Declaração de práticas de certificação

informações gerais

Controle documental

Classificação de segurança:	Público
Versão:	4.2
Data de edição:	03/04/2024
Arquivo:	PSC-1.1-DPC_ES_v4.2
Código:	DPC-1.1-

estatuto formal

Preparado por:	Revisados pela:	Aprovado por:
Nome: Alejandro Grande Data: 03/04/2024	Nome: Donald David Márquez Data: 03/04/2024	Nome: Gabriel García Data: 03/04/2024

Controle de versão

Versão	Partes que mudam	Descrição da mudança	Autor da mudança	Data da mudança
1,0	Original	Criação de documento	GA/AC	22/03/2016
1.1	5.8	A comunicação é acrescentada ao Ministério em caso de cessação de atividade.	A.C.	24/05/2016
	6.1.1.1	Acrescenta-se que a UANATACA só pode criar as chaves através de um DCCF ou num HSM, e que a UANATACA nunca gera chaves em software para serem enviadas ao signatário.	A.C.	24/05/2016
	6.2.5	Acrescenta-se que a UANATACA não gera nem arquiva chaves de certificados, emitidas em software. O assinante não pode armazenar as chaves entregues no software.	A.C.	24/05/2016
	6.1.1	Foi corrigido o prazo de validade dos certificados UANATACA CA1 2016 e UANATACA CA2 2016.	A.C.	24/05/2016
1.2	1.1 1.2.1 1.4.1.5 1.4.1.6 1.4.1.7 1.4.1.8 3.1.1.5 3.1.1.6 6.1.1	Os perfis do certificado de representante de pessoa singular perante as Administrações de Pessoa Jurídica e os Certificados de Representante de Pessoa singular perante as Administrações de Entidade sem Personalidade Jurídica são acrescentados com a informação correspondente a cada secção.	DMP	30/01/2017
	1.3.3.1 3.2 3.2.3 3.2.3.2 4.1.1	Acrescenta-se a assunção de pessoas singulares como assinantes do serviço de certificação.	DMP	30/01/2017

	4.7.3.1			
	3.2.5	Autenticação de Autoridades de Registro e seus operadores é adicionada	DMP	30/01/2017
	6.1.1	Esclarecimento foi feito sobre o período de validade dos certificados de usuário final	DMP	01/07/2017
	Em geral	Adaptação de termos, normas e referências de acordo com o Regulamento (UE) 910/2014 eIDAS. Foram eliminados os serviços de emissão de certificados de selos de órgãos eletrônicos para AAPP de médio e alto nível.	DMP	04/06/2017
2,0	Em geral	Adaptação geral das Práticas de Certificação ao Regulamento eIDAS e regulamentos técnicos aplicáveis. As políticas e os perfis de certificado são redefinidos.	MSC	12/05/2017
Errata	1.4.1.19	O número de identificação da política de certificação foi corrigido.	DMP	23/06/2017
2.1	3.2, 5.3.2, 9.4 1.1, 1.2.1, 1.4.1, 3.1.1, 3.1.5, 6.1.2, 6.2.4 5.2.1, 6.1, 4.7.1, 4.1.1, 9.6.1	1.- Adaptação geral ao Regulamento Europeu nº2016/679 Geral de Proteção de Dados. 2.-Inclusão dos novos perfis de certificados no QSCD Centralizado. 3.- Pequenos ajustes operacionais: acrescenta-se a função oficial de confiança, aumento do limite de certificados para 5 anos e ajustes de procedimentos, pequenas correções e de formato.	ABD	05/09/2018
2.2.	Informações gerais +	1.- O documento foi ajustado às políticas e procedimentos de	ABD	02/05/2019

	Formato 1.1, 1.2.1, 1.4.1, 3.1.1, 3.2, 3.3.2, 4.3.2, 4.4.4, 4.9.4 3.3.2, 4.2, 4.4, 4.7	acordo com o SGSI UANATACA. 2.- Inclusão de novos perfis de selos eletrônicos para PSD2. Os procedimentos foram ajustados de acordo com ETSI 119 495. 3.- Otimização dos procedimentos de emissão, renovação e entrega de certificados. Inclusão do sistema de renovação online.		
23	1.3.1.3 e 6.1.1	Ajustes para incluir os perfis de certificado de entidade final UANATACA CA 1, no âmbito da política de certificação UANATACA CA 2.	ABD	12/03/2019
2.4	3.2.7	Implementação de meios alternativos de identificação de acordo com o disposto no Real Decreto-Lei 11/2020, de 31 de março, que adota medidas complementares urgentes no âmbito social e económico para enfrentar a COVID-19.	ABD	01/04/2020
3,0	Completo	Adaptação completa do documento de acordo com a lei 6/2020 e Portaria ETD/465/2021. Incluindo novos métodos de identificação. Ampliação da hierarquia gerando duas novas Autoridades Certificadoras Subordinadas.	AGB	31/05/2021

4,0	Completo	Adequação e correção dos processos de gestão do ciclo de vida dos certificados de acordo com a Lei 6/2020. Modificação da seção relativa às comunicações a terceiros relativas à emissão e revogação. Esclarecimento relativamente aos campos " *Identificador da Organização* " e " *Número de Série* " dos perfis conforme estabelecido na ETSI 319 412-1. Atualização do processo de geração e entrega de certificados. Especificação dos casos de caso fortuito e força maior.	RFC	16/08/2022
Errata	6.1.1.	A seção indicada é corrigida adicionando as entidades certificadoras intermediárias "UANATACA CA1 2021" e "UANATCA CA2 2021".	RFC	03/08/2023
4.1	1.5.1 1.5.2 9.4 3.1.4	Atualização da sede social de Uanataca, SA Inclusão explicativa de atributos de certificados para identificação de interessados perante Administrações Públicas	APV	01/06/2023

4.2	3.1.2.1	Alteração dos aspectos relacionados com a emissão de certificados de ensaio na sequência de solicitação da Entidade Supervisora Nacional	AGB	03/04/2024

Índice

1. Introdução

1.1. Apresentação

Este documento declara as práticas de certificação de assinatura eletrônica da UANATACA.

Os certificados emitidos são os seguintes:

- **De Pessoa Física**
  - Certificado Qualificado de Pessoa Física em software
  - Certificado qualificado de assinatura de Pessoa Singular em QSCD
  - Certificado Qualificado de Pessoa Física em QSCD
  - Certificado Qualificado de Pessoa Física em HSM centralizado
  - Certificado Qualificado de Pessoa Física em QSCD centralizado
  - Certificado qualificado de assinatura de Pessoa Singular em QSCD centralizado

- **Representante da Entidade**
  - Certificado Qualificado de Representante Pessoa Física em software
  - Certificado qualificado de assinatura de Representante Pessoa Física no QSCD
  - Certificado qualificado de assinatura do Representante Pessoa Física em QSCD centralizado

- **Selo de Órgão**
  - Certificado qualificado de selo eletrônico de nível médio APE
  - Certificado qualificado de selo eletrônico de alto nível APE
  - Certificado de selo eletrônico de alto nível APE qualificado em QSCD centralizado

- **Funcionário público**
  - Certificado Qualificado de Funcionário Público de Nível Médio
  - Certificado de autenticação eletrônica para Funcionário Público de Alto Nível

- Certificado qualificado de assinatura de funcionário público de alto nível
- Certificado qualificado de assinatura de Funcionário Público de Alto Nível em QSCD centralizado

- **Representante de Pessoa Jurídica perante Administrações Públicas**
  - Certificado qualificado de pessoa física Representante de Pessoa Jurídica perante as administrações em software
  - Certificado Habilitado de Pessoa Física Representante de Pessoa Jurídica perante as administrações em QSCD
  - Certificado qualificado de Pessoa Física Representante de Pessoa Jurídica perante as administrações em HSM centralizado
  - Certificado qualificado de Pessoa Física Representante de Pessoa Jurídica perante as administrações em QSCD centralizado

- **Representante de Entidade sem Personalidade Jurídica perante Administrações Públicas**
  - Certificado qualificado de pessoa singular Representante de Entidade sem Personalidade Jurídica perante as administrações em software
  - Certificado qualificado de pessoa singular representante de entidade sem personalidade jurídica perante as administrações em QSCD
  - Certificado qualificado de pessoa singular representante de entidade sem personalidade jurídica perante as administrações em HSM centralizado
  - Certificado qualificado de pessoa singular representante de entidade sem personalidade jurídica perante as administrações em QSCD centralizado

- **Selo da empresa**
  - Certificado de Selo Eletrônico Qualificado em software
  - Certificado de Selo Eletrônico Qualificado em QSCD
  - Certificado de Selo Eletrônico Qualificado em HSM centralizado
  - Certificado de Selo Eletrônico Qualificado em QSCD centralizado

- **Selo Eletrônico para PSD2**
  - Certificado de selo eletrônico qualificado para PSD2 em software

- Certificado de Selo Eletrônico Qualificado para PSD2 em HSM centralizado
- Certificado de Selo Eletrônico Qualificado para PSD2 em QSCD centralizado

- **Carimbo de data e hora**
  - Certificado de carimbo de data/hora eletrônico qualificado

1.2. Nome e identificação do documento

Este documento estabelece a Declaração de Práticas de Certificação dedicada à emissão de certificados eletrônicos da Uanataca SA, doravante UANATACA.

1.2.1. Identificadores de certificado

A UANATACA atribuiu a cada política de certificados um identificador de objeto (OID), para identificação pelas aplicações.

Número OID	Tipo de certificados
	Pessoa física
1.3.6.1.4.1.47286.1.1.1	*Certificado Qualificado de Pessoa Física em software*
1.3.6.1.4.1.47286.1.1.2.2	*Certificado qualificado de assinatura de Pessoa Singular em QSCD*
1.3.6.1.4.1.47286.1.1.3	*Certificado Qualificado de Pessoa Física em QSCD*
1.3.6.1.4.1.47286.1.1.5	*Certificado Qualificado de Pessoa Física em HSM centralizado*
1.3.6.1.4.1.47286.1.1.6	Certificado Qualificado de Pessoa Física em QSCD centralizado
1.3.6.1.4.1.47286.1.1.6.2	Certificado qualificado de assinatura de Pessoa Singular em QSCD centralizado
	Representante da Entidade
1.3.6.1.4.1.47286.1.2.1	*Certificado Qualificado de Representante Pessoa Física em software*
1.3.6.1.4.1.47286.1.2.2.2	*Certificado qualificado de assinatura de Representante Pessoa Física no QSCD*

1.3.6.1.4.1.47286.1.2.6.2	*Certificado qualificado de assinatura do Representante Pessoa Física em QSCD centralizado*
	Selo de Órgão
1.3.6.1.4.1.47286.1.3.1	*Certificado qualificado de selo eletrônico de nível médio APE*
1.3.6.1.4.1.47283.1.3.2	*Certificado qualificado de selo eletrônico de alto nível APE*
1.3.6.1.4.1.47286.1.3.6	*Certificado de selo eletrônico de alto nível APE qualificado em QSCD centralizado*
	Empregado público
1.3.6.1.4.1.47286.1.4.1	*Certificado Qualificado de Funcionário Público de Nível Médio*
1.3.6.1.4.1.47286.1.4.2.1	*Certificado de autenticação eletrônica para Funcionário Público de Alto Nível*
1.3.6.1.4.1.47286.1.4.2.2	*Certificado qualificado de assinatura de funcionário público de alto nível*
1.3.6.1.4.1.47286.1.4.6.2	*Certificado qualificado de assinatura de Funcionário Público de Alto Nível em QSCD centralizado*
	Representante Pessoa Jurídica perante a AAPP
1.3.6.1.4.1.47286.1.7.1	*Certificado qualificado de pessoa física Representante de Pessoa Jurídica perante as administrações em software*
1.3.6.1.4.1.47286.1.7.2.2	*Certificado Habilitado de Pessoa Física Representante de Pessoa Jurídica perante as administrações em QSCD*
1.3.6.1.4.1.47286.1.7.5	*Certificado Habilitado de Pessoa Física Representante de Pessoa Jurídica perante as administrações em HSM Centralizado*
1.3.6.1.4.1.47286.1.7.6	*Certificado qualificado de Pessoa Física Representante de Pessoa Jurídica perante as administrações em QSCD centralizado*
	Representante de Entidade sem Personalidade Jurídica perante a AAPP
1.3.6.1.4.1.47286.1.8.1	*Certificado qualificado de pessoa singular Representante de Entidade sem Personalidade Jurídica perante as administrações em software*
1.3.6.1.4.1.47286.1.8.2.2	*Certificado qualificado de pessoa singular representante de entidade sem personalidade jurídica perante as administrações em QSCD*
1.3.6.1.4.1.47286.1.8.5	*Certificado qualificado de pessoa singular representante de entidade sem personalidade jurídica perante as administrações em HSM centralizado*

1.3.6.1.4.1.47286.1.8.6	*Certificado qualificado de pessoa singular representante de entidade sem personalidade jurídica perante as administrações em QSCD centralizado*
	Selo da empresa
1.3.6.1.4.1.47286.1.9.1	*Certificado de Selo Eletrônico Qualificado em software*
1.3.6.1.4.1.47286.1.9.2	*Certificado de Selo Eletrônico Qualificado em QSCD*
1.3.6.1.4.1.47286.1.9.5	*Certificado de Selo Eletrônico Qualificado em HSM centralizado*
1.3.6.1.4.1.47286.1.9.6	*Certificado de Selo Eletrônico Qualificado em QSCD centralizado*
	Selo eletrônico para PSD2
1.3.6.1.4.1.47286.1.11.1	*Certificado de selo eletrônico qualificado para PSD2 em software*
1.3.6.1.4.1.47286.1.11.5	*Certificado de Selo Eletrônico Qualificado para PSD2 em HSM centralizado*
1.3.6.1.4.1.47286.1.11.6	*Certificado de Selo Eletrônico Qualificado para PSD2 em QSCD centralizado*
	Certificado de carimbo de data/hora
1.3.6.1.4.1.47286.1.5	*Certificado de carimbo de data/hora eletrônico qualificado*

No caso de contradição entre esta Declaração de Práticas de Certificação e outros documentos de práticas e procedimentos, as disposições desta Declaração de Práticas prevalecerão.

1.3. Participantes em serviços de certificação

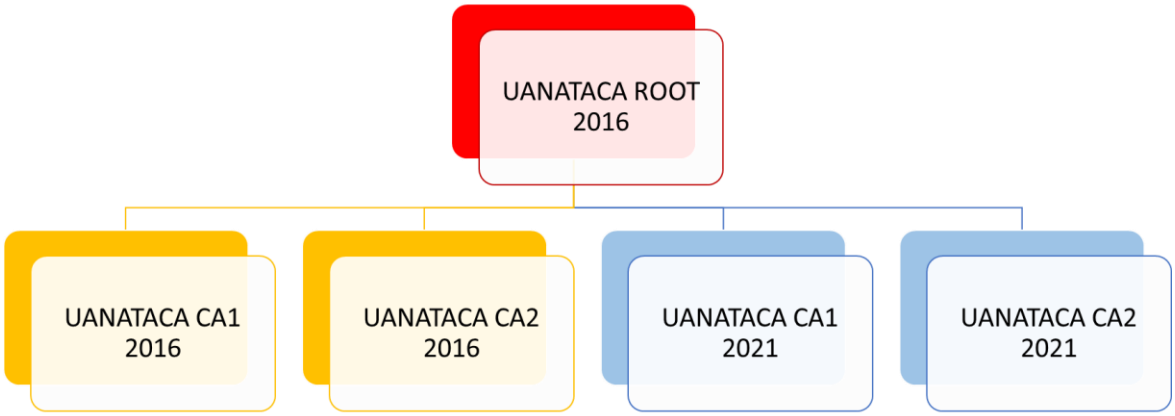
1.3.1. Provedor de serviços de certificação

O prestador de serviços de certificação eletrónica é a pessoa singular ou coletiva que emite e gere certificados para entidades finais, recorrendo a uma Autoridade Certificadora, ou presta outros serviços relacionados com assinaturas eletrónicas.

UANATACA é um prestador de serviços eletrónicos de confiança, que atua de acordo com o disposto no Regulamento (UE) 910/2014 DO PARLAMENTO EUROPEU E DO CONSELHO de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de

confiança para transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE , bem como as normas técnicas do ETSI aplicáveis à emissão e gestão de certificados qualificados, principalmente EN 319 411-1 e EN 319 411-2, a fim de facilitar o cumprimento dos requisitos legais e o reconhecimento internacional dos seus serviços.

Para a prestação de serviços de certificação, a UANATACA estabeleceu uma hierarquia de entidades certificadoras:



1.3.1.1. RAIZ DE UANTACA 2016

Esta é a Autoridade Certificadora raiz da hierarquia que emite certificados para outras entidades certificadoras e cujo certificado de chave pública foi autoassinado.

Dados de identificação:

CN:	RAIZ DE UANTACA 2016
Impressão digital:	6d c0 84 50 a9 5c d3 26 62 c0 91 0f 8c 2d ce 23 0d 74 66 anúncio
Válido de:	Sexta-feira, 11 de março de 2016
Valido ate:	Segunda-feira, 11 de março de 2041
Comprimento da chave RSA:	4.096 bits

1.3.1.2. UANTACA CA1 2016

É a Autoridade Certificadora dentro da hierarquia que emite os certificados às entidades fim, e cujo certificado de chave pública foi assinado digitalmente pela UANATACA ROOT 2016.

Dados de identificação:

CN:	UANTACA CA1 2016
Impressão digital:	7f 2c b4 f7 69 22 4c b0 cf 8b 69 27 51 cb d4 cc 64 a2 c4 50
Válido de:	Sexta-feira, 11 de março de 2016
Valido ate:	Domingo, 11 de março de 2029
Comprimento da chave RSA:	4.096 bits

1.3.1.3. UANTACA CA2 2016

Esta é a Autoridade Certificadora dentro da hierarquia que emite o certificados às entidades finais e os certificados de carimbo eletrônico de data e hora, e cujo certificado de chave pública foi assinado digitalmente pela UANATACA ROOT 2016.

Dados de identificação:

CN:	UANTACA CA2 2016
Impressão digital:	0e ce 52 78 03 c9 db 6e 63 bc ea 55 36 b9 3a e8 28 4e 8d 2d
Válido de:	Sexta-feira, 11 de março de 2016
Valido ate:	Domingo, 11 de março de 2029
Comprimento da chave RSA:	4.096 bits

1.3.1.4. UANTACA CA1 2021

Esta é a Autoridade Certificadora dentro da hierarquia que emite o certificados às entidades finais e os certificados de carimbo eletrônico de data e hora, e cujo certificado de chave pública foi assinado digitalmente pela UANATACA ROOT 2016.

Dados de identificação:

CN:	UANTACA CA1 2021
Impressão digital:	a1 db ea 6c 10 7a a3 e8 1e 16 c9 af 8e 55 7f ed 3d 90 cf 98
Válido de:	Quinta-feira, 3 de junho de 2021
Valido ate:	Sábado, 3 de junho de 2034
Comprimento da chave RSA:	4.096 bits

1.3.1.5. UANTACA CA2 2021

Esta é a Autoridade Certificadora dentro da hierarquia que emite o certificados às entidades finais e os certificados de carimbo eletrônico de data e hora, e cujo certificado de chave pública foi assinado digitalmente pela UANATACA ROOT 2016.

Dados de identificação:

CN:	UANTACA CA2 2021
Impressão digital:	2d 35 17 27 f4 5b 01 2a a4 88 03 4b db 01 1c da 4f 61 a4 2e
Válido de:	Quinta-feira, 3 de junho de 2021
Valido ate:	Sábado, 3 de junho de 2034
Comprimento da chave RSA:	4.096 bits

1.3.2. Autoridade de Registro

A Autoridade de Registro UANATACA é a entidade responsável por:

- Processar solicitações de certificado.
- Identifique o solicitante e verifique se ele atende aos requisitos necessários para solicitar os certificados.
- Valide as circunstâncias pessoais da pessoa que aparecerá como signatária do certificado.
- Gerencie a geração de chaves e a emissão de certificados.
- Entregar o certificado ao assinante ou os meios para a sua geração.
- Custódia da documentação relativa à identificação e registo de signatários e/ou assinantes e gestão do ciclo de vida dos certificados.

Podem atuar como AR da UANATACA:

- Qualquer entidade autorizada pela UANATACA.
- UANATACA diretamente.

A UANATACA formalizará contratualmente as relações entre si e cada uma das entidades que atuam como Autoridade de Registro da UANATACA.

A entidade que atua como Autoridade de Registro da UANATACA pode autorizar uma ou mais pessoas como Operador de RA a operar com o sistema de emissão de certificados da UANATACA em nome da Autoridade de Registro.

A Autoridade de Registo poderá delegar as funções de identificação de assinantes e/ou signatários, mediante acordo de colaboração em que seja aceite a delegação dessas funções. A UANATACA deverá autorizar expressamente o referido acordo de colaboração.

