma de um URI."
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.2 userNotice explicitText: “O certificado emitido segundo esta política é equivalente a um certificado digital		Valor do OID: 1.3.6.1.5.5.7.2.2 (id-qt-unotice)

			qualificado, nos termos definidos na legislação de Cabo Verde aplicável para o efeito.”		Descrição do OID: "User notice é utilizado para apresentar às partes confiantes quando um certificado é utilizado” (http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.2.html)
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.7_ OID da DPC	o	Identificador da Declaração de Práticas de Certificados
	policyIdentifier		https://pki.nosi.cv/dpc_nosica-g2.pdf		Contém um apontador para a Declaração de Prática de Certificado publicada pela NOSI CA. O apontador está na forma de um URI."
	Basic Constraints	4.2.1.9		c	Esta extensão é marcada CRÍTICA.
	CA		FALSE		
	Extended Key Usage	4.2.1.12			
	KeyPurposeId		id-kp-emailProtection		OID: 1.3.6.1.5.5.7.3.4
	CRLDistributionPoints	4.2.1.13		o	
	distributionPoint		https://crl.nosi.cv/nosica-g2.crl	o	URL para aceder a CRL
	Subject Alternative name	4.2.1.6	RFC822 name = <endereço do correio eletrónico do titular do certificado>	o	
	Qualified Certificate Statement		id-pe-qcStatements = “1.3.6.1.5.5.7.1.3”[1]		A extensão QCStatements é uma extensão introduzida pelo PKIX Qualified Certificate Profile11 e ETSI .
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcCompliance = "0.4.0.1862.1.1"		Declaração do NOSI CA, representada por um OID, indicando que este certificado é emitido de acordo com o Anexo III do Regulamento (EU) 910/2014).

	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcSSCD = " 0.4.0.1862.1.4"		Declaração efetuada pela do NOSI CA, indicando que a chave privada associada à chave pública no certificado está guardada num dispositivo qualificado de criação de selo eletrónico, de acordo com o Anexo III do Regulamento (EU) 910/2014. Esta declaração indica que os certificados são emitidos em conformidade com a política SSCD, conforme ETSI TS 101 456.
	id-qcs-pkixQCSyntax-v2		id-etsi-qct-esign="0.4.0.1862.1.6.1" Text="Certificate for electronic signatures as defined in Regulation (EU) No 910/2014"		Declaração da NOSI CA, representada por um OID, indicando que este certificado é emitido como um certificado qualificado de selo eletrónico, de acordo com o Anexo III do Regulamento (EU) 910/2014.
	Internet Certificate Extensions				
	Authority Information Access	4.2.2.1		o	
	accessMethod		1.3.6.1.5.5.7.48.1	o	Valor do OID: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp)
	accessLocation		https://ocsp.nosi.cv/ejbca/publicweb/status/ocsp	o	URL para aceder ao OCSP
	Signature Algorithm	4.1.1.2	2.16.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha-256WithRSA OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}
	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.

7.1.14. PERFIL DE CERTIFICADO AVANÇADO DE AUTENTICAÇÃO

Componente do Certificado		Secção no RFC 5280	Valor	Tipos	Comentários
tbsCertificate	**Version**	4.1.2.1	v3	m	Versão do certificado de acordo com o standard X.509
	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"		País do titular
	Organization (O)		"ICP-CV"		
	Organization Unit (OU)		"NOSI – Nucleo Operacional da Sociedade de Informacao"		
	Common Name (CN)		"NOSICA - G2"		Nome da EC
	Validity	4.1.2.5		m	Validade do Certificado
	Not Before		<data de emissão>		Validade máxima de 5 anos e 2 meses
	Not After		<data de emissão + máximo de 5 anos>		Validade máxima de 5 anos e 2 meses.
	Subject	4.1.2.6		m	
	Country (C)		<CV>		
	Organization (O)		<Organização à qual o titular do certificado pertence>	o	
	Organization Unit (OU)		<Área/Departamento da Organização à qual o titular do certificado pertence>	o	
	Organization Unit (OU)		Certificado para Pessoa Singular Autenticacao	m	Designação do tipo de certificado.