As unidades designadas para esta função pelos assinantes dos certificados, como um departamento de pessoal, também poderão ser Autoridades de Registro sujeitas a esta Declaração de Práticas de Certificação, desde que possuam registros autênticos sobre o vínculo dos signatários com o assinante.

1.3.3. Entidades finais

As entidades finais são as pessoas ou organizações destinatárias dos serviços de emissão, gestão e utilização de certificados digitais, para autenticação e utilização de assinatura eletrónica.

Serão as entidades finalistas dos serviços de certificação UANATACA:

1. Assinantes do Serviço de Certificação
2. Signatários
3. Partes do usuário

1.3.3.1. Assinantes do Serviço de Certificação

Os assinantes do serviço de certificação são:

- As empresas, entidades, corporações ou organizações que os adquirem da UANATACA (diretamente ou através de terceiros) para uso no seu âmbito empresarial, societário ou organizacional, e estão identificadas nos certificados.
- As pessoas singulares que adquirem os certificados para si e são identificadas nos certificados.

O assinante do serviço de certificação adquire uma licença de utilização do certificado, para uso próprio ou para efeitos de facilitar a certificação da identidade de determinada pessoa devidamente autorizada para diversas ações no âmbito organizacional do assinante. Neste último caso, esta pessoa é identificada no certificado.

O assinante do serviço eletrónico de confiança é, portanto, cliente do prestador de serviços de certificação, nos termos do direito privado, e tem os direitos e obrigações que lhe são definidos pelo prestador de serviços de certificação, os quais são adicionais e entendem-se sem prejuízo do os direitos e obrigações dos signatários, conforme autorizado e regulamentado nas normas técnicas europeias aplicáveis à emissão de certificados eletrónicos qualificados.

1.3.3.2. Signatários

São signatários as pessoas singulares que possuam exclusivamente as chaves de assinatura eletrónica para autenticação e/ou assinatura eletrónica avançada ou qualificada; sendo normalmente funcionários, representantes legais ou voluntários, bem como outras pessoas vinculadas aos assinantes; incluindo pessoas ao serviço das Administrações Públicas, nos certificados de funcionários públicos.

Os signatários são devidamente autorizados pelo subscritor e devidamente identificados no certificado através do seu nome e apelido, e número de identificação inequívoco, não sendo geralmente possível a utilização de pseudónimos.

A chave privada de um signatário não pode ser recuperada ou deduzida pelo prestador de serviços eletrónicos de confiança, pelo que as pessoas singulares identificadas nos certificados correspondentes Eles são os únicos responsáveis pela sua proteção e devem considerar as implicações da perda de uma chave privada.

Dada a existência de certificados para outras utilizações que não a assinatura electrónica, como a autenticação, é também utilizado o termo mais genérico “pessoa singular identificada no certificado”, sempre com total respeito pelo cumprimento do regulamento de assinatura electrónica em relação aos direitos e obrigações do signatário.

1.3.3.3. Partes do usuário

Os usuários são as pessoas e organizações que recebem assinaturas eletrônicas e certificados digitais.

Como passo prévio à confiança nos certificados, os utilizadores devem verificá-los, conforme estabelecido nesta declaração de práticas de certificação e nas instruções correspondentes disponíveis no site da Autoridade Certificadora.

1.4. Uso de certificados

Esta seção lista os aplicativos para os quais cada tipo de certificado pode ser usado, define limitações para determinados aplicativos e proíbe determinados aplicativos dos certificados.

1.4.1. Usos permitidos para certificados

as utilizações permitidas indicadas nos diversos campos dos perfis dos certificados, disponíveis no site https://web.uanataca.com/ .

1.4.1.1. Certificado Qualificado de Pessoa Física em software

Este certificado possui o OID 1.3.6.1.4.1.47286.1.1.1. É um certificado qualificado de acordo com o disposto no artigo 28 do Regulamento (UE) 910/2014 eIDAS , que é emitido para assinatura e autenticação eletrónica, de acordo com a política de certificação QCP-n com OID 0.4.0.194112. 1.0.

Os certificados de pessoas singulares emitidos em software não garantem o seu funcionamento com dispositivos qualificados de criação de assinaturas, referidos nos artigos 29.º e 51.º do Regulamento (UE) 910/2014.

Estes certificados garantem a identidade do assinante e da pessoa indicada no certificado, e permitem a geração da "assinatura eletrónica avançada baseada num certificado eletrónico qualificado".

Os certificados podem ser usados em aplicações como as seguintes:

a) Autenticação em sistemas de controle de acesso.
b) Assinatura de e-mail segura.
c) Outras aplicações de assinatura eletrónica, de acordo com o acordado entre as partes ou com as normas legais aplicáveis em cada caso.

As informações de uso no perfil do certificado indicam o seguinte:

O campo “uso de chave” foi ativado e, portanto, nos permite realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Compromisso com o conteúdo (Compromisso de conteúdo , para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.2. Certificado qualificado de assinatura de Pessoa Singular em QSCD

Este certificado possui o OID 1.3.6.1.4.1.47286. 1.1.2.2 . É um certificado qualificado emitido para assinatura eletrônica qualificada , de acordo com a política de certificação QCP-n-qscd com o OID 0.4.0.194112.1.2, que está declarado no certificado. Este certificado emitido no QSCD é um certificado qualificado de acordo com o disposto no artigo 28 do Regulamento (UE) 910/2014 eIDAS.

Funciona com dispositivos qualificados de criação de assinaturas (QSCD), de acordo com os artigos 29 e 51 do Regulamento (UE) 910/2014, e cumpre o disposto nos regulamentos técnicos do Instituto Europeu de Normas de Telecomunicações, identificados com a referência EN 319 411 -2 .

Garante a identidade do signatário e a sua ligação com o assinante do serviço eletrónico de confiança, e permite a geração da “assinatura eletrónica qualificada”, ou seja, a assinatura eletrónica avançada que se baseia num certificado qualificado e que foi gerada utilizando um dispositivo qualificado, razão pela qual equivale a uma assinatura escrita para efeitos legais, sem necessidade de cumprir qualquer outro requisito adicional.

Também pode ser utilizado em aplicações que não necessitam de assinatura eletrônica equivalente a assinatura escrita, como as aplicações listadas abaixo:

a) Assinatura de e-mail segura.
b) Outros aplicativos de assinatura eletrônica.

As informações de uso no perfil do certificado indicam o seguinte:

O campo “uso de chave” está ativado e portanto nos permite realizar a seguinte função:

a. Compromisso com o conteúdo (Compromisso de conteúdo, para desempenhar a função de assinatura eletrônica)

1.4.1.3. Certificado Qualificado de Pessoa Física em QSCD

Este certificado possui o OID 1.3.6.1.4.1.47286. 1.1.3 . É um certificado qualificado emitido para assinatura e autenticação eletrônica qualificada , de acordo com a política de certificação QCP-n-qscd com OID 0.4.0.194112.1.2. Este certificado emitido no QSCD é um certificado qualificado de acordo com o disposto no artigo 28 do Regulamento (UE) 910/2014 eIDAS.

Funciona com dispositivos qualificados de criação de assinaturas, de acordo com os artigos 29.º e 51.º do Regulamento (UE) 910/2014, e cumpre o disposto nos regulamentos técnicos do Instituto Europeu de Normas de Telecomunicações, identificados com a referência EN 319. 411-2 .

Garante a identidade do signatário e a sua ligação ao assinante do serviço eletrónico de confiança, e permite a geração da “assinatura eletrónica qualificada”; Ou seja, a assinatura eletrónica avançada que se baseia num certificado qualificado e que foi gerada através de um dispositivo qualificado, pelo que equivale à assinatura escrita para efeitos legais, sem necessidade de cumprir quaisquer outros requisitos adicionais.

Também pode ser utilizado em aplicações que não necessitam de assinatura eletrônica equivalente a assinatura escrita, como as aplicações listadas abaixo:

a) Assinatura de e-mail segura.
b) Outros aplicativos de assinatura eletrônica.

As informações de uso no perfil do certificado indicam o seguinte:

O campo “uso de chave” foi ativado e, portanto, nos permite realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Compromisso com o conteúdo (Compromisso de conteúdo, para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.4. Certificado Qualificado de Pessoa Física em HSM centralizado

Este certificado possui o OID 1.3.6.1.4.1.47286. 1.1.5 . É um certificado qualificado emitido para assinatura e autenticação eletrônica avançada, de acordo com a política de certificação QCP-n com OID 0.4.0.194112.1.0. Os certificados de pessoas singulares emitidos em HSM Centralizado são certificados qualificados de acordo com o disposto nos artigos 24.º e 28.º do Regulamento (UE) 910/2014 .

Garantem a identidade do assinante e da pessoa indicada no certificado e permitem a geração da "assinatura eletrónica avançada baseada num certificado eletrónico qualificado".

Os certificados podem ser usados em aplicações como as seguintes:

a) Autenticação em sistemas de controle de acesso.
b) Assinatura de e-mail segura.
c) Outras aplicações de assinatura eletrónica, de acordo com o acordado entre as partes ou com as normas legais aplicáveis em cada caso.

As informações de uso no perfil do certificado indicam o seguinte:

O campo "uso de chave" foi ativado e, portanto, nos permite realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Compromisso com o conteúdo (Compromisso de conteúdo , para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.5. Certificado Qualificado de Pessoa Física em QSCD centralizado

Este certificado possui o OID 1.3.6.1.4.1.47286. 1.1.6 . É um certificado qualificado emitido para assinatura e autenticação eletrônica qualificada , de acordo com a política de certificação QCP-n-qscd com OID 0.4.0.194112.1.2. Este certificado emitido num QSCD centralizado é um certificado qualificado de acordo com o disposto no artigo 28 do Regulamento (UE) 910/2014 eIDAS.

Funciona com dispositivos qualificados de criação de assinaturas, de acordo com os artigos 29.º e 51.º do Regulamento (UE) 910/2014, e cumpre o disposto nos regulamentos técnicos do Instituto Europeu de Normas de Telecomunicações, identificados com a referência EN 319. 411-2 .

Garante a identidade do signatário e a sua ligação ao assinante do serviço eletrónico de confiança, e permite a geração da "assinatura eletrónica qualificada"; Ou seja, a assinatura eletrónica avançada que se baseia num certificado qualificado e que foi gerada através de um dispositivo qualificado, pelo que equivale à assinatura escrita para efeitos legais, sem necessidade de cumprir quaisquer outros requisitos adicionais.

Também pode ser utilizado em aplicações que não necessitam de assinatura eletrônica equivalente a assinatura escrita, como as aplicações listadas abaixo:

a) Assinatura de e-mail segura.
b) Outros aplicativos de assinatura eletrônica.

As informações de uso no perfil do certificado indicam o seguinte:

O campo "uso de chave" foi ativado e, portanto, nos permite realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Compromisso com o conteúdo (Compromisso de conteúdo, para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.6. Certificado qualificado de assinatura de Pessoa Singular em QSCD centralizado

Este certificado possui o OID 1.3.6.1.4.1.47286. 1.1.6.2 . É um certificado qualificado emitido para assinatura eletrônica qualificada , de acordo com a política de certificação QCP-n-qscd com o OID 0.4.0.194112.1.2, que está declarado no certificado. Este certificado emitido num QSCD centralizado é um certificado qualificado de acordo com o disposto no artigo 28 do Regulamento (UE) 910/2014 eIDAS.

Funciona com dispositivos qualificados de criação de assinaturas (QSCD), de acordo com os artigos 29 e 51 do Regulamento (UE) 910/2014, e cumpre o disposto nos regulamentos técnicos do Instituto Europeu de Normas de Telecomunicações, identificados com a referência EN 319 411 -2 .

Garante a identidade do signatário e a sua ligação com o assinante do serviço eletrónico de confiança, e permite a geração da "assinatura eletrónica qualificada", ou seja, a assinatura eletrónica avançada que se baseia num certificado qualificado e que foi gerada utilizando um dispositivo qualificado, razão pela qual equivale a uma assinatura escrita para efeitos legais, sem necessidade de cumprir qualquer outro requisito adicional.

Também pode ser utilizado em aplicações que não necessitam de assinatura eletrônica equivalente a assinatura escrita, como as aplicações listadas abaixo:

a) Assinatura de e-mail segura.
b) Outros aplicativos de assinatura eletrônica.

As informações de uso no perfil do certificado indicam o seguinte:

O campo "uso de chave" está ativado e portanto nos permite realizar a seguinte função:

a. Compromisso com o conteúdo (Compromisso de conteúdo, para desempenhar a função de assinatura eletrônica)

1.4.1.7. Certificado Qualificado de Representante Pessoa Física em software

Este certificado possui o OID 1.3.6.1.4.1.47286.1.2.1. É um certificado qualificado emitido para assinatura e autenticação eletrônica avançada, de acordo com a política de certificação QCP-n com OID 0.4.0.194112.1.0. se, como pessoa singular ou representante de uma entidade emitida em software de acordo com o disposto no artigo 28.º do Regulamento (UE) 910/2014 eIDAS, e que cumpra o disposto nos regulamentos técnicos do European Telecommunications Standards Institute, identificado com a referência EN 319 411-2 .

Garantem a identidade do assinante e do signatário, e uma relação de representação legal ou procuração entre o signatário e uma entidade, empresa ou organização descrita no campo "O" (Organização), e permitem a geração do "avançado assinatura eletrônica baseada em certificado eletrônico qualificado" .

Por outro lado, os certificados representativos emitidos em software podem ser utilizados em outras aplicações como as indicadas abaixo:

a) Autenticação em sistemas de controle de acesso.
b) Assinatura de e-mail segura.
c) Outros aplicativos de assinatura eletrônica.

As informações de uso no perfil do certificado indicam o seguinte:

O campo "uso de chave" foi ativado e, portanto, nos permite realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Compromisso com o conteúdo (Compromisso de conteúdo , para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.8. Certificado qualificado de assinatura de Representante Pessoa Física no QSCD

Este certificado possui o OID 1.3.6.1.4.1.47286. 1 .2.2.2 . É um certificado qualificado emitido para assinatura eletrônica qualificada, de acordo com a política de certificação QCP-n-qscd com OID 0.4.0.194112.1.2. Este certificado representativo emitido no QSCD é um certificado qualificado de acordo com o disposto no artigo 28 do Regulamento (UE) 910/2014 eIDAS.

Funciona com dispositivos qualificados de criação de assinaturas, de acordo com os artigos 29.º e 51.º do Regulamento (UE) 910/2014 , e cumpre o disposto nos regulamentos técnicos do Instituto Europeu de Normas de Telecomunicações, identificados com a referência EN 319 411-2 .

Garante a identidade do assinante e do signatário, e relação de representação legal ou procuração entre o signatário e uma entidade, empresa ou organização descrita no campo "O" (Organização), e permite a geração do "qualificado assinatura electrónica". Ou seja, a assinatura electrónica avançada que se baseia num certificado qualificado e que foi gerada através de um dispositivo qualificado, razão pela qual é equiparada à assinatura escrita para efeitos legais, sem necessidade de cumprir qualquer outro adicional. requisitos.

Também pode ser utilizado em aplicações que não necessitam de assinatura eletrônica equivalente a assinatura escrita, como as aplicações listadas abaixo:

a) Assinatura de e-mail segura.
b) Outros aplicativos de assinatura eletrônica.

As informações de uso no perfil do certificado indicam o seguinte:

O campo "uso de chave" foi ativado e, portanto, nos permite realizar as seguintes funções:

a. Compromisso com o conteúdo (Compromisso de conteúdo, para desempenhar a função de assinatura eletrônica)

1.4.1.9. Certificado qualificado de assinatura do Representante Pessoa Física em QSCD centralizado

Este certificado possui o OID 1.3.6.1.4.1.4 7286. 1 . 2.6.2. É um certificado qualificado emitido para assinatura eletrônica qualificada, de acordo com a política de certificação QCP-n-qscd com OID 0.4.0.194112.1.2. Este certificado representativo emitido em QSCD centralizado é um certificado qualificado de acordo com o disposto no artigo 28 do Regulamento (UE) 910/2014 eIDAS.

Funciona com dispositivos qualificados de criação de assinaturas, de acordo com os artigos 29.º e 51.º do Regulamento (UE) 910/2014 , e cumpre o disposto nos regulamentos técnicos do Instituto Europeu de Normas de Telecomunicações, identificados com a referência EN 319 411-2 .

Garante a identidade do assinante e do signatário, e relação de representação legal ou procuração entre o signatário e uma entidade, empresa ou organização descrita no campo "O" (Organização), e permite a geração do "qualificado assinatura electrónica". Ou seja, a assinatura electrónica avançada que se baseia num certificado qualificado e que foi gerada através de um dispositivo qualificado, razão pela qual é equiparada à assinatura escrita para efeitos legais, sem necessidade de cumprir qualquer outro adicional. requisitos.

Também pode ser utilizado em aplicações que não necessitam de assinatura eletrônica equivalente a assinatura escrita, como as aplicações listadas abaixo:

a) Assinatura de e-mail segura.
b) Outros aplicativos de assinatura eletrônica.

As informações de uso no perfil do certificado indicam o seguinte:

O campo "uso de chave" foi ativado e, portanto, nos permite realizar as seguintes funções:

a. Compromisso com o conteúdo (Compromisso de conteúdo, para desempenhar a função de assinatura eletrônica)

1.4.1.10. Certificado qualificado de selo eletrônico de nível médio APE

Este certificado possui o OID 1.3.6.1.4.1.4728 6.1.3 .1. É um certificado emitido de acordo com a política de certificação QCP-l com o OID 0.4.0.194112.1.1. Os certificados de selo eletrónico de nível médio APE são certificados qualificados emitidos de acordo com o disposto nos artigos 38 e seguintes do Regulamento (UE) 910/2014 eIDAS, e são emitidos de acordo com o Esquema de Autenticação e Assinatura Eletrónica das Administrações Públicas na sua atual versão na data deste documento.

Estes certificados de selo eletrónico garantem a identidade do organismo público e, quando aplicável, a do proprietário do organismo e da pessoa que o gere (criador do selo) incluída no certificado.

As informações de uso no perfil do certificado indicam o seguinte:

O campo “utilização da chave” está ativado e, portanto, permite-nos realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Compromisso com o conteúdo (Compromisso de conteúdo , para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.11. Certificado qualificado de selo eletrônico de alto nível APE

Este certificado possui o OID 1.3.6.1.4.1.47286.1.3.2. É um certificado emitido de acordo com a política de certificação QCP-l-qscd com o OID 0.4.0.194112.1.3.

Os certificados de selo eletrónico qualificado de alto nível são certificados qualificados emitidos de acordo com o disposto nos artigos 38 e seguintes do Regulamento (UE) 910/2014 eIDAS, e são emitidos de acordo com o Esquema de Autenticação/Identificação e Assinatura Eletrónica das Administrações Públicas em sua versão em vigor na data deste documento.

Estas certidões são emitidas para identificação e autenticação do exercício de competência em ação administrativa automatizada nos termos do artigo 42.º da Lei 40/2015, de 1 de outubro, do Regime Jurídico do Setor Público.

Estes certificados de selo eletrónico garantem a identidade do organismo público e, quando aplicável, a do proprietário do organismo e da pessoa que o gere (criador do selo) incluída no certificado.

As informações de uso no perfil do certificado indicam o seguinte:

O campo "utilização da chave" está ativado e, portanto, permite-nos realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Compromisso com o conteúdo (Compromisso de conteúdo , para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.12. Certificado de selo eletrônico de alto nível APE qualificado em QSCD centralizado

Este certificado possui o OID 1.3.6.1.4.1.47286.1.3.6. Este certificado emitido em QSCD centralizado é um certificado emitido de acordo com a política de certificação QCP-l-qscd com o OID 0.4.0.194112.1.3.

Os certificados de selo eletrónico qualificado de alto nível são certificados qualificados emitidos de acordo com o disposto nos artigos 38 e seguintes do Regulamento (UE) 910/2014 eIDAS, e são emitidos de acordo com o Esquema de Autenticação/Identificação e Assinatura Eletrónica das Administrações Públicas em sua versão em vigor na data deste documento.

Estas certidões são emitidas para identificação e autenticação do exercício de competência em ação administrativa automatizada nos termos do artigo 42.º da Lei 40/2015, de 1 de outubro, do Regime Jurídico do Setor Público.

Estes certificados de selo eletrónico garantem a identidade do organismo público e, quando aplicável, a do proprietário do organismo e da pessoa que o gere (criador do selo) incluída no certificado.

As informações de uso no perfil do certificado indicam o seguinte:

O campo "utilização da chave" está ativado e, portanto, permite-nos realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Compromisso com o conteúdo (Compromisso de conteúdo , para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.13. Certificado Qualificado de Funcionário Público de Nível Médio

Este certificado possui o OID 1.3.6.1.4.1.4728 6.1 .4.1. É um certificado qualificado emitido para assinatura e autenticação eletrônica avançada, de acordo com a política de certificação QCP-n com OID 0.4.0.194112.1.0. Os certificados de funcionários públicos de nível médio são certificados qualificados de acordo com o disposto no artigo 28 do Regulamento (UE) 910/2014 eIDAS.

São emitidos aos funcionários públicos para os identificar como pessoas ao serviço da Administração Pública, vinculando-os a esta, cumprindo os requisitos estabelecidos no artigo 43.º da Lei 40/2015, de 1 de outubro, sobre o Regime Jurídico do Setor Público. É emitido de acordo com o Esquema de Identificação e Assinatura Eletrónica das Administrações Públicas na sua versão em vigor à data deste documento.

Garante a identidade do assinante e da pessoa indicada no certificado e permite a geração da "assinatura eletrónica avançada baseada num certificado eletrónico qualificado".

Também podem ser utilizados em aplicações que não necessitam de assinatura eletrônica equivalente a uma assinatura escrita, como as aplicações listadas abaixo:

a) Assinatura de e-mail segura.
b) Outros aplicativos de assinatura eletrônica.

As informações de uso no perfil do certificado indicam o seguinte:

O campo "utilização da chave" está ativado e, portanto, permite-nos realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Compromisso com o conteúdo (Compromisso de conteúdo , para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.14. Certificado de autenticação eletrônica para Funcionário Público de Alto Nível

Este certificado possui o OID 1.3.6.1.4.1.47286. 1.4.2.1 . É um certificado emitido para autenticação, de acordo com a política de certificação NCP+. Este certificado é emitido aos funcionários públicos para os identificar como pessoas ao serviço da Administração Pública, vinculando-os a esta.

Este certificado de autenticação funciona com dispositivos qualificados de criação de assinatura, de acordo com os artigos 29 e 51 do Regulamento (UE) 910/2014 eIDAS , e é emitido de acordo com o Sistema de Identificação e Assinatura Electrónica das Administrações Públicas na sua versão actual à data deste documento.

As informações de uso no perfil do certificado indicam o seguinte:

O campo "uso de chave" foi ativado e, portanto, permite que as seguintes funções sejam executadas:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Criptografia de chave

1.4.1.15. Certificado qualificado de assinatura de funcionário público de alto nível

Este certificado possui o OID 1.3.6.1.4.1.47286 .1.4. 2.2. É um certificado qualificado emitido para assinatura eletrônica qualificada, de acordo com a política de certificação

QCP-n-qscd com OID 0.4.0.194112.1.2. Este certificado está qualificado de acordo com o disposto no artigo 28 do Regulamento (UE) 910/2014 eIDAS.

Este certificado qualificado é emitido aos funcionários públicos para os identificar como pessoas ao serviço da Administração Pública, vinculando-os a esta, cumprindo os requisitos estabelecidos no artigo 43.º da Lei 40/2015, de 1 de outubro, sobre o Regime Jurídico do Trabalho Público. Sector, para a assinatura electrónica do pessoal ao serviço das Administrações Públicas.

Funciona com dispositivos qualificados de criação de assinaturas, de acordo com os artigos 29.º e 51.º do Regulamento (UE) 910/2014, e cumpre o disposto nos regulamentos técnicos do Instituto Europeu de Normas de Telecomunicações, identificados com a referência EN 319. 411-2 . É emitido de acordo com o Esquema de Identificação e Assinatura Eletrónica das Administrações Públicas na sua versão em vigor à data deste documento.

Garante a identidade do assinante e do signatário, e permite a geração da "assinatura eletrónica qualificada"; ou seja, a assinatura eletrónica avançada que se baseia num certificado qualificado e que foi gerada através de um dispositivo qualificado, portanto, de acordo com o disposto no artigo 25.2 do Regulamento (UE) 910/2014, é equiparada à assinatura escrita para efeitos legais, sem a necessidade de atender a qualquer outro requisito adicional.

Eles também podem ser usados em outras aplicações, como as indicadas abaixo:

a) Assinatura de e-mail segura.
b) Outros aplicativos de assinatura eletrônica.

As informações de uso no perfil do certificado indicam o seguinte:

O campo "uso de chave" foi ativado e, portanto, permite que as seguintes funções sejam executadas:

a. Compromisso com o conteúdo (Compromisso de conteúdo, para desempenhar a função de assinatura eletrônica)

1.4.1.16. Certificado qualificado de assinatura de Funcionário Público de Alto Nível em QSCD centralizado

Este certificado possui o OID 1.3.6.1.4.1.47286 .1.4. 6.2. É um certificado qualificado emitido para assinatura eletrônica qualificada, de acordo com a política de certificação QCP-n-qscd com OID 0.4.0.194112.1.2. Este certificado está qualificado de acordo com o disposto no artigo 28 do Regulamento (UE) 910/2014 eIDAS.

Este certificado qualificado é emitido aos funcionários públicos para os identificar como pessoas ao serviço da Administração Pública, vinculando-os a esta, cumprindo os requisitos estabelecidos no artigo 43.º da Lei 40/2015, de 1 de outubro, sobre o Regime Jurídico do Trabalho Público. Sector, para a assinatura electrónica do pessoal ao serviço das Administrações Públicas.

o disposto nos regulamentos técnicos do Instituto Europeu de Normas de Telecomunicações. com a referência EN 319 411-2 . É emitido de acordo com o Esquema de Identificação e Assinatura Eletrónica das Administrações Públicas na sua versão em vigor à data deste documento.

Garante a identidade do assinante e do signatário, e permite a geração da "assinatura eletrónica qualificada"; ou seja, a assinatura eletrónica avançada que se baseia num certificado qualificado e que foi gerada através de um dispositivo qualificado, portanto, de acordo com o disposto no artigo 25.2 do Regulamento (UE) 910/2014, é equiparada à assinatura escrita para efeitos legais, sem a necessidade de atender a qualquer outro requisito adicional.

Eles também podem ser usados em outras aplicações, como as indicadas abaixo:

a) Assinatura de e-mail segura.
b) Outros aplicativos de assinatura eletrônica.

As informações de uso no perfil do certificado indicam o seguinte:

O campo “uso de chave” foi ativado e, portanto, permite que as seguintes funções sejam executadas:

a. Compromisso com o conteúdo (Compromisso de conteúdo, para desempenhar a função de assinatura eletrônica)

1.4.1.17. Certificado qualificado de pessoa física Representante de Pessoa Jurídica perante as administrações em software

Este certificado possui o OID 1.3.6.1.4.1.47286. 1.7.1 . É um certificado qualificado emitido para assinatura e autenticação eletrônica avançada, de acordo com a política de certificação QCP-n com OID 0.4.0.194112.1.0.

Este certificado emitido em software é um certificado qualificado de acordo com o disposto no artigo 28 do Regulamento (UE) 910/2014 eIDAS, e cumpre o disposto nos regulamentos técnicos do European Telecommunications Standards Institute, identificado com a referência EN 319 411 -2.

Garante a identidade do assinante e do signatário, e relação de representação legal ou procuração entre o signatário e uma entidade, empresa ou organização descrita no campo “O” (Organização), e permite a geração do “avançado assinatura eletrônica baseada em certificado eletrônico qualificado” .

Por outro lado, os certificados representativos emitidos em software podem ser utilizados em outras aplicações como as indicadas abaixo:

a) Autenticação em sistemas de controle de acesso.
b) Assinatura de e-mail segura.
c) Outros aplicativos de assinatura eletrônica.

As informações de uso no perfil do certificado indicam o seguinte:

O campo “uso de chave” foi ativado e, portanto, nos permite realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)

b. Compromisso com o conteúdo (Compromisso de conteúdo , para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.18. Certificado Habilitado de Pessoa Física Representante de Pessoa Jurídica perante as administrações em QSCD

Este certificado possui o OID 1.3.6.1.4.1.47286 . 1.7 . 2.2. É um certificado qualificado emitido para assinatura e autenticação eletrónica qualificada, de acordo com a política de certificação QCP-n-qscd com o OID 0.4.0.194112.1.2, que está declarado no certificado.

Este certificado emitido em QSCD, é um certificado qualificado de acordo com o disposto no artigo 28 do Regulamento (UE) 910/2014 eIDAS , e funciona com dispositivos de criação de assinatura qualificada, de acordo com os artigos 29 e 51 do Regulamento (UE) 910 /2014 , e cumpre o disposto nos regulamentos técnicos do European Telecommunications Standards Institute, identificado com a referência EN 319 411-2 .

Garante a identidade do assinante e do signatário, e relação de representação legal ou procuração entre o signatário e uma entidade, empresa ou organização descrita no campo “O” (Organização), e permite a geração do “qualificado assinatura electrónica”. Ou seja, a assinatura electrónica avançada que se baseia num certificado qualificado e que foi gerada através de um dispositivo qualificado, razão pela qual é equiparada à assinatura escrita para efeitos legais, sem necessidade de cumprir qualquer outro adicional. requisitos.

Também podem ser utilizados em aplicações que não necessitam de assinatura eletrônica equivalente a uma assinatura escrita, como as aplicações listadas abaixo:

a) Assinatura de e-mail segura.
b) Outros aplicativos de assinatura eletrônica.

As informações de uso no perfil do certificado indicam o seguinte:

O campo “uso de chave” foi ativado e, portanto, nos permite realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Compromisso com o conteúdo (Compromisso de conteúdo, para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.19. Certificado Habilitado de Pessoa Física Representante de Pessoa Jurídica perante as administrações em HSM Centralizado

Este certificado possui o OID 1.3.6.1.4.1.4728 6.1 .7.5. É um certificado qualificado emitido para assinatura e autenticação eletrônica avançada, de acordo com a política de certificação QCP-n com o OID 0.4.0.194112.1.0, que está declarado no certificado.

É um certificado qualificado de acordo com o disposto no artigo 28.º do Regulamento (UE) 910/2014 eIDAS, e cumpre o disposto nos regulamentos técnicos do Instituto Europeu de Normas de Telecomunicações, identificado com a referência EN 319 411-2.

Garante a identidade do assinante e do signatário, e relação de representação legal ou procuração entre o signatário e uma entidade, empresa ou organização descrita no campo "O" (Organização), e permite a geração do "avançado assinatura eletrônica baseada em certificado eletrônico qualificado" .

Por outro lado, os certificados podem ser utilizados em outras aplicações como as indicadas a seguir:

a) Autenticação em sistemas de controle de acesso.
b) Assinatura de e-mail segura.
c) Outros aplicativos de assinatura eletrônica.

As informações de uso no perfil do certificado indicam o seguinte:

O campo "uso de chave" foi ativado e, portanto, nos permite realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Compromisso com o conteúdo (Compromisso de conteúdo , para desempenhar a função de assinatura eletrônica)

c. Criptografia de chave

1.4.1.20. Certificado qualificado de Pessoa Física Representante de Pessoa Jurídica perante as administrações em QSCD centralizado

Este certificado possui o OID 1.3.6.1.4.1.47286. 1.7.6 . É um certificado qualificado emitido para assinatura e autenticação eletrónica qualificada, de acordo com a política de certificação QCP-n-qscd com o OID 0.4.0.194112.1.2, que está declarado no certificado.

Este certificado emitido num QSCD centralizado é um certificado qualificado de acordo com o disposto no artigo 28.º do Regulamento (UE) 910/2014 eIDAS , e funciona com dispositivos de criação de assinatura qualificada, de acordo com os artigos 29.º e 51.º do Regulamento (UE) 910/2014 , e cumpre o disposto nos regulamentos técnicos do Instituto Europeu de Normas de Telecomunicações, identificado com a referência EN 319 411-2 .

Garante a identidade do assinante e do signatário, e relação de representação legal ou procuração entre o signatário e uma entidade, empresa ou organização descrita no campo “O” (Organização), e permite a geração do “qualificado assinatura electrónica”. Ou seja, a assinatura electrónica avançada que se baseia num certificado qualificado e que foi gerada através de um dispositivo qualificado, razão pela qual é equiparada à assinatura escrita para efeitos jurídicos, sem necessidade de cumprir quaisquer outros requisitos adicionais. requisitos.

Também podem ser utilizados em aplicações que não necessitam de assinatura eletrônica equivalente a uma assinatura escrita, como as aplicações listadas abaixo:

a) Assinatura de e-mail segura.
b) Outros aplicativos de assinatura eletrônica.

As informações de uso no perfil do certificado indicam o seguinte:

O campo “uso de chave” foi ativado e, portanto, nos permite realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)

b. Compromisso com o conteúdo (Compromisso de conteúdo, para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.21. Certificado qualificado de pessoa singular Representante de Entidade sem Personalidade Jurídica perante as administrações em software

Este certificado possui o OID 1.3.6.1.4.1.47286.1.8.1. É um certificado qualificado emitido para assinatura e autenticação eletrônica avançada, conforme política de certificação QCP-n com o OID 0.4.0.194112.1.0, que está declarado no certificado.

É um certificado qualificado de acordo com o disposto no artigo 28.º do Regulamento (UE) 910/2014, e cumpre o disposto nos regulamentos técnicos do Instituto Europeu de Normas de Telecomunicações, identificado com a referência EN 319 411-2.

Garante a identidade do assinante e do signatário, e relação de representação legal ou procuração entre o signatário e uma entidade descrita no campo "O" (Organização), e permite a geração da "assinatura eletrônica avançada baseada em um certificado eletrônico qualificado." .

Por outro lado, este certificado pode ser utilizado em outras aplicações como as indicadas a seguir:

a) Autenticação em sistemas de controle de acesso.
b) Assinatura de e-mail segura.
c) Outros aplicativos de assinatura eletrônica.

As informações de uso no perfil do certificado indicam o seguinte:

O campo "uso de chave" foi ativado e, portanto, nos permite realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Compromisso com o conteúdo (Compromisso de conteúdo , para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.22. Certificado qualificado de pessoa singular representante de entidade sem personalidade jurídica perante as administrações em QSCD

Este certificado possui o OID 1.3.6.1.4.1.4728 6.1 . 8.2.2. É um certificado qualificado emitido para assinatura e autenticação eletrónica qualificada, de acordo com a política de certificação QCP-n-qscd com o OID 0.4.0.194112.1.2, que está declarado no certificado. Este certificado emitido no QSCD é um certificado qualificado de acordo com o disposto nos artigos 28 do Regulamento (UE) 910/2014 eIDAS.

O certificado emitido em QSCD funciona com dispositivos qualificados de criação de assinaturas, de acordo com os artigos 29 e 51 do Regulamento (UE) 910/2014, e cumpre o disposto nos regulamentos técnicos do European Telecommunications Standards Institute, identificados com a referência EN 319 411-2 .

Garante a identidade do assinante e do signatário, e relação de representação legal ou procuração entre o signatário e uma entidade descrita no campo "O" (Organização), e permite a geração da "assinatura eletrônica qualificada" que ou seja, a assinatura electrónica avançada que se baseia num certificado qualificado e que foi gerada através de um dispositivo qualificado, pelo que equivale a uma assinatura escrita para efeitos legais, sem necessidade de cumprir quaisquer outros requisitos adicionais.

Também pode ser utilizado em aplicações que não necessitam de assinatura eletrônica equivalente a assinatura escrita, como as aplicações listadas abaixo:

a) Assinatura de e-mail segura.
b) Outros aplicativos de assinatura eletrônica.

As informações de uso no perfil do certificado indicam o seguinte:

O campo "uso de chave" foi ativado e, portanto, nos permite realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Compromisso com o conteúdo (Compromisso de conteúdo, para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.23. Certificado qualificado de pessoa singular representante de entidade sem personalidade jurídica perante as administrações em HSM centralizado

Este certificado possui o OID 1.3.6.1.4.1.472 86.1.8 .5. É um certificado qualificado emitido para assinatura e autenticação eletrônica avançada, de acordo com a política de certificação QCP-n com OID 0.4.0.194112.1.0.

É um certificado qualificado, de acordo com o disposto no artigo 28.º do Regulamento (UE) 910/2014 eIDAS, e cumpre o disposto nos regulamentos técnicos do European Telecommunications Standards Institute, identificado com a referência EN 319 411-2.

Garante a identidade do assinante e do signatário, e relação de representação legal ou procuração entre o signatário e uma entidade descrita no campo "O" (Organização), e permite a geração da "assinatura eletrônica avançada baseada em um certificado eletrônico qualificado." .

Por outro lado, o certificado pode ser utilizado em outras aplicações como as indicadas a seguir:

a) Autenticação em sistemas de controle de acesso.
b) Assinatura de e-mail segura.
c) Outros aplicativos de assinatura eletrônica.

As informações de uso no perfil do certificado indicam o seguinte:

O campo "uso de chave" foi ativado e, portanto, nos permite realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Compromisso com o conteúdo (Compromisso de conteúdo , para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.24. Certificado qualificado de pessoa singular representante de entidade sem personalidade jurídica perante as administrações em QSCD centralizado

Este certificado possui o OID 1.3.6.1.4.1.47286 . 1.8.6 . É um certificado qualificado emitido para assinatura e autenticação eletrónica qualificada, de acordo com a política de certificação QCP-n-qscd com o OID 0.4.0.194112.1.2, que está declarado no certificado. Este certificado emitido no QSCD é um certificado qualificado de acordo com o disposto nos artigos 28 do Regulamento (UE) 910/2014 eIDAS.

O certificado emitido num QSCD centralizado funciona com dispositivos qualificados de criação de assinaturas, de acordo com os artigos 29.º e 51.º do Regulamento (UE) 910/2014, e cumpre o disposto nos regulamentos técnicos do Instituto Europeu de Normas de Telecomunicações. referência EN 319 411-2 .

Garante a identidade do assinante e do signatário, e relação de representação legal ou procuração entre o signatário e uma entidade descrita no campo "O" (Organização), e permite a geração da "assinatura eletrônica qualificada" que ou seja, a assinatura electrónica avançada que se baseia num certificado qualificado e que foi gerada através de um dispositivo qualificado, pelo que equivale a uma assinatura escrita para efeitos legais, sem necessidade de cumprir quaisquer outros requisitos adicionais.

Também pode ser utilizado em aplicações que não necessitam de assinatura eletrônica equivalente a assinatura escrita, como as aplicações listadas abaixo:

a) Assinatura de e-mail segura.
b) Outros aplicativos de assinatura eletrônica.

As informações de uso no perfil do certificado indicam o seguinte:

O campo "uso de chave" foi ativado e, portanto, nos permite realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Compromisso com o conteúdo (Compromisso de conteúdo, para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.25. Certificado de Selo Eletrônico Qualificado em software

Este certificado possui o OID 1.3.6.1.4.1.472 86.1. 9.1. É um certificado qualificado emitido de acordo com a política de certificação QCP-l com o OID 0.4.0.194112.1.1. Os certificados de selo eletrónico são certificados qualificados emitidos de acordo com o disposto nos artigos 38 do Regulamento (UE) 910/2014 eIDAS.

Estes certificados garantem a identidade da entidade subscritora vinculada e, se for o caso, do responsável pela gestão do selo neles identificado. As informações de uso no perfil do certificado indicam o seguinte:

O campo "utilização da chave" está ativado e, portanto, permite-nos realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Compromisso com o conteúdo (Compromisso de conteúdo , para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.26. Certificado de Selo Eletrônico Qualificado em QSCD

Este certificado possui o OID 1.3.6.1.4.1.47286.1.9.2. É um certificado qualificado emitido de acordo com a política de certificação QCP-l-qscd com o OID 0.4.0.194112.1.3. Os certificados de selo eletrónico são qualificados e emitidos de acordo com o disposto nos artigos 38 do Regulamento (UE) 910/2014 eIDAS.

Os certificados de selo eletrônico no QSCD garantem a identidade do responsável pelo selo e da entidade vinculada, incluída no certificado.

Estes certificados garantem a identidade da entidade subscritora vinculada e, se for o caso, do responsável pela gestão do selo neles identificado. As informações de uso no perfil do certificado indicam o seguinte:

O campo "utilização da chave" está ativado e, portanto, permite-nos realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)

b. Compromisso com o conteúdo (Compromisso de conteúdo , para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.27. Certificado Qualificado de Selo Eletrônico em HSM Centralizado

Este certificado possui o OID 1.3.6.1.4.1.4728 6.1.9 .5, e é um certificado emitido de acordo com a política de certificação QCP-l com o OID 0.4.0.194112.1.1. Os certificados de selo eletrónico são certificados qualificados emitidos de acordo com o disposto no artigo 38.º do Regulamento (UE) 910/2014 eIDAS.

Estes certificados garantem a identidade da entidade subscritora vinculada e, se for o caso, do responsável pela gestão do selo neles identificado. As informações de uso no perfil do certificado indicam o seguinte:

O campo “utilização da chave” está ativado e, portanto, permite-nos realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Compromisso com o conteúdo (Compromisso de conteúdo , para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.28. Certificado de Selo Eletrônico Qualificado em QSCD centralizado

Este certificado possui o OID 1.3.6.1.4.1.47286.1.9.6. É um certificado qualificado emitido de acordo com a política de certificação QCP-l-qscd com o OID 0.4.0.194112.1.3. Os certificados de selo eletrónico são qualificados e emitidos de acordo com o disposto nos artigos 38 do Regulamento (UE) 910/2014 eIDAS.