	Common Name (CN)		<nome do titular do certificado>	m	Nome completo do titular
	Title (title)		<Qualidade do titular do certificado, no âmbito da sua utilização para autenticação> - "Informação confirmada pela Entidade de Certificação apenas na data de emissão e que não foi confirmada posteriormente a essa data", ou informação similar.	o	
	Surname (SN)		<Nomes de família do titular do certificado>	o	
	Given Name (givenName)		<Nomes próprio do titular do certificado>	o	
	Serial Number (serialNumber)		<Identificador único do titular do certificado>	o	Corresponde ao NIF do titular.
	Subject Public Key Info	4.1.2.7		m	Utilizado para conter a chave pública e identificar o algoritmo com o qual a chave é utilizada (e.g., RSA, DSA ou Diffie-Hellman).
	algorithm		1.2.840.113549.1.1.1		O OID rsaEncryption identifica chaves públicas RSA. pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 } rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1} O OID rsaEncryption deve ser utilizado no campo algorithm com um valor do tipo AlgorithmIdentifier. Os parâmetros do campo TÊM que ter o tipo ASN.1 a NULL para oidentificador deste algoritmo.24.
	subjectPublicKey		<Chave Pública com *modulus* n de 2048 bits>		
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		o	
	keyIdentifier		O *key Identifier* é composto pela *hash* de 160-bit SHA-1	m	O key Identifier é composto pela hash de 160-bit SHA-1 do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>

	Subject Key Identifier	4.2.1.2	O *key Identifier* é composto pela hash de 160-bit SHA-1	m	O key Identifier é composto pela hash de 160-bit SHA-1 do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>
	Key Usage	4.2.1.3		mc	Esta extensão é marcada CRÍTICA
	Digital Signature		"1" selecionado		
	Non Repudiation		"0" selecionado		
	Key Encipherment		"0" selecionado		
	Data Encipherment		"0" selecionado		
	Key Agreement		"0" selecionado		
	Key Certificate Signature		"0" selecionado		
	CRL Signature		"0" selecionado		
	Encipher Only		"0" selecionado		
	Decipher Only		"0" selecionado		
	Certificate Policies	4.2.1.4		o	
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.1.3 OID da PC	m	Identificador da Politica de Certificado
	policyQualifiers		https://pki.nosi.cv/pc_nosica-g2.pdf		Contém um apontador para a Politica de Certificado publicada pela EC. O apontador está na forma de um URI."
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.1.3 OID da DPC	m	Identificador da Declaração de Prática de Certificado
	policyQualifiers		https://pki.nosi.cv/dpc_nosica-g2.pdf		Contém um apontador para a Declaração de prática de Certificado publicada pela NOSI CA. O apontador está na forma de um URL."
	Basic Constraints	4.2.1.9		c	Esta extensão é marcada CRÍTICA.
	CA		FALSE		

	Extended Key Usage	4.2.1.12			
	KeyPurposeId		TLS Web Client Authentication		OID: 1.3.6.1.5.5.7.3.4
	CRLDistributionPoints	4.2.1.13		o	
	distributionPoint		https://crl.nosi.cv/nosica-g2.crl	o	URL para aceder a CRL
	Authority Information Access	4.2.2.1		o	
	accessMethod		1.3.6.1.5.5.7.48.1	o	Valor do OID: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp)
	accessLocation		https://ocsp.nosi.cv/ejbca/publicweb/status/ocsp	o	URL para aceder ao OCSP
	Signature Algorithm	4.1.1.2	2.16.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo
	Signature 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.

7.1.15. 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).

7.2. 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 o NOSI CA e a Entidade requerente. Este certificado difere dos certificados usuais, considerados finais no seguinte:

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

7.3. 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.

7.3.1. PERFIL DO CERTIFICADO DO CRL DO NOSI CA

Componente do Certificado		Secção no RFC 5280	Valor	Tipos	Comentários
tbsCertificate	**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	5.1.2.3		m	
	Country (C)		“CV”		País do titular
	Organization (O)		“ICP-CV”		
	Organization Unit (OU)		"NOSI – Nucleo Operacional da Sociedade de Informaçao"		
	Common Name (CN)		“NOSICA - G2”		Nome da EC
	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 CRL = thisUpdate + N>	m	Este campo indica a data em que a próxima CRL vai ser emitida. A próxima CRL pode ser emitida antes da data indicada, mas não será emitida depois dessa data. Os emissores da CRL DEVEM emitir CRL com o tempo de nextUpdate maior ou igual a todas as CRL 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	5.2.1		o	
	keyIdentifier		O key Identifier é composto pela hash de 160-bit SHA-256 do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>		
	CRL Number	5.2.3	<número sequencial único e incrementado>	m	
	CRL DistributionPoints	5.2.5		c	
	distributionPoint		https://crl.nosi.cv/nosica-g2.crl		URL para aceder a CRL
	CRL Entry Extensions	5.3		o	
	Reason Code	5.3.1			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.