Os certificados de selo eletrônico em QSCD centralizado garantem a identidade do responsável pelo selo e da entidade vinculada, incluída no certificado.

Estes certificados garantem a identidade da entidade subscritora vinculada e, se for o caso, do responsável pela gestão do selo neles identificado. As informações de uso no perfil do certificado indicam o seguinte:

O campo “utilização da chave” está ativado e, portanto, permite-nos realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Compromisso com o conteúdo (Compromisso de conteúdo , para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.29. Certificado de selo eletrônico qualificado para PSD2 em software

Este certificado possui o OID 1.3.6.1.4.1.47286. 1.11.1 . É um certificado qualificado emitido de acordo com a política de certificação QCP-l com o OID 0.4.0.194112.1.1. Os certificados de selo eletrónico são certificados qualificados emitidos de acordo com o disposto nos artigos 38 do Regulamento (UE) 910/2014 eIDAS.

Este certificado qualificado é emitido a Prestadores de Serviços de Pagamento devidamente credenciados junto da Autoridade Nacional Competente, cumprindo os requisitos estabelecidos no Regulamento Delegado (UE) 2018/389 da Comissão, de 27 de novembro de 2017, que complementa a Diretiva (UE) 2015/2366 do Parlamento Europeu. e do Conselho relativamente às normas técnicas regulamentares para uma autenticação forte do cliente e normas de comunicação abertas comuns e seguras.

Estes certificados garantem a identidade da entidade subscritora vinculada e, se for o caso, do responsável pela gestão do selo neles identificado. As informações de uso no perfil do certificado indicam o seguinte:

O campo “utilização da chave” está ativado e, portanto, permite-nos realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Compromisso com o conteúdo (Compromisso de conteúdo , para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.30. Certificado de Selo Eletrônico Qualificado para PSD2 em HSM Centralizado

Este certificado possui o OID 1.3.6.1.4.1.4728 6.1 .11.5, e é um certificado emitido de acordo com a política de certificação QCP-l com o OID 0.4.0.194112.1.1. Os certificados de selo eletrónico são certificados qualificados emitidos de acordo com o disposto no artigo 38.º do Regulamento (UE) 910/2014 eIDAS.

Este certificado qualificado é emitido para prestadores de serviços de pagamento, cumprindo os requisitos estabelecidos no Regulamento Delegado (UE) 2018/389 da Comissão, de 27 de novembro de 2017, que complementa a Diretiva do Parlamento (UE) 2015/2366. Regulamentos europeus e do Conselho relativos a normas técnicas regulamentares para autenticação forte de clientes e padrões de comunicação abertos comuns e seguros.

Estes certificados garantem a identidade da entidade subscritora vinculada e, se for o caso, do responsável pela gestão do selo neles identificado. As informações de uso no perfil do certificado indicam o seguinte:

O campo “utilização da chave” está ativado e, portanto, permite-nos realizar as seguintes funções:

a. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
b. Compromisso com o conteúdo (Compromisso de conteúdo , para desempenhar a função de assinatura eletrônica)
c. Criptografia de chave

1.4.1.31. Certificado de Selo Eletrônico Qualificado em QSCD para PSD2 centralizado

Este certificado possui o OID 1.3.6.1.4.1.47286.1.11.6. É um certificado qualificado emitido de acordo com a política de certificação QCP-l-qscd com o OID 0.4.0.194112.1.3. Os certificados de selo eletrónico são qualificados e emitidos de acordo com o disposto nos artigos 38 do Regulamento (UE) 910/2014 eIDAS.

Este certificado qualificado é emitido para prestadores de serviços de pagamento, cumprindo os requisitos estabelecidos no Regulamento Delegado (UE) 2018/389 da Comissão, de 27 de novembro de 2017, que complementa a Diretiva do Parlamento (UE)

2015/2366. Regulamentos europeus e do Conselho relativos a normas técnicas regulamentares para autenticação forte de clientes e padrões de comunicação abertos comuns e seguros.

Estes certificados garantem a identidade da entidade subscritora vinculada e, se for o caso, do responsável pela gestão do selo neles identificado. As informações de uso no perfil do certificado indicam o seguinte:

O campo “utilização da chave” está ativado e, portanto, permite-nos realizar as seguintes funções:

d. Assinatura Digital (Assinatura Digital, para realizar a função de autenticação)
e. Compromisso com o conteúdo (Compromisso de conteúdo , para desempenhar a função de assinatura eletrônica)
f. Criptografia de chave

1.4.1.32. Certificado de carimbo de data/hora eletrônico qualificado

Este certificado possui o OID 1.3.6.1.4.1.47286.1.5, e é emitido de acordo com a política de certificação QCP-l-qscd com o OID 0.4.0.194112.1.3.

Os certificados de carimbo temporal eletrónico qualificados são certificados emitidos para o funcionamento das autoridades de carimbo temporal e temporal, para a assinatura dos carimbos temporais que produzem.

Estes certificados permitem a assinatura dos carimbos temporais emitidos, a partir do momento em que tenham obtido um certificado eletrónico de carimbo temporal válido e enquanto este for válido.

A sincronização dos horários no UANATACA é realizada através de um serviço de servidor de horário NTP Stratum 3.

Este servidor, um Meinberg Lantime M300/GPS, com oscilador TCXO de alta estabilidade, receptor GPS, composto por uma placa GPS interna para sincronizar simultaneamente com os satélites com os quais tem visibilidade em todos os momentos (entre 3 e 8), e proteção contra -Deus do céu.

1.4.2. Limites e proibições ao uso de certificados

Os certificados são utilizados para função própria e finalidade estabelecida, não podendo ser utilizados em outras funções ou para outros fins.

Da mesma forma, os certificados devem ser utilizados apenas de acordo com a regulamentação aplicável, especialmente tendo em conta as restrições de importação e exportação existentes em cada momento.

Os certificados não podem ser usados para assinar certificados de chave pública de qualquer tipo, nem podem assinar listas de certificados revogados (CRLs).

Os certificados não foram concebidos, não podem ser utilizados e não estão autorizados para utilização ou revenda como equipamento para controlar situações perigosas ou para utilizações que exijam ações de segurança, como a operação de instalações nucleares, sistemas de navegação ou comunicações aéreas., ou sistemas de controle de armas, onde uma falha pode levar diretamente à morte, ferimentos pessoais ou danos ambientais graves.

Devem ser levados em consideração os limites indicados nos diversos campos dos perfis de certificados, disponíveis no site da UANATACA .

A utilização de certificados digitais em operações que contrariem esta Declaração de Práticas de Certificação, os documentos legais vinculativos de cada certificado, ou contratos com entidades registadoras ou com os seus signatários/assinantes, é considerada utilização indevida para efeitos legais. legislação vigente, de qualquer responsabilidade por esse uso indevido dos certificados efetuado pelo signatário ou por terceiros.

A UANATACA não tem acesso aos dados sobre os quais pode ser aplicada a utilização de um certificado. Assim, e como consequência desta impossibilidade técnica de acesso ao conteúdo da mensagem, não é possível à UANATACA emitir qualquer avaliação sobre o referido conteúdo, assumindo assim o assinante, o signatário ou o responsável pela

custódia, qualquer responsabilidade decorrente. do conteúdo anexado ao uso de um certificado.

Da mesma forma, será imputável ao assinante, ao signatário ou ao responsável pela guarda, qualquer responsabilidade que possa advir da sua utilização fora dos limites e condições de utilização constantes desta Declaração de Práticas de Certificação, dos documentos legais vinculativos a cada certificado, ou dos contratos ou acordos com as entidades registadoras ou com os seus assinantes, bem como quaisquer outras uso indevido derivado desta seção ou que possa ser interpretado como tal com base na legislação vigente.

1.5. Administração de políticas

1.5.1. Organização que gerencia o documento

Uanataca, SA
Avenida Meridiana, 350, 3º andar,
08027 Barcelona

1.5.2. Detalhes de contato da organização

Uanataca, SA
Avenida Meridiana, 350, 3º andar,
08027 Barcelona

+34 935 27 22 90
info@uanataca.com

1.5.3. Procedimentos de gerenciamento de documentos

O sistema documental e organizacional da UANATACA garante, através da existência e aplicação dos procedimentos correspondentes, a correta manutenção deste documento e das especificações de serviço a ele relacionadas.

2. Publicação de informações e depósito de certificados

2.1. Repositórios de certificados

A UANATACA possui um Repositório de Certificados, no qual são publicadas informações relacionadas aos serviços de certificação.

O referido serviço está disponível 24 horas por dia, 7 dias por semana e, em caso de falha do sistema fora do controle da UANATACA, envidará todos os esforços para voltar a disponibilizar o serviço no prazo estabelecido na seção 5.7.4deste Declaração de práticas de certificação

2.2. Publicação de informações do provedor de serviços de certificação

A UANATACA publica em seu Depósito as seguintes informações:

- Listas de certificados revogados e outras informações de status de revogação de certificados.
- As políticas de certificado aplicáveis.
- A Declaração de Práticas de Certificação.
- Textos de divulgação (Policy Disclosure Statements - PDS), pelo menos em espanhol e inglês.

2.3. Frequência de postagem

As informações do provedor de serviços de certificação, incluindo políticas e a Declaração de Práticas de Certificação, são publicadas à medida que ficam disponíveis.

As alterações na Declaração de Práticas de Certificação são regidas pelas disposições da seção 1.5deste documento.

As informações sobre o status de revogação do certificado são publicadas de acordo com esta Declaração de Práticas de Certificação.

2.4. Controle de acesso

A UANATACA não limita o acesso de leitura às informações estabelecidas na seção 2.2, mas estabelece controles para evitar que pessoas não autorizadas adicionem, modifiquem ou excluam registros do Depositário, para proteger a integridade e autenticidade das informações, especialmente informações de status de revogação.

A UANATACA utiliza sistemas confiáveis para o Armazém, para que:

- Somente pessoas autorizadas podem fazer anotações e modificações.
- A autenticidade das informações pode ser verificada.
- Qualquer alteração técnica que afete os requisitos de segurança pode ser detectada.

3. Identificação e autenticação

3.1. Registro inicial

3.1.1. Tipos de nomes

Todos os certificados contêm um nome distinto (DN ou *nome distinto*) de acordo com o padrão X.509 no campo *Assunto* , incluindo um componente *Nome Comum* (CN=), relativo à identidade do assinante e da pessoa física identificada no certificado , bem como diversas informações de identidade adicionais no campo *SubjectAlternativeName* .

Os nomes contidos nos certificados são os seguintes.

3.1.1.1. Certificado Qualificado de Pessoa Física em software

País	Estado[1]
Organização (O)	Organização à qual o signatário está vinculado
Unidade Organizacional (OU)	Unidade da Organização à qual o signatário está vinculado
Identificador da Organização	Identificador único da Organização à qual o signatário está vinculado de acordo com o indicado na ETSI EN 319 412-1
Título	Título ou especialidade do signatário
Sobrenome	Sobrenome do signatário
Nome dado	Nome do signatário
Número de série	Identificador único do signatário de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Nome e sobrenome do signatário

[1]O campo "Estado" corresponderá ao estado onde ocorre a relação contratual entre o signatário e a entidade a que está vinculado (por ser empregado, associado, sócio ou outro vínculo), independentemente da nacionalidade do trabalhador.

3.1.1.2. Certificado qualificado de assinatura de Pessoa Singular em QSCD

País	Estado[2]
Organização (O)	Organização à qual o signatário está vinculado
Unidade Organizacional (OU)	Unidade da Organização à qual o signatário está vinculado
Identificador da Organização	Identificador único da Organização à qual o signatário está vinculado de acordo com o indicado na ETSI EN 319 412-1
Título	Título ou especialidade do signatário
Sobrenome	Sobrenome do signatário
Nome dado	Nome do signatário
Número de série	Identificador único do signatário de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Nome e sobrenome do signatário

3.1.1.3. Certificado Qualificado de Pessoa Física em QSCD

País	Estado[3]
Organização (O)	Organização à qual o signatário está vinculado
Unidade Organizacional (OU)	Unidade da Organização à qual o signatário está vinculado
Identificador da Organização	Identificador único da Organização à qual o signatário está vinculado de acordo com o indicado na ETSI EN 319 412-1
Título	Título ou especialidade do signatário
Sobrenome	Sobrenome do signatário

[2]O campo "Estado" corresponderá ao estado onde ocorre a relação contratual entre o signatário e a entidade a que está vinculado (por ser empregado, associado, sócio ou outro vínculo), independentemente da nacionalidade do trabalhador.

[3]O campo "Estado" corresponderá ao estado onde ocorre a relação contratual entre o signatário e a entidade a que está vinculado (por ser empregado, associado, sócio ou outro vínculo), independentemente da nacionalidade do trabalhador.

Nome dado	Nome do signatário
Número de série	Identificador único do signatário de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Nome e sobrenome do signatário

3.1.1.4. Certificado Qualificado de Pessoa Física em HSM centralizado

País	Estado[4]
Organização (O)	Organização à qual o signatário está vinculado
Unidade Organizacional (OU)	Unidade da Organização à qual o signatário está vinculado
Identificador da Organização	Identificador único da Organização à qual o signatário está vinculado de acordo com o indicado na ETSI EN 319 412-1
Título	Título ou especialidade do signatário
Sobrenome	Sobrenome do signatário
Nome dado	Nome do signatário
Número de série	Identificador único do signatário de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Nome e sobrenome do signatário

3.1.1.5. Certificado Qualificado de Pessoa Física em QSCD centralizado

País	Estado[5]

[4]O campo "Estado" corresponderá ao estado onde ocorre a relação contratual entre o signatário e a entidade a que está vinculado (por ser empregado, associado, sócio ou outro vínculo), independentemente da nacionalidade do trabalhador.

Organização (O)	Organização à qual o signatário está vinculado
Unidade Organizacional (OU)	Unidade da Organização à qual o signatário está vinculado
Identificador da Organização	Identificador único da Organização à qual o signatário está vinculado de acordo com o indicado na ETSI EN 319 412-1
Título	Título ou especialidade do signatário
Sobrenome	Sobrenome do signatário
Nome dado	Nome do signatário
Número de série	Identificador único do signatário de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Nome e sobrenome do signatário

3.1.1.6. Certificado qualificado de assinatura de Pessoa Singular em QSCD centralizado

País	Estado[6]
Organização (O)	Organização à qual o signatário está vinculado
Unidade Organizacional (OU)	Unidade da Organização à qual o signatário está vinculado
Identificador da Organização	Identificador único da Organização à qual o signatário está vinculado de acordo com o indicado na ETSI EN 319 412-1
Título	Título ou especialidade do signatário
Sobrenome	Sobrenome do signatário
Nome dado	Nome do signatário
Número de série	Identificador único do signatário de acordo com as

[5]O campo "Estado" corresponderá ao estado onde ocorre a relação contratual entre o signatário e a entidade a que está vinculado (por ser empregado, associado, sócio ou outro vínculo), independentemente da nacionalidade do trabalhador.

[6]O campo "Estado" corresponderá ao estado onde ocorre a relação contratual entre o signatário e a entidade a que está vinculado (por ser empregado, associado, sócio ou outro vínculo), independentemente da nacionalidade do trabalhador.

	disposições da ETSI EN 319 412-1
Nome Comum (CN)	Nome e sobrenome do signatário

3.1.1.7. Certificado Qualificado de Representante Pessoa Física em software

País	Estado[7]
Organização (O)	Organização que o signatário representa
Unidade Organizacional (OU)	Unidade da Organização à qual o signatário está vinculado
Identificador da Organização	Identificador único da Organização que o signatário representa de acordo com as disposições da ETSI EN 319 412-1
Título	Tipo de representação
Sobrenome	Sobrenome do signatário
Nome dado	Nome do signatário
Número de série	Identificador único do signatário de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Nome e sobrenome do representante

3.1.1.8. Certificado qualificado de assinatura de Representante Pessoa Física no QSCD

País	Estado[8]
Organização (O)	Organização que o signatário representa

[7]O campo "Estado" corresponderá ao estado onde ocorre a relação contratual entre o signatário e a entidade a que está vinculado (por ser empregado, associado, sócio ou outro vínculo), independentemente da nacionalidade do trabalhador.

[8]O campo "Estado" corresponderá ao estado onde ocorre a relação contratual entre o signatário e a entidade a que está vinculado (por ser empregado, associado, sócio ou outro vínculo), independentemente da nacionalidade do trabalhador.

Unidade Organizacional (OU)	Unidade da Organização à qual o signatário está vinculado
Identificador da Organização	Identificador único da Organização que o signatário representa de acordo com as disposições da ETSI EN 319 412-1
Título	Tipo de representação
Sobrenome	Sobrenome do signatário
Nome dado	Nome do signatário
Número de série	Identificador único do signatário de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Nome e sobrenome do representante

3.1.1.9. Certificado qualificado de assinatura do Representante Pessoa Física em QSCD centralizado

País	Estado[9]
Organização (O)	Organização que o signatário representa
Unidade Organizacional (OU)	Unidade da Organização à qual o signatário está vinculado
Identificador da Organização	Identificador único da Organização que o signatário representa de acordo com as disposições da ETSI EN 319 412-1
Título	Tipo de representação
Sobrenome	Sobrenome do signatário
Nome dado	Nome do signatário
Número de série	Identificador único do signatário de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Nome e sobrenome do representante

[9]O campo "Estado" corresponderá ao estado onde ocorre a relação contratual entre o signatário e a entidade a que está vinculado (por ser empregado, associado, sócio ou outro vínculo), independentemente da nacionalidade do trabalhador.

3.1.1.10. Certificado qualificado de selo eletrônico de nível médio APE

País	Estado[10]
Organização (O)	Nome da organização
Unidade Organizacional (OU)	Indica a natureza do certificado
Unidade Organizacional (OU)	Nome da unidade
Unidade Organizacional (OU)	Código da unidade DIR3
Identificador da Organização	Identificador único da Organização de acordo com as disposições da ETSI EN 319 412-1
Sobrenome	Sobrenome do responsável pelo certificado
Nome dado	Nome do responsável pelo certificado
Número de série	Identificador único do signatário de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Nome do sistema ou aplicação do processo automático

3.1.1.11. Certificado qualificado de selo eletrônico de alto nível APE

País	Estado[11]
Organização (O)	Nome da organização
Unidade Organizacional (OU)	Indica a natureza do certificado
Unidade Organizacional (OU)	Nome da unidade
Unidade Organizacional (OU)	Código da unidade DIR3
Identificador da Organização	Identificador único da Organização de acordo com as disposições da ETSI EN 319 412-1
Sobrenome	Sobrenome do responsável pelo certificado

[10] O campo "Estado" será "ES" (Espanha) por se tratar de um certificado destinado a entidades públicas espanholas.

[11] O campo "Estado" será "ES" (Espanha) por se tratar de um certificado destinado a entidades públicas espanholas.

Nome dado	Nome do responsável pelo certificado
Número de série	Identificador único do signatário em conformidade com as disposições da ETSI EN 319 412-1.
Nome Comum (CN)	Nome do sistema ou aplicação do processo automático

3.1.1.12. Certificado de selo eletrônico de alto nível APE qualificado em QSCD centralizado

País	Estado[12]
Organização (O)	Nome da organização
Unidade Organizacional (OU)	Indica a natureza do certificado
Unidade Organizacional (OU)	Nome da unidade
Unidade Organizacional (OU)	Código da unidade DIR3
Identificador da Organização	Identificador único da Organização de acordo com as disposições da ETSI EN 319 412-1
Sobrenome	Sobrenome do responsável pelo certificado
Nome dado	Nome do responsável pelo certificado
Número de série	Identificador único do signatário de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Nome do sistema ou aplicação do processo automático

3.1.1.13. Certificado Qualificado de Funcionário Público de Nível Médio

País	Estado[13]
Organização (O)	Administração, órgão ou entidade de direito público

[12] O campo "Estado" será "ES" (Espanha) por se tratar de um certificado destinado a entidades públicas espanholas.

[13] O campo "Estado" será "ES" (Espanha) por se tratar de um certificado destinado a funcionários públicos espanhóis.

	a que o trabalhador esteja vinculado
Unidade Organizacional (OU)	Descrição do tipo de certificado
Unidade Organizacional (OU)	Unidade, dentro da Administração, que inclui o funcionário responsável pelo certificado
Unidade Organizacional (OU)	Código da unidade DIR3
Unidade Organizacional (OU)	NRP ou PIN do funcionário responsável pelo certificado
Título	Cargo ou cargo da pessoa singular, que a vincule à administração, órgão ou entidade de direito público subscritor do certificado
Sobrenome	Sobrenomes de funcionários públicos
Nome dado	Nome do funcionário público
Número de série	Identificador único do signatário de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Nome, sobrenome e DNI/NIF do funcionário público (signatário)

3.1.1.14. Certificado de autenticação eletrônica para Funcionário Público de Alto Nível

País	Estado[14]
Organização (O)	Administração, órgão ou entidade de direito público a que o trabalhador esteja vinculado
Unidade Organizacional (OU)	Descrição do tipo de certificado
Unidade Organizacional (OU)	Unidade, dentro da Administração, que inclui o funcionário responsável pelo certificado
Unidade Organizacional (OU)	Código da unidade DIR3
Unidade Organizacional (OU)	NRP ou PIN do funcionário responsável pelo certificado
Título	Cargo ou cargo da pessoa singular, que a vincule à

[14] O campo "Estado" será "ES" (Espanha) por se tratar de um certificado destinado a funcionários públicos espanhóis.

	administração, órgão ou entidade de direito público subscritor do certificado
Sobrenome	Sobrenomes de funcionários públicos
Nome dado	Nome do funcionário público
Número de série	Identificador único do signatário de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Nome, sobrenome e DNI/NIF do funcionário público (signatário)

3.1.1.15. Certificado qualificado de assinatura de funcionário público de alto nível

País	Estado[15]
Organização (O)	Administração, órgão ou entidade de direito público a que o trabalhador esteja vinculado
Unidade Organizacional (OU)	Descrição do tipo de certificado
Unidade Organizacional (OU)	Unidade, dentro da Administração, que inclui o funcionário responsável pelo certificado
Unidade Organizacional (OU)	Código da unidade DIR3
Unidade Organizacional (OU)	NRP ou PIN do funcionário responsável pelo certificado
Título	Cargo ou cargo da pessoa singular, que a vincule à administração, órgão ou entidade de direito público subscritor do certificado
Sobrenome	Sobrenomes de funcionários públicos
Nome dado	Nome do funcionário público
Número de série	Identificador único do signatário de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Nome, sobrenome e DNI/NIF do funcionário público (signatário)

[15] O campo "Estado" será "ES" (Espanha) por se tratar de um certificado destinado a funcionários públicos espanhóis.

3.1.1.16. Certificado qualificado de assinatura de Funcionário Público de Alto Nível em QSCD centralizado

País	Estado[16]
Organização (O)	Administração, órgão ou entidade de direito público a que o trabalhador esteja vinculado
Unidade Organizacional (OU)	Descrição do tipo de certificado
Unidade Organizacional (OU)	Unidade, dentro da Administração, que inclui o funcionário responsável pelo certificado
Unidade Organizacional (OU)	Código da unidade DIR3
Unidade Organizacional (OU)	NRP ou PIN do funcionário responsável pelo certificado
Título	Cargo ou cargo da pessoa singular, que a vincule à administração, órgão ou entidade de direito público subscritor do certificado
Sobrenome	Sobrenomes de funcionários públicos
Nome dado	Nome do funcionário público
Número de série	Identificador único do signatário de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Nome, sobrenome e DNI/NIF do funcionário público (signatário)

3.1.1.17. Certificado qualificado de pessoa física Representante de Pessoa Jurídica perante as administrações em software

País	Estado
Organização (O)	Organização da qual o signatário é representante
Unidade Organizacional (OU)	Unidade da Organização à qual pertence o signatário

[16] O campo "Estado" será "ES" (Espanha) por se tratar de um certificado destinado a funcionários públicos espanhóis.

Identificador da Organização	Identificador único da Organização que o signatário representa de acordo com as disposições da ETSI EN 319 412-1
Título	Nome da representação do signatário
Sobrenome	Sobrenome do signatário
Nome dado	Nome do signatário
Número de série	Identificador único do signatário de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Identificador único, nome e apelido do signatário e NIF da organização
Descrição	Informações sobre o registro da outorga de representação

3.1.1.18. Certificado Habilitado de Pessoa Física Representante de Pessoa Jurídica perante as administrações em QSCD

País	Estado
Organização (O)	Organização da qual o signatário é representante
Unidade Organizacional (OU)	Unidade Organização à qual pertence o signatário
Identificador da Organização	Identificador único da Organização que o signatário representa de acordo com as disposições da ETSI EN 319 412-1
Título	Nome da representação do signatário
Sobrenome	Sobrenome do signatário
Nome dado	Nome do signatário
Número de série	Identificador único do signatário em conformidade com as disposições da ETSI EN 319 412-1.
Nome Comum (CN)	Identificador único, nome e apelido do signatário e NIF da organização
Descrição	Informações sobre o registro da outorga de representação

3.1.1.19. Certificado Habilitado de Pessoa Física Representante de Pessoa Jurídica perante as administrações em HSM Centralizado

País	Estado
Organização (O)	Organização da qual o signatário é representante
Unidade Organizacional (OU)	Unidade Organização à qual pertence o signatário
Identificador da Organização	Identificador único da Organização que o signatário representa de acordo com as disposições da ETSI EN 319 412-1
Título	Nome da representação do signatário
Sobrenome	Sobrenome do signatário
Nome dado	Nome do signatário
Número de série	Identificador único do signatário em conformidade com as disposições da ETSI EN 319 412-1.
Nome Comum (CN)	Identificador único, nome e apelido do signatário e NIF da organização
Descrição	Informações sobre o registro da outorga de representação

3.1.1.20. Certificado qualificado de Pessoa Física Representante de Pessoa Jurídica perante as administrações em QSCD centralizado

País	Estado
Organização (O)	Organização da qual o signatário é representante
Unidade Organizacional (OU)	Unidade Organização à qual pertence o signatário
Identificador da Organização	Identificador único da Organização que o signatário representa de acordo com as disposições da ETSI EN 319 412-1
Título	Nome da representação do signatário
Sobrenome	Sobrenome do signatário
Nome dado	Nome do signatário
Número de série	Identificador único do signatário em conformidade com as disposições da ETSI EN 319 412-1.

Nome Comum (CN)	Identificador único, nome e apelido do signatário e NIF da organização
Descrição	Informações sobre o registro da outorga de representação

3.1.1.21. Certificado qualificado de pessoa singular Representante de Entidade sem Personalidade Jurídica perante as administrações em software

País	Estado
Organização (O)	Organização da qual o signatário é representante
Unidade Organizacional (OU)	Unidade Organização à qual pertence o signatário
Identificador da Organização	Identificador único da Organização que o signatário representa de acordo com as disposições da ETSI EN 319 412-1
Título	Nome da representação do signatário
Sobrenome	Sobrenome do signatário
Nome dado	Nome do signatário
Número de série	Identificador único do signatário de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Identificador único, nome e sobrenome do signatário e Identificador único da organização
Descrição	Informações sobre o registro da outorga de representação

3.1.1.22. Certificado qualificado de pessoa singular representante de entidade sem personalidade jurídica perante as administrações em QSCD

País	Estado
Organização (O)	Organização da qual o signatário é representante
Unidade Organizacional (OU)	Unidade Organização à qual pertence o signatário
Identificador da Organização	Identificador único da Organização que o signatário representa de acordo com as disposições da ETSI EN 319 412-1
Título	Nome da representação do signatário
Sobrenome	Sobrenome do signatário

Nome dado	Nome do signatário
Número de série	Identificador único do signatário de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Identificador único, nome e sobrenome do signatário e Identificador único da organização
Descrição	Informações sobre o registro da outorga de representação

3.1.1.23. Certificado qualificado de pessoa singular representante de entidade sem personalidade jurídica perante as administrações em HSM centralizado

País	Estado
Organização (O)	Organização da qual o signatário é representante
Unidade Organizacional (OU)	Unidade Organização à qual pertence o signatário
Identificador da Organização	Identificador único da Organização que o signatário representa de acordo com as disposições da ETSI EN 319 412-1
Título	Nome da representação do signatário
Sobrenome	Sobrenome do signatário
Nome dado	Nome do signatário
Número de série	Identificador único do signatário de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Identificador único, nome e sobrenome do signatário e Identificador único da organização
Descrição	Informações sobre o registro da outorga de representação

3.1.1.24. Certificado qualificado de pessoa singular representante de entidade sem personalidade jurídica perante as administrações em QSCD centralizado

País	Estado
Organização (O)	Organização da qual o signatário é representante
Unidade Organizacional (OU)	Unidade Organização à qual pertence o signatário
Identificador da Organização	Identificador único da Organização que o signatário

	representa de acordo com as disposições da ETSI EN 319 412-1
Título	Nome da representação do signatário
Sobrenome	Sobrenome do signatário
Nome dado	Nome do signatário
Número de série	Identificador único do signatário de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Identificador único, nome e sobrenome do signatário e Identificador único da organização
Descrição	Informações sobre o registro da outorga de representação

3.1.1.25. Certificado de Selo Eletrônico Qualificado em software

País	Informar onde a entidade está registrada a Organização
Organização (O)	Nome da organização
Unidade Organizacional (OU)	Indica a natureza do certificado
Identificador da Organização	Identificador único da Organização à qual o selo eletrónico está vinculado, de acordo com o disposto na ETSI EN 319 412-1
Sobrenome	Sobrenome do responsável pelo certificado
Nome dado	Nome do responsável pelo certificado
Número de série	Identificador único da pessoa responsável pelo certificado de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Nome do sistema automático

3.1.1.26. Certificado de Selo Eletrônico Qualificado em QSCD

País	Informar onde a entidade está registrada a Organização
Organização (O)	Nome da organização
Unidade Organizacional (OU)	Indica a natureza do certificado

Identificador da Organização	Identificador único da Organização à qual o selo eletrónico está vinculado, de acordo com o disposto na ETSI EN 319 412-1
Sobrenome	Sobrenome do responsável pelo certificado
Nome dado	Nome do responsável pelo certificado
Número de série	Identificador único da pessoa responsável pelo certificado de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Nome do sistema automático

3.1.1.27. Certificado Qualificado de Selo Eletrônico em HSM Centralizado

País	Informar onde a entidade está registrada a Organização
Organização (O)	Nome da organização
Unidade Organizacional (OU)	Indica a natureza do certificado
Identificador da Organização	Identificador único da Organização à qual o selo eletrónico está vinculado, de acordo com o disposto na ETSI EN 319 412-1
Sobrenome	Sobrenome do responsável pelo certificado
Nome dado	Nome do responsável pelo certificado
Número de série	Identificador único da pessoa responsável pelo certificado de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Nome do sistema automático

3.1.1.28. Certificado de Selo Eletrônico Qualificado em QSCD centralizado

País	Informar onde a entidade está registrada a Organização
Organização (O)	Nome da organização
Unidade Organizacional (OU)	Indica a natureza do certificado
Identificador da Organização	Identificador único da Organização à qual o selo

	eletrónico está vinculado, de acordo com o disposto na ETSI EN 319 412-1
Sobrenome	Sobrenome do responsável pelo certificado
Nome dado	Nome do responsável pelo certificado
Número de série	Identificador único da pessoa responsável pelo certificado de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Nome do sistema automático

3.1.1.29. Certificado de selo eletrônico qualificado para PSD2 em software

País	Informar onde a entidade está registrada a Organização
Organização (O)	Nome da organização
Unidade Organizacional (OU)	Indica a natureza do certificado
Identificador da Organização	Número de autorização como prestador de serviços de pagamento concedido pela autoridade nacional competente
Sobrenome	Sobrenome do responsável pelo certificado
Nome dado	Nome do responsável pelo certificado
Número de série	Identificador único da Organização da Organização à qual o selo eletrónico está vinculado , de acordo com o disposto na ETSI EN 319 412-1
Nome Comum (CN)	Nome descritivo do criador do selo

3.1.1.30. Certificado de Selo Eletrônico Qualificado para PSD2 em HSM Centralizado

País	Informar onde a entidade está registrada a Organização
Organização (O)	Nome da organização
Unidade Organizacional (OU)	Indica a natureza do certificado
Identificador da Organização	Número de autorização como prestador de serviços de pagamento concedido pela autoridade nacional

	competente
Sobrenome	Sobrenome do responsável pelo certificado
Nome dado	Nome do responsável pelo certificado
Número de série	Identificador único da Organização da Organização à qual o selo eletrónico está vinculado , de acordo com o disposto na ETSI EN 319 412-1
Nome Comum (CN)	Nome descritivo do criador do selo

3.1.1.31. Certificado de Selo Eletrônico Qualificado para PSD2 em QSCD centralizado

País	Informar onde a entidade está registrada a Organização
Organização (O)	Nome da organização
Unidade Organizacional (OU)	Indica a natureza do certificado
Identificador da Organização	Número de autorização como prestador de serviços de pagamento concedido pela autoridade nacional competente
Sobrenome	Sobrenome do responsável pelo certificado
Nome dado	Nome do responsável pelo certificado
Número de série	Identificador único da Organização da Organização à qual o selo eletrónico está vinculado , de acordo com o disposto na ETSI EN 319 412-1
Nome Comum (CN)	Nome descritivo do criador do selo

3.1.1.32. Certificado de carimbo de data/hora eletrônico qualificado

País	Estado de onde o serviço é prestado
Organização (O)	Nome da organização
Localização (L)	Localização da organização
Identificador da Organização	Identificador único da Organização de acordo com as disposições da ETSI EN 319 412-1
Nome Comum (CN)	Nome do Serviço
Unidade Organizacional (OU)	Unidade que presta o serviço

3.1.2. Significado dos nomes

Os nomes contidos nos campos *SubjectName* e *SubjectAlternativeName* dos certificados são compreensíveis em linguagem natural, conforme estabelecido na seção anterior.

3.1.2.1. Emissão de certificados de conjuntos de testes e certificados de testes em geral

A emissão dos certificados de ensaio deverá ser realizada com os seguintes dados identificativos:

- Número do Documento Nacional de Identidade (DNI): 00000000T
- Número de Identidade de Estrangeiro (NIE): X0000000T, Y0000000R, Z0000000W
- Nome nome
- Sobrenome: Sobrenome1
- Segundo sobrenome: Sobrenome2

Os restantes campos que compõem o "DN" ou "Assunto" do certificado devem utilizar palavras que indiquem a sua invalidade (ex. "TESTE", "Teste" ou "Inválido").

Se necessário e com aviso prévio ao Órgão Fiscalizador Nacional, a UANATACA poderá gerar certificados de testes com outros dados, cuja validade estará limitada à duração dos testes.

Todos os certificados de teste serão considerados sem validade legal e, portanto, sem qualquer responsabilidade da UANATACA.

Esses certificados são emitidos para realizar testes técnicos de interoperabilidade e permitir que o órgão regulador os avalie.

3.1.3. Uso de anônimos e pseudônimos

Sob nenhuma circunstância poderão ser utilizados pseudônimos para identificar uma entidade, empresa ou organização, ou um signatário. Da mesma forma, em nenhum caso são emitidos certificados anônimos.

3.1.4. Interpretação de formatos de nomes

Os formatos de nome serão interpretados de acordo com a lei do país de estabelecimento do assinante, nos seus próprios termos.

O campo "país" ou "estado" será o do titular do certificado.

Os certificados cujos assinantes sejam pessoas colectivas, entidades ou organismos da administração pública, evidenciam a relação entre estes e uma pessoa singular, independentemente da nacionalidade da pessoa singular.

O campo "número de série" inclui o DNI, NIE, Passaporte ou outro número de identificação adequado do signatário, reconhecido por lei.

Sem prejuízo do acima exposto, qualquer tipo de certificado eletrônico qualificado , quando emitido para identificação de interessados perante as Administrações Públicas, deverá conter como atributos **seu nome** e **sobrenome** e seu **número Documento Nacional de Identidade, Número de Identificação de Estrangeiro ou Número de Identificação Fiscal** de forma inequívoca, conforme o caso.

3.1.5. Singularidade dos nomes

Os nomes dos assinantes do certificado serão únicos, para cada política de certificado UANATACA.

Um nome de assinante já utilizado não pode ser atribuído a um assinante diferente, situação que, em princípio, não deveria ocorrer, graças à presença do número de Identificação Fiscal, ou equivalente, no esquema de nomenclatura.

Um assinante pode solicitar mais de um certificado desde que a combinação dos seguintes valores na solicitação seja diferente de um certificado válido:

- Número de Identificação Fiscal (NIF) ou outro identificador legalmente válido da pessoa singular.

- Número de Identificação Fiscal (CIF/NIF) ou outro identificador legalmente válido do assinante.
- Tipo de certificado (OID do identificador da política de certificação).
- Suporte de certificado (QSCD, software, HSM centralizado, QSCD centralizado)

Excecionalmente, esta DPC permite a emissão de um certificado quando o CIF/NIF do assinante, o NIF do signatário, o Tipo de certificado e o Suporte do certificado coincidem com um certificado ativo, desde que exista algum elemento diferenciador entre os dois, em os campos cargo (cargo) e/ou departamento (Unidade Organizacional).

3.1.6. Resolvendo conflitos de nomes

Os solicitantes do certificado não incluirão nas solicitações nomes que possam implicar violação, por parte do futuro assinante, de direitos de terceiros.

A UANATACA não será obrigada a determinar previamente que o requerente do certificado detém direitos de propriedade industrial sobre o nome que consta do pedido de certificado, mas procederá, em princípio, à sua certificação.

Da mesma forma, não atuará como árbitro ou mediador, nem de qualquer outra forma resolverá qualquer disputa relativa à propriedade de nomes de pessoas ou organizações, números de identificação de empresas, nomes de domínio, marcas ou nomes comerciais.

No entanto, se você receber uma notificação sobre um conflito de nome, de acordo com a legislação do país do assinante, você poderá tomar as medidas adequadas para bloquear ou retirar o certificado emitido.

Em qualquer caso, o prestador de serviços eletrónicos de confiança reserva-se o direito de rejeitar um pedido de certificado devido a conflitos de nomes e/ou discrepâncias entre os dados apresentados pelo requerente e o conteúdo incluído nos registos oficiais.

Qualquer controvérsia ou conflito decorrente deste documento será definitivamente resolvido, através da arbitragem legal de um árbitro, no âmbito do Tribunal Arbitral

Espanhol, de acordo com o seu Regulamento e Estatuto, ao qual é confiada a administração da arbitragem e o nomeação do árbitro ou tribunal arbitral. As partes manifestam o seu compromisso de cumprimento da adjudicação emitida no documento contratual que formaliza o serviço.

3.2. Validação de identidade inicial

A identidade dos subscritores do certificado é estabelecida no momento da assinatura do contrato entre a UANATACA e o subscritor, momento em que se verifica a existência do subscritor através do seu documento oficial de identidade ou escritura correspondente, bem como os poderes de atuação do pessoa que se apresenta como representante, se aplicável. Para esta verificação poderá ser utilizada documentação pública ou notarial, ou consulta direta aos registos públicos correspondentes.

No caso de pessoas físicas identificadas em certificados cujo titular seja pessoa jurídica, suas identidades serão validadas por meio dos registros societários da entidade, empresa ou organização de direito público ou privado, titular dos certificados. O assinante produzirá uma certificação dos dados necessários, e os enviará à UANATACA, pelo meio que lhe for permitido, para o registo da identidade dos signatários.

No caso dos Prestadores de Serviços de Pagamento, para emissão de certificados qualificados de Selo Electrónico para PSD2, além do acima referido, serão validados os atributos específicos deste tipo de organização (número de autorização, função, nome da Autoridade Autoridade Nacional Competente, etc.) consultando a informação disponibilizada pelas Autoridades Nacionais Competentes.

3.2.1. Prova de posse de chave privada

A posse da chave privada é demonstrada em virtude do procedimento confiável de entrega e aceitação do certificado pelo assinante, em certificados de selo, ou pelo signatário, em certificados de assinatura.

3.2.2. Validação de identidade

Para a solicitação do certificado, os Operadores de Registro da UANATACA verificarão a identidade do signatário para quem o certificado é emitido (ver pessoa física ou

representante autorizado da pessoa jurídica), bem como qualquer atributo específico da pessoa física ou jurídica com a qual tem um relacionamento ou conexão.

A verificação será realizada diretamente ou por meio de terceiros, de acordo com a legislação nacional, de acordo com os seguintes métodos:

a) Na presença da pessoa física ou de representante autorizado da pessoa jurídica. O comparecimento poderá ser dispensado quando o pedido de emissão de certidão qualificada tiver sido legitimado em presença notarial, ou
b) Remotamente, através de meios e identificação electrónica, para os quais tenha sido garantida a presença da pessoa singular de um representante autorizado da pessoa colectiva antes da emissão do certificado qualificado e que cumpram os requisitos estabelecidos no artigo 8.º do Regulamento eIDAS no que diz respeito níveis de segurança "substanciais" ou "altos", ou
c) Por meio de certificado de assinatura eletrónica qualificada ou de selo eletrónico qualificado emitido nos termos da alínea a) ou b), ou
d) Através do procedimento de identificação eletrónica através do sistema de identificação remota por vídeo UANATACA, de acordo com os métodos de identificação reconhecidos nacionalmente através do Despacho ETD/465/2021, de 6 de maio, que regulamenta os métodos de identificação.

Sem prejuízo do anterior, a validação de identidade não será exigida quando a identidade ou outras circunstâncias permanentes dos signatários a quem os certificados são emitidos já estejam registadas na UANATACA em virtude de uma relação pré-existente, desde que para identificar o signatário, foi utilizado um método de identificação presencial e não se passaram mais de 5 anos.