7.4. 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

c) Outras normas e legislação aplicável

7.4.1. 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.

7.4.2. PERFIL DE CERTIFICADO DE OCSP DO NOSI CA

Componente do Certificado		Secção no RFC 5280	Valor	Tipos	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"		País do titular
	Organization (O)		"ICP-CV"		
	Organization Unit (OU)		"NOSI – Nucleo Operacional da Sociedade de Informaçao"		
	Common Name (CN)		"NOSICA - G2"		Nome da EC
	Validity	4.1.2.5		m	Validade do Certificado
	Not Before		<data de emissão>		TEM que utilizar tempo UTC até 2049, passando a partir daí a utilizar GeneralisedTime
	Not After		<data de emissão + máximo de 5 anos>		Validade máxima de 5 anos e 2 meses.
	Subject	4.1.2.6		m	
	Country (C)		"CV"		

	Organization (O)		“ICP-CV”		
	Organization Unit (OU)		“Validacao online”		
	Organization Unit (OU)		"NOSI – Nucleo Operacional da Sociedade de Informaçao"		
	Common Name (CN)		"Servico de Validacao Online da Nosi G2 <nnnn>"		<nnn> - sequencia do certificado
	Subject Public Key Info	4.1.2.7		m	Utilizado para conter a chave pública e identificar o algoritmo com o qual a chave é utilizada (e.g., RSA, DSA ou Diffie-Hellman).
	algorithm		1.2.840.113549.1.1.1		O OID rsaEncryption identifica chaves públicas RSA. pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 } rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1} O OID rsaEncryption deve ser utilizado no campo algorithm com um valor do tipo AlgorithmIdentifier. Os parâmetros do campo TÊM que ter o tipo ASN.1 a NULL para o identificador deste algoritmo.24
	subjectPublicKey		<Chave Pública com modulus n de 4096 bits>		
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		m	
	keyIdentifier		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	4.2.1.3		mc	Esta extensão é marcada CRÍTICA
	Digital Signature		“1” selecionado		
	Non Repudiation		“1” selecionado		
	Key Encipherment		“0” selecionado		
	Data Encipherment		“0” selecionado		
	Key Agreement		“0” selecionado		
	Key Certificate Signature		“0” selecionado		
	CRL Signature		“0” selecionado		
	Encipher Only		“0” selecionado		
	Decipher Only		“0” selecionado		
	Certificate Policies	4.2.1.4		o	
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.1.2_ OID da PC	m	Identificador da Politica de Certificado
	policyQualifiers		https://pki.nosi.cv/pc_nosica-g2.pdf		Contém um apontador para a Politica de Certificados publicada pela Nosi CA. O apontador está na forma de um URL."

	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.1.3_ OID da DPC	o	Identificador da Declaração de Práticas de Certificado
	policyQualifiers		https://pki.nosi.cv/dpc_nosica-g2.pdf	o	Contém um apontador para a Declaração de Prática de Certificados publicada pela NOSI CA. O apontador está na forma de um URL."
	Extended Key Usage	4.2.1.12		c	
	OCSP Signer		1.3.6.1.5.5.7.3.9		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	
	accessMethod		1.3.6.1.5.5.7.48.1	o	Valor do OID: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp)
	accessLocation		https://ocsp.nosi.cv/ejbca/publicweb/status/ocsp	o	URL para aceder ao OCSP

	Signature Algorithm	4.1.1.2	2.16.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha256WithRSA 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.

8. Auditoria e Avaliações de Conformidade

Descrito no capítulo 8 e na secção 9.14 (legislação e normas aplicáveis) da Declaração de Práticas de Certificação disponível em https://pki.nosi.cv.

9. Outras Situações e Assuntos Legais

Descrito no capítulo 9 da Declaração de Práticas de Certificação disponível em https://pki.nosi.cv.

10. 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] CABForum Baseline Requirements
[25] CABForum-EV-Guidelines –v1.7.0.