3.2.3. Autenticação da identidade de uma organização, empresa ou entidade através de um representante

As pessoas singulares com capacidade para agir em nome de pessoas colectivas ou entidades sem personalidade jurídica, públicas ou privadas, que sejam subscritores de certificados, podem actuar como seus representantes, desde que exista uma situação prévia de representação legal ou voluntária entre elas. a pessoa singular e a organização

em causa, o que carece de reconhecimento por parte da UANATACA, o que se realizará através do seguinte procedimento:

1. O representante do assinante deverá comprovar a sua identidade através de um dos métodos de identificação especificados na secção 3.2.2., de forma a que:
    - (i) Se você se identificar pessoalmente perante um operador ou pessoa autorizada de uma Autoridade de Registro UANATACA:
        - Apresentando o seu Documento de Identidade, passaporte ou outro meio idóneo reconhecido por lei para a identificação do representante.
        - Acreditando o caráter e os poderes que ele afirma possuir.

    - (ii) Caso você se identifique eletronicamente através do sistema de identificação remota por vídeo UANATACA:
        - Apresentando o seu Documento de Identidade, passaporte ou outro meio idóneo reconhecido por lei para a identificação do representante.
        - Fornecimento de prova de vida através da utilização de meios técnicos de captura de imagens e vídeo utilizando algoritmos de criptografia biométrica facial e inteligência artificial para a comparação inequívoca da identidade do requerente e a verificação da prova de vida do requerente, bem como da autenticidade do documento de identificação exibido.
        - Acreditando o caráter e os poderes que ele afirma possuir.

2. O representante fornecerá as seguintes informações e os documentos comprovativos correspondentes:
    - Os seus dados de identificação, como representante:
        - Nomes e sobrenomes
        - Local e data de nascimento
        - Documento: Documento de identidade, passaporte ou outro meio idóneo reconhecido por lei para a identificação do representante.
    - Os dados de identificação do assinante que representa:
        - Denominação ou razão social.

- Toda a informação cadastral existente, incluindo dados relativos à constituição e personalidade jurídica e à extensão e validade dos poderes de representação do requerente.
- Documento: NIF ou documento comprovativo da identificação fiscal da entidade.
- Documento: Documentos públicos que servem para certificar de forma confiável os pontos acima mencionados e seu registro no registro público correspondente, se necessário. A referida verificação poderá também ser efectuada através de consulta ao registo público em que se encontrem registados os documentos de constituição e procuração, podendo utilizar os meios telemáticos disponibilizados pelos referidos registos públicos.

- Os dados relativos à representação ou qualidade de exercício exercida:
  - A validade da representação ou a capacidade para agir (data de início e término), se aplicável.
  - O âmbito e os limites, se for o caso, da representação ou da capacidade de atuação:
    - TOTAL. Representação ou capacidade total. Esta verificação pode ser efetuada através de consulta eletrónica ao registo público onde está registada a representação.
    - PARCIAL. Representação ou capacidade parcial. Essa verificação poderá ser realizada por meio de cópia eletrônica autêntica do instrumento notarial de procuração, nos termos do regulamento notarial.

3. O operador ou pessoal autorizado da Autoridade de Registro UANATACA verificará a identidade do representante agindo da seguinte forma:
   - Quando a identificação tiver sido realizada presencialmente, através da análise de:
     - Documento de identificação fornecido.
     - Documentação que comprove sua representação.

- Quando a identificação tiver sido realizada através do método de identificação eletrônica através da identificação por vídeo UANATACA através de:
  - Revisão dos vídeos e imagens captadas do documento de identificação fornecido e do próprio requerente.
  - Revisão da prova de vida do requerente, através dos resultados fornecidos pelo sistema remoto de identificação por vídeo.
  - Revisão da comparação produzida pelo sistema de identificação remota por vídeo da fotografia do documento de identidade com as imagens e vídeo obtidos durante o registo do requerente.
  - Revisão produzida pelo sistema de identificação remota por vídeo, através de inteligência artificial para detecção de documentos de identidade falsos.
  - Documentação que comprove sua representação.

4. O operador ou pessoal autorizado da Autoridade de Registro UANATACA verificará as informações fornecidas para autenticação e devolverá a documentação original fornecida quando apropriado.

5. Alternativamente, a assinatura do formulário poderá ser reconhecida em cartório e enviada ao operador ou pessoal autorizado da Autoridade de Registro UANATACA por correio postal certificado, caso em que não serão necessários os passos 3 e 4 acima.

A prestação do serviço de certificação digital é formalizada através de contrato próprio entre a UANATACA e o assinante, devidamente representado.

3.2.4. Autenticação da identidade de um prestador de serviços de pagamento

Sem prejuízo do disposto na secção anterior, ao tentar validar a identidade de um Prestador de Serviços de Pagamento, a UANATACA verificará:

1. O número de autorização ou outro identificador reconhecido emitido por uma Autoridade Nacional Competente que certifique que o Prestador de Serviços de Pagamento pode desempenhar a sua função.

2. O papel desempenhado pelo prestador de serviços de pagamento relacionado com o número de autorização.

3. O nome da Autoridade Nacional Competente.

4. Todas as informações necessárias de acordo com as regras estabelecidas pelas Autoridades Nacionais Competentes.

Para validá-los, será utilizada a informação publicada pelas Autoridades Nacionais Competentes, quer através dos registos nacionais públicos e/ou dos registos e instituições da Autoridade Bancária Europeia (EBA).

3.2.5. Autenticação da identidade de uma pessoa física

Esta seção descreve os métodos de verificação da identidade de uma pessoa física identificada em um certificado.

3.2.5.1. Nos certificados

A identidade das pessoas singulares signatárias identificadas nos certificados é validada através dos métodos de identificação especificados na secção 3.2.2., de forma a que:

- (i) Se você se identificar pessoalmente perante um operador ou pessoa autorizada de uma Autoridade de Registro UANATACA:
  - Apresentando o seu Documento de Identidade, passaporte ou outro meio idóneo reconhecido por lei.

- (ii) Se você se identificar eletronicamente através do sistema de identificação remota por vídeo UANATACA:
  - Apresentando o seu Documento de Identidade, passaporte ou outro meio idóneo reconhecido por lei.
  - Fornecimento de prova de vida através da utilização de meios técnicos de captura de imagens e vídeo utilizando algoritmos de criptografia biométrica facial e inteligência artificial para a comparação inequívoca da identidade do requerente e a

verificação da prova de vida do requerente, bem como da autenticidade do documento de identificação exibido.

Os dados de identificação das pessoas singulares identificadas nos certificados cujo titular seja uma entidade com ou sem personalidade jurídica, poderão ser validados através da comparação dos dados constantes do pedido com os registos da entidade , empresa ou organismo de direito público ou privado a que se pertence. vinculado, ou com a documentação que tenha fornecido sobre a pessoa física que identifica como signatária, garantindo a veracidade das informações a serem certificadas.

3.2.5.2. Validação de identidade

Para solicitar certificados, o operador ou pessoal autorizado da Autoridade de Registro UANATACA verificará a identidade da pessoa física identificada na solicitação de certificado, agindo da seguinte forma:

- Quando a identificação tiver sido realizada presencialmente, através da análise de:
  - Documento de identificação fornecido.

- Quando a identificação tiver sido realizada através do método de identificação eletrônica através da identificação por vídeo UANATACA através de:
  - Revisão dos vídeos e imagens captadas do documento de identificação fornecido e do próprio requerente.
  - Revisão da prova de vida do requerente, através dos resultados fornecidos pelo sistema remoto de identificação por vídeo.
  - Revisão da comparação produzida pelo sistema de identificação remota por vídeo da fotografia do documento de identidade com as imagens e vídeo obtidos durante o registo do requerente.
  - Revisão produzida pelo sistema de identificação remota por vídeo, através de inteligência artificial para detecção de documentos de identidade falsos.

Para solicitação de certificados cujo titular seja pessoa jurídica, não é necessária a presença física direta, devido ao relacionamento já credenciado entre a pessoa física e entidade, empresa ou organização de direito público ou privado a que esteja vinculado,

desde que não tenham decorrido mais de 5 (cinco) anos desde a identificação. No entanto, antes da entrega de um certificado, a entidade subscritora, empresa ou organização de direito público ou privado, através do seu certificador, se tiver um, ou outro membro designado, deve verificar a identidade da pessoa singular identificada no certificado através de um dos procedimentos descritos no parágrafo anterior.

Durante este processo é rigorosamente confirmada a identidade da pessoa singular identificada no certificado. Por este motivo, em todos os casos em que é emitido um certificado, a identidade da pessoa singular assinante é acreditada junto de um operador de registo.

A Autoridade de Registo verificará, através da exibição de documentos ou através de fontes de informação próprias, os restantes dados e atributos a incluir no certificado, guardando documentação que comprove a sua validade.

3.2.5.3. Vinculação da pessoa física

A justificação documental da ligação de uma pessoa singular identificada em certidão à entidade, empresa ou organização de direito público ou privado dá-se pelo seu registo nos registos internos (contrato de trabalho como trabalhador por conta de outrem, ou contrato comercial que a vincula, ou a ata indicando o seu cargo, ou a candidatura como membro da organização...) de cada uma das pessoas públicas e privadas a que estão vinculados.

3.2.6. Informações de assinante não verificadas

UANATACA não inclui nenhuma informação não verificada do assinante nos certificados, exceto o endereço de e-mail do assinante ou signatário.

3.2.7. Autenticação da identidade de um RA e seus operadores

Para a constituição de uma nova Autoridade de Registo, a UANATACA realiza as verificações necessárias para confirmar a existência da entidade ou organização em

questão. Para isso, a UANATACA poderá recorrer à exposição documental ou utilizar fontes próprias de informação.

Da mesma forma, a UANATACA, diretamente ou através da sua Autoridade de Registo, verifica e valida a identidade dos operadores das Autoridades de Registo, para o que estas enviam à UANATACA a documentação de identificação correspondente ao novo operador, juntamente com a sua autorização para atuar como tal.

A UANATACA assegura que os operadores da Autoridade de Registo recebem formação suficiente para o desempenho das suas funções, o que é verificado com a avaliação correspondente. A referida formação e avaliação poderão ser realizadas pela Autoridade de Registo previamente autorizada pela UANATACA.

Para a prestação dos serviços, a UANATACA garante que os operadores da Autoridade de Registo acedem ao sistema através de autenticação forte com certificado digital.

3.3. Identificação e autenticação de pedidos de renovação

3.3.1. Validação para renovação de certificado de rotina

Antes de renovar um certificado, o operador ou pessoal autorizado da Autoridade de Registo UANATACA verifica se as informações utilizadas para verificar a identidade e os restantes dados do assinante e da pessoa singular identificada no certificado continuam válidos.

Os métodos aceitáveis para tal verificação são:

- A utilização do código "CRE" ou "ERC" relativo ao certificado anterior, ou outros métodos de autenticação pessoal, que consiste em informação que só a pessoa singular identificada no certificado conhece, e que lhe permite renovar automaticamente o seu certificado, desde que que o prazo máximo legalmente estabelecido não tenha sido ultrapassado.
- Não foi ultrapassado o uso do certificado atual para a sua renovação e o prazo máximo legalmente estabelecido para esta possibilidade.

Caso alguma informação do assinante ou da pessoa singular identificada no certificado tenha sido alterada, a nova informação é devidamente registada e é produzida uma identificação completa, de acordo com o disposto na secção 3.2.

3.3.2. Identificação e autenticação do pedido de renovação

Antes de renovar um certificado, o operador ou pessoal autorizado da Autoridade de Registro UANATACA verificará se as informações utilizadas no momento para verificar a identidade e os demais dados do assinante e da pessoa física identificada no certificado continuam válidas, em que caso Neste caso, aplicar-se-á o disposto na secção anterior.

A renovação de certificados após revogação não será possível nos seguintes casos:

- O certificado foi revogado devido à emissão errada a uma pessoa diferente da pessoa identificada no certificado.
- O certificado foi revogado devido à emissão não autorizada pela pessoa física identificada no certificado.
- O certificado revogado pode conter informações erradas ou falsas.

Caso alguma informação do assinante ou da pessoa singular identificada no certificado tenha sido alterada, a nova informação é devidamente registada e é produzida uma identificação completa, de acordo com o disposto na secção 3.2.

Sem prejuízo do acima exposto, no que diz respeito à renovação de certificados de selo eletrónico qualificado para PSD2, a UANATACA efetuará uma identificação completa, especialmente dos atributos específicos que caracterizam este tipo de certificados.

3.4. Identificação e autenticação do pedido de revogação, suspensão ou reativação

A UANATACA ou um operador ou pessoal autorizado da Autoridade de Registo autentica os pedidos e relatórios relativos à revogação, suspensão ou reactivação de um certificado, verificando se provêm de uma pessoa autorizada.

A identificação dos assinantes e/ou signatários em processo de revogação, suspensão ou reativação de certificados poderá ser realizada por:

- O assinante e/ou signatário:
  - Identificar-se e autenticar-se através da utilização do Código de Revogação (ERC ou ERC) através do site da UANATACA 24x7.
  - Outros meios de comunicação, como telefone, e-mail, etc. quando houver garantias razoáveis da identidade do requerente da suspensão ou revogação, na opinião da UANATACA e/ou das Autoridades de Registro.

- As autoridades de registro de Uanataca: deverão identificar o signatário e/ou assinante diante de um pedido de revogação, suspensão ou reativação de acordo com os meios que considerem necessários. Será considerado que foi corretamente identificado:
  - Através de solicitação enviada pelo signatário, assinada junto com o próprio certificado.
  - Através de requerimento assinado pelo assinante ou seu representante, comprovando sua identidade e poderes.

Quando durante o horário comercial o assinante deseja iniciar um pedido de revogação e há dúvidas quanto à sua identificação, seu certificado entra em estado de suspensão.

4. Requisitos de operação do ciclo de vida do certificado

4.1. Solicitação de emissão de certificado

4.1.1. Legitimação para solicitar a emissão

O requerente do certificado, seja pessoa singular ou coletiva, deverá celebrar um contrato de prestação de serviços de certificação com a UANATACA.

Da mesma forma, antes da emissão e entrega de um certificado, deve haver um pedido de certificados quer no próprio contrato, num documento específico de formulário de pedido de certificado ou junto da autoridade de registo.

Quando o requerente for outra pessoa que não o assinante, deverá haver autorização do titular para que o requerente possa efetuar o pedido, o qual é legalmente concretizado através de formulário de pedido de certificado assinado pelo referido requerente em seu próprio nome, no caso de certificados para uma pessoa física, ou em nome do assinante, caso o assinante seja pessoa jurídica, empresa ou organização de direito público ou privado.

4.1.2. Procedimento de registro e responsabilidades

A UANATACA recebe solicitações de certidões, feitas por pessoas, entidades, empresas ou organizações de direito público ou privado.

As solicitações são implementadas através de formulário em papel ou formato eletrônico, individualmente ou em lotes, ou através da conexão com bases de dados externas, ou através de uma camada *de Web Services* cujo destinatário é a UANATACA. No caso de certificados cujo titular seja uma entidade, empresa ou organização de direito público ou privado que atue como Autoridade de Registo da UANATACA, poderá gerir diretamente os pedidos acedendo aos sistemas informáticos da UANATACA e gerar os certificados correspondentes para a própria entidade. empresa ou organização ou para seus membros.

O pedido deverá ser acompanhado de documentação comprovativa da identidade e demais circunstâncias da pessoa singular identificada no certificado, de acordo com o disposto na secção 3.2.5. Deverá também ser incluída uma morada física ou outra informação que permita contactar a pessoa singular identificada no certificado.

4.2. Processamento de Solicitação de Certificação

4.2.1. Execução de funções de identificação e autenticação

Assim que uma solicitação de certificado for recebida, a UANATACA garante que as solicitações de certificado sejam completas, precisas e devidamente autorizadas antes de processá-las.

Em caso afirmativo, a UANATACA verifica a informação prestada, verificando os aspectos descritos na secção 3.2

No caso de certificado qualificado, a documentação que comprova a aprovação do pedido deverá ser conservada e devidamente registrada e com garantias de segurança e integridade durante o período de 15 anos contados da expiração do certificado ou do término do serviço prestado, ainda em caso de perda antecipada de validade por revogação.

4.2.2. Aprovação ou rejeição do pedido

Se os dados forem verificados corretamente, a UANATACA deverá aprovar o pedido do certificado e proceder à sua emissão e entrega.

Se a verificação indicar que a informação não está correta, ou se houver suspeita de que não está correta ou que pode afetar a reputação da Autoridade Certificadora, das Autoridades de Registro ou dos assinantes, a UANATACA negará o pedido, ou interromperá o seu processamento. .aprovação até que sejam realizadas as verificações adicionais que julgar oportunas.

Caso as verificações adicionais não revelem a veracidade da informação a verificar, a UANATACA negará definitivamente o pedido.
A UANATACA notifica o requerente da aprovação ou indeferimento do pedido.

4.2.3. Prazo para resolver a solicitação

A UANATACA responde às solicitações de certificados por ordem de chegada, dentro de um prazo razoável, podendo ser especificado no contrato de emissão do certificado um prazo máximo de garantia.

As solicitações permanecem ativas até serem aprovadas ou rejeitadas.

4.3. Emissão de certificado

4.3.1. Ações da CA durante o processo de emissão

Após a aprovação da solicitação de certificação, o certificado é emitido de forma segura e disponibilizado ao signatário para aceitação.

Os procedimentos estabelecidos nesta secção aplicam-se também no caso de renovação de certificado, uma vez que esta implica a emissão de um novo certificado.

Durante o processo, UANATACA:

- Protege a confidencialidade e integridade dos dados cadastrais disponíveis para você.
- Utilizar sistemas e produtos confiáveis, protegidos contra qualquer alteração e que garantam a segurança técnica e, se for o caso, criptográfica dos processos de certificação que suportam.
- Gera o par de chaves, usando um procedimento de geração de certificado vinculado de forma segura ao procedimento de geração de chaves.
- Ele emprega um procedimento de geração de certificado que vincula de forma segura o certificado às informações de registro, incluindo a chave pública certificada.

- Garante que o certificado é emitido por sistemas que utilizam proteção antifalsificação e que garantem a confidencialidade das chaves durante o processo de geração de chaves.
- Indica a data e hora em que um certificado foi emitido.
- Garante o controle exclusivo das chaves por parte do usuário, não podendo a própria UANATACA ou suas Autoridades de Registro deduzi-las ou utilizá-las de forma alguma.

4.3.2. Notificação de problema ao assinante

A UANATACA notifica a emissão do certificado ao assinante e/ou à pessoa singular identificada no certificado e ao método de geração/descarregamento.

Relativamente aos certificados de Representação, a UANATACA assinou um contrato com o Colégio de Registos Imobiliários e Comerciais de Espanha, doravante CORPME, ao abrigo do qual a CORPME oferece a recepção de informação relativa aos registos imobiliários e comerciais à UANATACA, devendo a UANATACA notificar a CORPME de a emissão de certificado representativo de administrador único ou co-administrador, bem como a revogação do referido certificado.

No caso de Certificados de Selo Eletrônico qualificados para PSD2, a UANATACA notificará a Autoridade Nacional Competente da informação relativa ao certificado emitido de acordo com o disposto no regulamento de referência, desde que tenha informado à UANATACA um endereço de e-mail onde você pode enviar essas notificações.

4.4. Entrega e aceitação do certificado

4.4.1. Responsabilidades da CA

Durante este processo, o operador ou pessoal autorizado da Autoridade de Registro UANATACA deverá realizar as seguintes ações:

- Comprovar definitivamente a identidade da pessoa singular identificada no certificado, de acordo com o disposto nos pontos 3.2.3e 3.2.5.
- Ter o Contrato de Prestação de Serviços de Confiança devidamente assinado pelo Assinante.
- Entregar a folha de entrega e aceitação do certificado à pessoa singular identificada no certificado com o seguinte conteúdo mínimo:
    - Informações básicas sobre a utilização do certificado, incluindo especialmente informações sobre o prestador de serviços de certificação e a Declaração de Práticas de Certificação aplicável, tais como suas obrigações, poderes e responsabilidades.
    - Informações sobre o certificado.
    - Reconhecimento, por parte do signatário, da recepção do certificado e/ou dos mecanismos para a sua geração/descarregamento e da aceitação dos elementos acima mencionados.
    - Regime de obrigações do signatário.
    - Responsabilidade do signatário.
    - Método de atribuição exclusiva ao signatário da sua chave privada e dos dados de ativação do seu certificado, de acordo com o disposto nas secções 6.2 e 6.4.
    - A data do ato de entrega e aceitação.

  Todas essas informações poderão constar no próprio Contrato de Prestação de Serviços de Confiança. Dito isto, quando o Assinante assinar o Contrato de Prestação de Serviços de Confiança, a entrega e aceitação do certificado considerar-se-á concluída.
- Obtenha a assinatura da pessoa identificada no certificado.

As Autoridades de Registo são responsáveis pela realização destes processos, devendo documentar os actos anteriores e preservar os referidos documentos originais (fichas de entrega e aceitação), enviando uma cópia electrónica à UANATACA, bem como os originais quando a UANATACA solicitar o acesso aos mesmos. .

4.4.2. Conduta que constitui aceitação do certificado

Quando a folha de aceitação é entregue, a aceitação do certificado pela pessoa singular identificada no certificado ocorre mediante assinatura da folha de entrega e aceitação.

Quando a geração e entrega do certificado for realizada através do procedimento automatizado definido pela UANATACA, a aceitação do certificado pela pessoa física nele identificada ocorre mediante assinatura do contrato de Prestação de Serviços de Confiança utilizando o próprio certificado.

4.4.3. Publicação de certificado

A UANATACA publica o certificado no Depositário referido no ponto 2.1, com os respetivos controlos de segurança e desde que a UANATACA tenha a autorização da pessoa singular identificada no certificado.

4.4.4. Notificação do problema a terceiros

A UANATACA não efetua qualquer notificação de emissão de certificados a terceiros, exceto nos casos abaixo previstos.

- Relativamente aos certificados de Representante qualificado, a UANATACA assinou um contrato com o Colégio de Registos Imobiliários e Comerciais de Espanha, doravante CORPME, ao abrigo do qual a CORPME oferece a recepção de informação relativa aos registos imobiliários e comerciais à UANATACA, devendo a UANATACA notificar a CORPME de a emissão de certificado representativo de administrador único ou co-administrador, bem como a revogação do referido certificado.

- Relativamente aos Certificados de Selo Electrónico qualificados para PSD2, a UANATACA notificará a Autoridade Nacional Competente da informação relativa ao certificado emitido de acordo com o disposto no regulamento de referência, desde que tenha informado à UANATACA um endereço de correio electrónico para onde possa dirigir-se. essas notificações.

4.5. Usando o par de chaves e o certificado

4.5.1. Utilização pelo signatário

A UANATACA obriga:

- Fornecer à UANATACA informações completas e adequadas, de acordo com os requisitos desta Declaração de Práticas de Certificação, especialmente no que diz respeito ao procedimento de registro.
- Expresse seu consentimento antes da emissão e entrega de um certificado.
- Use o certificado de acordo com as disposições da seção 1.4.
- Quando o certificado funcionar em conjunto com um DCCF, reconhecer a sua capacidade de produzir assinaturas eletrónicas qualificadas; isto é, equivalentes a assinaturas manuscritas, bem como outros tipos de assinaturas eletrônicas e mecanismos de criptografia de informações.
- Seja especialmente diligente na salvaguarda da sua chave privada, a fim de evitar o uso não autorizado.
- Informar a UANATACA, as Autoridades de Registo e qualquer pessoa que possa confiar no certificado, sem atrasos injustificáveis:
    - A perda, roubo ou potencial comprometimento de sua chave privada.
    - Perda de controle sobre sua chave privada, devido ao comprometimento dos dados de ativação (por exemplo, código PIN) ou por qualquer outro motivo.
    - Imprecisões ou alterações no conteúdo do certificado que o assinante conhece ou poderia conhecer.
- Deixar de utilizar a chave privada após o período indicado na secção 6.3.2.

A UANATACA obriga o signatário a ser responsável por:

- Que todas as informações fornecidas pelo signatário contidas no certificado estão corretas.
- Que o certificado seja utilizado exclusivamente para usos legais e autorizados, de acordo com a Declaração de Práticas de Certificação.
- Que nenhuma pessoa não autorizada jamais teve acesso à chave privada do certificado e que você é o único responsável por quaisquer danos causados pela sua falha em proteger a chave privada.

- Que o signatário é uma entidade final e não um prestador de serviços de certificação, e que não utilizará a chave privada correspondente à chave pública listada no certificado para assinar qualquer certificado (ou qualquer outro formato de chave pública certificada), ou Lista de Revogação de Certificados, nem título de prestador de serviços de certificação ou em qualquer outro caso.

4.5.2. Uso pelo assinante

4.5.2.1. Obrigações do assinante do certificado

A UANATACA obriga contratualmente o assinante a:

- Fornecer à Autoridade Certificadora informações completas e adequadas, de acordo com os requisitos desta Declaração de Práticas de Certificação, especialmente no que diz respeito ao procedimento de registro.
- Expresse seu consentimento antes da emissão e entrega de um certificado.
- Use o certificado de acordo com as disposições da seção 1.4.
- Informar a UANATACA, as Autoridades de Registo e qualquer pessoa em quem o assinante acredite poder confiar no certificado, sem atrasos injustificáveis:
    - A perda, roubo ou potencial comprometimento de sua chave privada.
    - Perda de controle sobre sua chave privada, devido ao comprometimento dos dados de ativação (por exemplo, código PIN) ou por qualquer outro motivo.
    - Imprecisões ou alterações no conteúdo do certificado que o assinante conhece ou poderia conhecer.
    - A perda, alteração, uso não autorizado, roubo ou comprometimento, quando aplicável, do cartão.
- Transferir às pessoas singulares identificadas no certificado o cumprimento das suas obrigações específicas e estabelecer mecanismos que garantam o seu efetivo cumprimento.
- Não monitorar, manipular ou realizar atos de engenharia reversa na implementação técnica dos serviços de certificação da UANATACA, sem autorização prévia por escrito.

- Não comprometa a segurança dos serviços de certificação do fornecedor de serviços de certificação UANATACA.

4.5.2.2. Responsabilidade civil do titular do certificado

A UANATACA obriga contratualmente o assinante a ser responsável por:

- Que todas as declarações feitas na aplicação estão corretas.
- Que todas as informações fornecidas pelo assinante contidas no certificado estão corretas.
- Que o certificado seja utilizado exclusivamente para usos legais e autorizados, de acordo com a Declaração de Práticas de Certificação.
- Que nenhuma pessoa não autorizada jamais teve acesso à chave privada do certificado e que você é o único responsável por quaisquer danos causados pela sua falha em proteger a chave privada.
- Que o assinante é uma entidade final e não um prestador de serviços de certificação, e que não utilizará a chave privada correspondente à chave pública listada no certificado para assinar qualquer certificado (ou qualquer outro formato de chave pública certificada), ou Lista de Revogação de Certificados, nem título de prestador de serviços de certificação ou em qualquer outro caso.

4.5.3. Uso por terceiros que confiam nos certificados

4.5.3.1. Obrigações do terceiro que confia nos certificados

A UANATACA informa ao terceiro que depende de certificados que deverá assumir as seguintes obrigações:

- Procure aconselhamento independente sobre se o certificado é apropriado para o uso pretendido.
- Verificar a validade, suspensão ou revogação dos certificados emitidos, para os quais serão utilizadas informações sobre o estado dos certificados.
- Verifique todos os certificados na hierarquia de certificados antes de confiar na assinatura digital ou em qualquer um dos certificados na hierarquia.

- Reconhecer que as assinaturas eletrónicas verificadas produzidas num dispositivo de criação de assinatura qualificada (DCCF) são legalmente consideradas assinaturas eletrónicas qualificadas; ou seja, equivalente a assinaturas manuscritas, bem como o certificado permite a criação de outros tipos de assinaturas eletrônicas e mecanismos de criptografia.
- Tenha em mente quaisquer limitações ao uso do certificado, independentemente de se encontrarem no próprio certificado ou no contrato do terceiro que confia no certificado.
- Tenha em mente quaisquer cuidados estabelecidos em contrato ou outro instrumento, independentemente de sua natureza jurídica.
- Não monitorar, manipular ou realizar atos de engenharia reversa na implementação técnica dos serviços de certificação da UANATACA, sem autorização prévia por escrito.
- Não comprometa a segurança dos serviços de certificação UANATACA.

4.5.3.2. Responsabilidade civil do terceiro que depende de certidões

A UANATACA informa aos terceiros que dependem de certificados que deverão assumir as seguintes responsabilidades:

- Que você tenha informações suficientes para tomar uma decisão informada sobre confiar ou não no certificado.
- Quem é o único responsável por confiar ou não nas informações contidas no certificado.
- Que você será o único responsável caso não cumpra suas obrigações como terceiro que depende do certificado.

4.6. Renovação de certificado

A renovação de certificados exige a renovação de chaves, pelo que deverá ser seguido o disposto na secção 4.7.

4.7. Renovação de chaves e certificados

4.7.1. Causas para renovação de chaves e certificados

Os certificados atuais podem ser renovados através de procedimento de candidatura específico e simplificado, de forma a manter a continuidade do serviço de certificação.

São consideradas pelo menos duas possibilidades para a renovação de certificados:

- Processo de renovação, que será realizado da mesma forma que a emissão de um novo certificado.
- Processo de renovação online (via internet), detalhado a seguir.

4.7.2. Procedimento de renovação de certificado online

4.7.2.1. Circunstâncias para renovação online

A renovação online do certificado só poderá ser efetuada se estiverem reunidas as seguintes condições:

- A Autoridade de Registo e/ou UANATACA dispõe do serviço de renovação online.
- O certificado com o qual é assinada a renovação está atual, ou seja, não expirou, foi revogado ou suspenso.
- Que não tenham se passado mais de 5 anos desde o último credenciamento de sua identidade perante um operador de identificação para obtenção de um certificado.

4.7.2.2. Quem pode solicitar a renovação online de um certificado

Qualquer signatário poderá solicitar a renovação online do seu certificado caso se verifiquem as circunstâncias descritas no ponto anterior.

O signatário poderá formalizar sua solicitação acessando o serviço online de renovação de certificados no site da UANATACA.

4.7.2.3. Aprovação ou rejeição do pedido

Se os dados forem verificados corretamente, a UANATACA aprovará o pedido de renovação do certificado e procederá à sua emissão e entrega.

A UANATACA notifica o requerente da aprovação ou indeferimento do pedido.

4.7.2.4. Processando solicitações de renovação on-line

A solicitação de renovação do certificado será feita de acordo com o seguinte:

- Quando o certificado digital de um usuário está prestes a expirar, a UANATACA poderá enviar uma ou mais notificações distribuídas ao longo do tempo, convidando-o a renová-lo.
- O signatário conectar-se-á ao serviço de renovação no site da UANATACA e procederá ao pedido de renovação.
- O Operador de Registro verificará se as informações utilizadas para verificar a identidade e os demais dados do usuário identificado no certificado ainda são válidos.
- Caso alguma informação do usuário identificada no certificado tenha mudado, a nova informação é devidamente registrada e uma identificação completa é produzida, de acordo com a seção 3.2.
- O signatário assinará a renovação do seu certificado válido.
- O novo par de chaves será gerado e o certificado será gerado e importado, respeitando as seguintes condições:
    - Protege a confidencialidade e integridade dos dados cadastrais disponíveis para você.
    - Utilizar sistemas e produtos confiáveis, protegidos contra qualquer alteração e que garantam a segurança técnica e, se for o caso, criptográfica dos processos de certificação que suportam.
    - Gera o par de chaves, usando um procedimento de geração de certificado vinculado de forma segura ao procedimento de geração de chaves.
    - Ele emprega um procedimento de geração de certificado que vincula de forma segura o certificado às informações de registro, incluindo a chave pública certificada.

- Garante que o certificado é emitido por sistemas que utilizam proteção antifalsificação e que garantem a confidencialidade das chaves durante o processo de geração de chaves.
- Indica a data e hora em que um certificado foi emitido.
- Garante o controle exclusivo do usuário sobre suas próprias chaves, não podendo a própria UANATACA ou suas Autoridades de Registro deduzi-las ou utilizá-las.

4.7.2.5. Notificação da emissão do certificado renovado

A UANATACA notifica a emissão do certificado ao titular e à pessoa singular identificada no certificado.

4.7.2.6. Conduta que constitui aceitação do certificado renovado

O certificado será considerado aceito mediante assinatura eletrônica da renovação.

4.7.2.7. Publicação do certificado renovado

A UANATACA publica o certificado renovado no Depositário referido no ponto 2.1, com os respetivos controlos de segurança.

4.7.2.8. Notificação do problema a terceiros

A UANATACA não notifica nenhuma emissão de certificados a terceiros, exceto nos casos abaixo indicados:

Relativamente aos certificados de Representante qualificado, a UANATACA assinou um contrato com o Colégio de Registos Imobiliários e Comerciais de Espanha, doravante CORPME, ao abrigo do qual a CORPME oferece a recepção de informação relativa aos registos imobiliários e comerciais à UANATACA, devendo a UANATACA notificar a CORPME de a emissão de certificado representativo de administrador único ou co-administrador, bem como a revogação do referido certificado.

Relativamente aos Certificados de Selo Electrónico qualificados para PSD2, onde a UANATACA notificará a Autoridade Nacional Competente da informação relativa ao certificado emitido de acordo com o disposto no regulamento de referência, desde que tenha informado à UANATACA um endereço de correio electrónico onde você pode direcionar essas notificações.

4.8. Modificação do certificado

A modificação dos certificados, exceto a modificação da chave pública certificada, que é considerada renovação, será tratada como uma nova emissão do certificado, aplicando-se o descrito nas seções 4.1, 4.2, 4.3e 4.4.

4.9. Revogação, suspensão ou reativação de certificados

A revogação de um certificado implica a perda definitiva da validade do mesmo e é irreversível.

A suspensão (ou revogação temporária) de um certificado implica a perda temporária da validade do certificado, sendo reversível. Apenas os certificados finais da entidade podem ser suspensos.

Reativar um certificado significa alterá-lo do status suspenso para o status ativo.

4.9.1. Causas para revogação de certificado

A UANATACA revoga um certificado quando ocorre qualquer uma das seguintes causas:

1) Circunstâncias que afetam as informações contidas no certificado:
   a) Modificação de qualquer um dos dados contidos no certificado, após a correspondente emissão do certificado que inclui as modificações.
   b) Descoberta de que algum dado contido na solicitação de certificado está incorreto.
   c) Descoberta de que algum dos dados contidos no certificado está incorreto.
   d) Alteração posterior das circunstâncias verificadas para a emissão do certificado, tais como as relacionadas com o cargo ou poderes.

2) Circunstâncias que afetam a segurança da chave ou certificado:
   a) Comprometimento da chave privada, infraestrutura ou sistemas do prestador de serviços confiável que emitiu o certificado, sempre que afete a confiabilidade dos certificados emitidos a partir daquele incidente.
   b) Violação, por parte da UANATACA, dos requisitos previstos nos procedimentos de gestão de certificados, estabelecidos nesta Declaração de Práticas de Certificação.
   c) Comprometimento ou suspeita de comprometimento da segurança da chave ou certificado emitido.
   d) Acesso ou utilização não autorizada, por terceiro, da chave privada correspondente à chave pública contida no certificado.
   e) Utilização irregular do certificado pela pessoa singular nele identificada, ou falta de diligência na guarda da chave privada.
   f) Utilização de dispositivos qualificados de criação de assinaturas que não cumpram os padrões mínimos de segurança necessários para garantir a segurança do certificado ou das suas chaves privadas.

3) Circunstâncias que afetam o assinante ou a pessoa singular identificada no certificado:
   a) Cessação da relação jurídica de prestação de serviços entre a UANATACA e o assinante.
   b) Modificação ou extinção da relação jurídica subjacente ou da causa que motivou a emissão do certificado à pessoa singular nele identificada.
   c) Violação pelo requerente do certificado dos requisitos pré-estabelecidos para a solicitação do certificado.
   d) Violação, por parte do assinante ou da pessoa identificada no certificado, das suas obrigações, responsabilidades e garantias, estabelecidas no documento legal correspondente, bem como nesta Declaração de Práticas de Certificação.
   e) A incapacidade repentina ou morte do titular da chave.

f) A extinção da pessoa colectiva subscritora do certificado, bem como o fim da autorização do subscritor ao titular da chave ou a cessação da relação entre o subscritor e a pessoa identificada no certificado.

g) Solicitação do assinante para revogação de certificado, de acordo com o disposto na seção 3.4.

4) Outras circunstâncias:

a) A extinção do serviço de certificação da Autoridade Certificadora UANATACA, a menos que, de acordo com o seu plano de extinção, a gestão dos certificados seja transferida para outro Prestador de Serviços de Confiança.

b) Resolução judicial ou administrativa que o ordene.

c) A utilização do certificado que é prejudicial e continuada para UANATACA. Neste caso, um uso é considerado prejudicial com base nos seguintes critérios:

- A natureza e o número de reclamações recebidas.
- A identidade das entidades que apresentam as reclamações.
- A legislação relevante em vigor em todos os momentos.
- A resposta do assinante ou da pessoa identificada no certificado às reclamações recebidas.

4.9.2. Causas para suspensão de um certificado

Os certificados UANATACA poderão ser suspensos pelos seguintes motivos:

- Quando solicitado pelo titular ou pela pessoa singular identificada no certificado.
- Resolução judicial ou administrativa ordenando a suspensão.
- Caso se suspeite que o dispositivo qualificado de criação de assinatura utilizado não cumpre os padrões mínimos de segurança necessários para garantir a segurança do certificado ou das suas chaves privadas.
- Quando a documentação exigida no pedido de revogação for suficiente, mas o assinante ou a pessoa singular identificada no certificado não puder ser razoavelmente identificado.
- Se houver suspeita de comprometimento de uma chave, até que seja confirmado. Neste caso, a UANATACA deve garantir que o certificado não

seja suspenso por mais tempo do que o necessário para confirmar o seu compromisso.

4.9.3. Causas para reativar um certificado

Os certificados UANATACA podem ser reativados pelos seguintes motivos:

- Quando o certificado está em estado suspenso.
- Quando solicitado pelo titular ou pela pessoa singular identificada no certificado.

4.9.4. Quem pode solicitar revogação, suspensão ou reativação

Você pode solicitar a revogação, suspensão ou reativação de um certificado:

- A pessoa identificada no certificado, ver signatário.
- O assinante do certificado através de seu representante legal ou voluntário ou terceiro autorizado, autoridade judicial ou administrativa através da resolução correspondente.
- No caso de Certificados de Selo Eletrónico qualificados para PSD2, as Autoridades Nacionais Competentes poderão solicitar a revogação.

4.9.5. Procedimentos para solicitar revogação, suspensão ou reativação

A entidade que requerer a revogação, suspensão ou reativação de um certificado pode solicitá-lo diretamente à UANATACA ou à Autoridade de Registo do Assinante ou fazê-lo ela própria através do serviço online disponível no site da UANATACA. O pedido de revogação, suspensão ou reativação deverá incluir as seguintes informações:

- Data do pedido de revogação, suspensão ou reativação.
- Identidade do assinante.
- Nome e cargo da pessoa que solicita a revogação, suspensão ou reativação.
- Informações de contato da pessoa que solicita a revogação, suspensão ou reativação.
- Motivo detalhado da solicitação de revogação.

A solicitação deverá ser autenticada, pela UANATACA, de acordo com os requisitos estabelecidos na seção 3.4desta política, antes de proceder à revogação, suspensão ou reativação.

O serviço de revogação, suspensão ou reativação encontra-se no site da UANATACA no endereço: https://web.uanataca.com/

Caso o destinatário de um pedido de revogação, suspensão ou reativação por parte de uma pessoa singular identificada no certificado seja a entidade subscritora, uma vez autenticado o pedido, deverá ser enviado um pedido nesse sentido à UANATACA.

O pedido de revogação, suspensão ou reativação será processado mediante receção, sendo o titular e, quando aplicável, a pessoa singular identificada no certificado, informado sobre a alteração do estado do certificado.

Tanto o serviço de gestão de revogação, suspensão ou reactivação como o serviço de consulta são considerados serviços críticos e estão portanto incluídos no Plano de Contingência e no plano de continuidade de negócio da UANATACA.

4.9.6. Prazo temporário para solicitação de revogação, suspensão ou reativação

Os pedidos de revogação, suspensão ou reativação serão enviados imediatamente assim que forem conhecidos.

4.9.7. Prazo temporário para processamento do pedido de revogação, suspensão ou reativação

Os pedidos de revogação, suspensão ou reativação efetuados através do serviço online serão processados imediatamente.

Se for realizado por meio de operador de registro, será executado dentro do horário normal de funcionamento da UANATACA. ou, se for caso disso, a Autoridade de Registo. Em qualquer caso, os pedidos serão processados num prazo não superior a 24 horas a partir da recepção.

4.9.8. Obrigação de consultar informações sobre revogação ou suspensão de certificados

Terceiros devem verificar o status dos certificados nos quais desejam confiar.

Um método pelo qual o status dos certificados pode ser verificado é consultando a Lista de Revogação de Certificados mais recente emitida pela Autoridade Certificadora UANATACA.

As Listas de Revogação de Certificados são publicadas no Repositório da Autoridade de Certificação, bem como nos seguintes endereços da web, indicados nos certificados:

- UANTACA CA1 2016
  - http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl
  - http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl

- UANTACA CA2 2016
  - http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl
  - http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl

- UANTACA CA1 2021
  - http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
  - http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl

- UANTACA CA2 2021
  - http://crl1.uanataca.com/public/pki/crl/2021CA2sub.crl
  - http://crl2.uanataca.com/public/pki/crl/2021CA2sub.crl

O status de validade dos certificados também pode ser verificado usando o protocolo OCSP.

- http://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

4.9.9. Frequência de emissão de listas de revogação de certificados (CLRs)

A UANATACA emite um LRC pelo menos a cada 24 horas.

O LRC indica o horário programado para a emissão de um novo LRC, embora um LRC possa ser emitido antes do prazo indicado no LRC anterior, para refletir as revogações.

O LRC mantém obrigatoriamente o certificado revogado ou suspenso até que expire.

4.9.10. Período máximo de publicação para LRCs

Os LRCs são publicados no Depositário num prazo razoável imediatamente após a sua geração, que em nenhum caso excede alguns minutos.

4.9.11. Disponibilidade de serviços online de verificação de status de certificado

Alternativamente, terceiros que dependem de certificados podem consultar o Repositório de Certificados UANATACA, que está disponível 24 horas por dia, 7 dias por semana no site:

- https://www.uanataca. com /public/pki/crtlist

Para verificar a última CRL emitida em cada CA você deve baixar:

- *Autoridade de certificação raiz (UANATACA ROOT 2016):*
  - http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl
  - http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl

- *Autoridade Certificadora Subordinada - UANATACA CA1 2016*
  - http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl
  - http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl

- *Autoridade Certificadora Subordinada - UANATACA CA2 2016*
  - http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl
  - http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl

- *Autoridade Certificadora Subordinada - UANATACA CA1 2021*
  - http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
  - http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl

- *Autoridade Certificadora Subordinada - UANATACA CA2 2021*
  - http://crl1.uanataca.com/public/pki/crl/2021CA2sub.crl
  - http://crl2.uanataca.com/public/pki/crl/2021CA2sub.crl

Em caso de falha dos sistemas de verificação do estado dos certificados por motivos alheios à vontade da UANATACA, esta deverá envidar todos os esforços para garantir que este serviço permaneça inativo pelo mínimo de tempo possível, que não poderá exceder um dia.

A UANATACA fornece informações a terceiros que dependem de certificados sobre o funcionamento do serviço de informações sobre o status dos certificados.

4.9.12. Obrigação de consultar os serviços de verificação do estado dos certificados

É obrigatório verificar o status dos certificados antes de confiar neles.

4.9.13. Requisitos especiais em caso de comprometimento da chave privada

O comprometimento da chave privada da UANATACA é notificado a todos os participantes nos serviços de certificação, na medida do possível, através da publicação desse facto no site da UANATACA, bem como, se for considerado necessário, noutros meios de comunicação, mesmo em papel.

4.9.14. Período máximo de um certificado digital em estado suspenso

O prazo máximo de permanência do certificado digital em situação suspensa será de 90 (noventa) dias contados da solicitação de suspensão pelo ASSINANTE ou SIGNATÁRIO. Uma vez ultrapassado o prazo máximo sem que seja reativado, a UANATACA procederá à sua revogação direta.

Se durante o período de suspensão o certificado digital expirar ou for solicitada a sua revogação, a sua validade terminará nas mesmas condições de um certificado digital em vigor.

Sem prejuízo do anterior, o prazo máximo de noventa (90) dias poderá ser alterado em função de procedimento de investigação da UANATACA ou de processos judiciais ou administrativos em curso. Nestes casos, o certificado digital ficará suspenso pelo prazo exigido e, após esse prazo, será revogado definitivamente. Em nenhum caso o período de suspensão do certificado digital poderá ultrapassar o seu prazo de validade.

4.10. Rescisão de Assinatura

Decorrido o período de validade do certificado, a assinatura do serviço terminará.

Excecionalmente, o assinante poderá manter o serviço atual, solicitando a renovação do certificado, com a antecedência determinada nesta Declaração de Práticas de Certificação.

A UANATACA poderá emitir novo certificado de ofício, desde que os assinantes mantenham essa qualidade.

4.11. Depósito e recuperação de chaves

4.11.1. Principais políticas e práticas de depósito e recuperação

A UANATACA não fornece serviços de depósito e recuperação de chaves.

4.11.2. Política e práticas de encapsulamento e recuperação de chave de sessão

Nenhuma estipulação.

5. Segurança física, gerenciamento e controles de operações

5.1. Controles de segurança física

A UANATACA estabeleceu controles de segurança física e ambiental para proteger os recursos das instalações onde os sistemas estão localizados, os próprios sistemas e os equipamentos utilizados nas operações para fornecer serviços eletrônicos confiáveis.

Especificamente, a política de segurança da UANATACA aplicável aos serviços eletrónicos confiáveis estabelece requisitos sobre o seguinte:

- Controles de acesso físico.
- Proteção contra desastres naturais.
- Medidas de proteção contra incêndio.
- Falha nos sistemas de apoio (energia electrónica, telecomunicações, etc.)
- Colapso da estrutura.
- Inundações.
- Proteção anti-roubo.
- Saída não autorizada de equipamentos, informações, suportes e aplicações relacionadas a componentes utilizados nos serviços do prestador de serviços de certificação.

Estas medidas são aplicáveis às instalações a partir das quais são prestados serviços eletrónicos confiáveis, nos seus ambientes de produção e de contingência, os quais são auditados periodicamente de acordo com a regulamentação aplicável e as políticas próprias da UANATACA destinadas a esse fim.

As instalações possuem sistemas de manutenção preventiva e corretiva com atendimento 24 horas por dia, 365 dias por ano com atendimento em até 24 horas após aviso prévio.

5.1.1. Localização e construção de instalações

A proteção física é alcançada através da criação de perímetros de segurança claramente definidos em torno dos serviços. A qualidade e solidez dos materiais de construção das instalações garantem níveis adequados de proteção contra intrusões por força bruta e localizadas numa zona de baixo risco de desastres e permitem acesso rápido.

A sala onde são realizadas as operações criptográficas do Centro de Processamento de Dados possui redundância em sua infraestrutura, além de diversas fontes alternativas de energia elétrica e refrigeração em caso de emergência.

A UANATACA possui instalações que protegem fisicamente a prestação de serviços de gerenciamento de aprovação e revogação de pedidos de certificados contra comprometimento causado por acesso não autorizado a sistemas ou dados, bem como sua divulgação.

5.1.2. Acesso físico

A UANATACA possui três níveis de segurança física (Entrada do Edifício onde está localizado o CPD, acesso à sala do CPD e acesso ao Rack) para proteção do serviço de geração de certificados, que deve ser acessado dos níveis inferiores para os níveis superiores .

O acesso físico às instalações da UANATACA onde são realizados os processos de certificação é limitado e protegido através de uma combinação de medidas físicas e processuais. Então:

- É limitado a pessoal expressamente autorizado, com identificação no momento do acesso e inscrição, incluindo filmagens em circuito fechado de televisão e seu arquivo.
- O acesso às salas é feito através de leitores de cartões de identificação e gerido por um sistema informático que mantém um registo automático de entradas e saídas.
- Para acessar o rack onde estão localizados os processos criptográficos, é necessária autorização prévia da UANATACA aos administradores do serviço de hospedagem que possuem a chave para abertura da gaiola.

5.1.3. Eletricidade e ar condicionado

As instalações da UANATACA dispõem de equipamentos estabilizadores de corrente e sistema duplicado de alimentação de equipamentos com grupo gerador.

As salas que abrigam equipamentos de informática possuem sistemas de controle de temperatura com equipamentos de ar condicionado.

5.1.4. Exposição à água

As instalações estão localizadas em uma área de baixo risco de inundação.

As salas onde estão alojados os equipamentos informáticos dispõem de sistema de detecção de humidade.

5.1.5. Prevenção e proteção contra incêndio

As instalações e ativos da UANATACA dispõem de sistemas automáticos de detecção e extinção de incêndios.

5.1.6. Armazenamento de mídia

Somente pessoal autorizado tem acesso à mídia de armazenamento.

O mais alto nível de informação de classificação é armazenado num cofre fora das instalações do Centro de Processamento de Dados.

5.1.7. Tratamento de esgoto

A eliminação de suportes, tanto em papel como magnéticos, é efectuada através de mecanismos que garantem a impossibilidade de recuperação da informação.

No caso das mídias magnéticas, elas são descartadas e, nesse caso, são destruídas fisicamente, ou são reutilizadas após um processo permanente de apagamento ou formatação. No caso de documentação em papel, através de trituradoras ou em caixotes dispostos para o efeito para posterior destruição, sob controlo.

5.1.8. Backup externo

A UANATACA utiliza um armazém externo seguro para a guarda de documentos, dispositivos magnéticos e eletrônicos independentes do centro de operações.

5.2. Controles de procedimento

A UANATACA garante o funcionamento seguro dos seus sistemas, pelo que estabeleceu e implementou procedimentos para as funções que afectam a prestação dos seus serviços.

O pessoal ao serviço da UANATACA executa os procedimentos administrativos e de gestão de acordo com a política de segurança.

5.2.1. Recursos confiáveis

A UANATACA identificou, de acordo com a sua política de segurança, as seguintes funções ou papéis com estatuto de confiança:

- **Auditor Interno:** Responsável pelo cumprimento dos procedimentos operacionais. Trata-se de uma pessoa externa ao departamento de Sistemas de Informação. As tarefas do Auditor Interno são incompatíveis no tempo com as tarefas de Certificação e incompatíveis com os Sistemas. Estas funções estarão subordinadas ao gestor de operações, reportando-se tanto a este como à direção técnica.
- **Administrador de Sistemas** : Responsável pelo correto funcionamento do hardware e software de suporte à plataforma de certificação.
- **Administrador da CA** : Responsável pelas ações a serem executadas com o material criptográfico, ou pelo desempenho de qualquer função que envolva

a ativação das chaves privadas das autoridades certificadoras descritas neste documento, ou qualquer um de seus elementos.

- **Operador CA:** Responsável em conjunto com o Administrador da CA pela guarda do material de ativação da chave criptográfica, sendo também responsável pelas operações de backup e manutenção da CA.
- **Operador de Registro:** Pessoa responsável por aprovar as solicitações de certificação feitas pelo assinante e emitir certificados digitais.
- **Oficial de Revogação:** Pessoa responsável por efetuar alterações no status de um certificado, principalmente procedendo à sua suspensão e revogação.
- **Gerente de Segurança** : Responsável por coordenar, controlar e fazer cumprir as medidas de segurança definidas pelas políticas de segurança da UANATACA. Você deve ser responsável pelos aspectos relacionados à segurança da informação: lógicos, físicos, de redes, organizacionais, etc.

As pessoas que ocupam os cargos acima estão sujeitas a procedimentos específicos de investigação e controle. Adicionalmente, a UANATACA implementa nas suas políticas critérios de segregação de funções, como medida de prevenção de atividades fraudulentas.

5.2.2. Número de pessoas por tarefa

A UANATACA garante pelo menos duas pessoas para realizar as tarefas relacionadas com a geração, recuperação e backup da chave privada das Autoridades Certificadoras . O mesmo critério se aplica à execução de tarefas de emissão e ativação de certificados e chaves privadas das Autoridades Certificadoras, e em geral qualquer manipulação do dispositivo de custódia das chaves da Autoridade Certificadora raiz e intermediária.

5.2.3. Identificação e autenticação para cada função

As pessoas designadas para cada função são identificadas pelo auditor interno que garantirá que cada pessoa execute as operações para as quais está designada.

Cada pessoa controla apenas os ativos necessários para a sua função, garantindo assim que nenhuma pessoa acesse recursos não atribuídos.

O acesso aos recursos é realizado dependendo do ativo através de nome de usuário/senha, certificado digital, cartão de acesso físico e/ou chaves.

5.2.4. Funções que exigem separação de funções

As seguintes tarefas são realizadas por pelo menos duas pessoas:

- As tarefas do papel de Auditor serão incompatíveis com a operação e administração de sistemas e, em geral, aqueles dedicados à prestação direta de serviços eletrónicos confiáveis.
- A emissão e revogação de certificados serão tarefas incompatíveis com a Administração e operação dos sistemas.
- A administração e operação dos sistemas e das ACs serão incompatíveis entre si.

5.2.5. Sistema de gerenciamento de PKI

O sistema PKI é composto pelos seguintes módulos:

- Componente/módulo de gerenciamento da Autoridade de Certificação Subordinada.
- Componente/módulo de gerenciamento da Autoridade de Registro.
- Componente/módulo de gerenciamento de solicitações.
- Componente/módulo de gerenciamento de chaves (HSM).
- Componente/módulo de banco de dados.
- Componente/módulo de gerenciamento de CRL.
- Componente/módulo de gerenciamento de autoridade de validação (serviços OCSP).

5.3. Controles de pessoal

5.3.1. Histórico, qualificações, experiência e requisitos de licenciamento

Todo o pessoal está qualificado e/ou foi devidamente instruído para realizar as operações que lhe são atribuídas.

O pessoal que ocupa cargos de confiança não tem interesses pessoais que entrem em conflito com o desenvolvimento da função que lhes é confiada.

A UANATACA garante que o pessoal de registo seja fiável para realizar as tarefas de registo. O Administrador de Registro recebe treinamento para executar as tarefas de validação de solicitações.

Em geral, a UANATACA afastará um funcionário das suas funções de confiança quando tiver conhecimento da existência de conflitos de interesses e/ou da prática de um ato criminoso que possa afetar o desempenho das suas funções.

A UANATACA não atribuirá a um local de confiança ou de gestão uma pessoa que não seja idónea para o cargo, especialmente por falta que afete a sua idoneidade para o cargo. Por este motivo, é previamente realizada uma investigação, **na medida do permitido pela legislação aplicável** , relativamente aos seguintes aspectos:

- Estudos, incluindo supostas qualificações.
- Empregos anteriores, até cinco anos, incluindo referências profissionais.
- Referências profissionais.

Em qualquer caso, as Autoridades de Registro poderão estabelecer diversos processos de verificação de antecedentes, sempre preservando as políticas da UANATACA, sendo responsáveis pelas ações das pessoas que autorizam em suas operações.

5.3.2. Procedimentos de investigação histórica

A UANATACA, antes de contratar uma pessoa ou de lhe dar acesso ao trabalho, realiza as seguintes verificações:

- Referências a obras dos últimos anos
- Referências profissionais
- Estudos, incluindo supostas qualificações.

UANATACA obtém o consentimento inequívoco da parte afetada para a referida investigação prévia, e processa e protege todos os seus dados pessoais em conformidade com a normativa vigente sobre proteção de dados pessoais, refletida no Regulamento Europeu nº2016/679 Proteção Geral de Dados e em geral quaisquer regulamentos nacionais que são aplicáveis.

Todas as verificações são realizadas na medida permitida pela legislação vigente aplicável. Os motivos que podem levar à rejeição do candidato a um cargo confiável são os seguintes:

- Falsidades na candidatura de emprego, feita pelo candidato.
- Referências profissionais muito negativas ou pouco confiáveis em relação ao candidato.

5.3.3. Requisitos de treinamento

A UANATACA forma pessoal em cargos de confiança e de gestão, até que obtenham as qualificações necessárias, mantendo um arquivo dessa formação.

Os programas de treinamento são revisados periodicamente e atualizados para melhor e melhorados periodicamente.

A formação inclui, pelo menos, os seguintes conteúdos:

- Princípios e mecanismos de segurança da hierarquia de certificação, bem como o ambiente do usuário da pessoa a ser treinada.
- Tarefas que a pessoa deve realizar.
- Políticas e procedimentos de segurança da UANATACA. Uso e operação de máquinas e aplicações instaladas.
- Gestão e processamento de incidentes e compromissos de segurança.
- Continuidade de negócios e procedimentos de emergência.
- Procedimento de gestão e segurança em relação ao tratamento de dados pessoais.

5.3.4. Requisitos e frequência de atualizações de treinamento

A UANATACA atualiza a formação do pessoal de acordo com as necessidades e com frequência suficiente para cumprir as suas funções de forma competente e satisfatória, especialmente quando são feitas modificações substanciais nas tarefas de certificação.

5.3.5. Sequência e frequência da rotação de cargos

Não aplicável.

5.3.6. Sanções por ações não autorizadas

A UANATACA dispõe de um sistema sancionatório para determinar as responsabilidades derivadas de ações não autorizadas, adequado à legislação trabalhista aplicável.

As ações disciplinares incluem suspensão, afastamento de funções e até demissão do responsável pela ação danosa, proporcional à gravidade da ação não autorizada.

5.3.7. Requisitos de contratação profissional

Os funcionários contratados para desempenhar tarefas confiáveis assinam previamente as cláusulas de confidencialidade e requisitos operacionais utilizados pela UANATACA. Qualquer ação que comprometa a segurança dos processos aceitos poderá, uma vez avaliada, levar à rescisão do contrato de trabalho.

No caso de todos ou parte dos serviços de certificação serem operados por terceiros, os controles e disposições feitas nesta seção, ou em outras partes do A Declaração de Práticas de Certificação será aplicada e cumprida pelo terceiro que executa as funções de operação dos serviços de certificação, porém a Autoridade Certificadora será responsável em todos os casos pela efetiva execução. Estes aspectos estão especificados no instrumento jurídico utilizado para acordar a prestação de serviços de certificação por um terceiro que não a UANATACA.

5.3.8. Fornecimento de documentação aos funcionários

O prestador de serviços de certificação fornecerá em todos os momentos a documentação estritamente exigida pelo seu pessoal, a fim de realizar o seu trabalho de forma competente e satisfatória.

5.4. Procedimentos de auditoria de segurança

5.4.1. Tipos de eventos registrados

A UANATACA produz e mantém registros de pelo menos os seguintes eventos relacionados à segurança da entidade:

- Sistema ligado e desligado.
- Tentativas de criar, excluir, definir senhas ou alterar privilégios.
- Tentativas de login e logout.
- Tentativas de obter acesso não autorizado ao sistema AC através da rede.
- Tentativas de acesso não autorizado ao sistema de arquivos.
- Acesso físico aos logs.
- Mudanças na configuração e manutenção do sistema.
- Registros de aplicações AC.
- Ligar e desligar o aplicativo AC.
- Alterações nos detalhes do AC e/ou suas chaves.
- Mudanças na criação de políticas de certificados.
- Geração de chaves próprias.
- Criação e revogação de certificados.
- Registros de destruição de mídia contendo chaves, dados de ativação.
- Eventos relacionados ao ciclo de vida do módulo criptográfico, como sua recepção, utilização e desinstalação.
- A cerimônia de geração de chaves e bancos de dados de gerenciamento de chaves.
- Registros de acesso físico.
- Mudanças de manutenção e configuração do sistema.
- Mudanças de pessoal.
- Relatórios de compromissos e discrepâncias.

- Registos de destruição de material contendo informações chave, dados de ativação ou informações pessoais do assinante, no caso de certificados individuais, ou da pessoa singular identificada no certificado, no caso de certificados de organização.
- Posse de dados de ativação, para operações com a chave privada da Autoridade Certificadora.
- Relatórios completos de tentativas de intrusão física nas infraestruturas que suportam a emissão e gestão de certificados.

As entradas do registro incluem os seguintes itens:

- Data e hora de entrada.
- Número de série ou sequência do lançamento, nos registros automáticos.
- Identidade da entidade que insere o registo.
- Tipo de entrada.

5.4.2. Frequência de processamento do log de auditoria

A UANATACA revisa seus logs quando ocorre um alerta do sistema devido à existência de um incidente.

O processamento de logs de auditoria consiste em uma revisão dos logs que inclui a verificação de que os logs não foram adulterados, uma breve inspeção de todas as entradas de log e uma investigação mais aprofundada de quaisquer alertas ou irregularidades nos logs. As ações tomadas após a revisão de auditoria são documentadas.

A UANATACA mantém um sistema que garante:

- Espaço suficiente para armazenamento de logs.
- Que os arquivos de log não sejam reescritos.
- Que as informações salvas incluam pelo menos: tipo de evento, data e hora, usuário que executa o evento e resultado da operação.
- Os arquivos de log serão salvos em arquivos estruturados que poderão ser incorporados a um banco de dados para posterior exploração.

5.4.3. Período de retenção do log de auditoria

A UANATACA armazena a informação de registo por um período entre 1 e 15 anos, dependendo do tipo de informação registada. Sem prejuízo do acima exposto, os registos de auditoria relativos à gestão do ciclo de vida dos certificados digitais serão conservados pelo período de 15 anos a contar da expiração do certificado ou do fim do serviço prestado.

5.4.4. Protegendo logs de auditoria

Os registros do sistema:

- Eles são protegidos contra manipulação assinando os arquivos que os contêm.
- Eles são armazenados em dispositivos à prova de fogo.
- A sua disponibilidade é protegida armazenando-o em instalações fora do centro onde se encontra o AC.

O acesso aos arquivos de log é reservado apenas para pessoas autorizadas. Da mesma forma, os dispositivos são sempre manuseados por pessoal autorizado.

Existe um procedimento interno que detalha os processos de gerenciamento de dispositivos que contêm dados de registro de auditoria.

5.4.5. Procedimentos de backup

A UANATACA dispõe de um procedimento de backup adequado para que, em caso de perda ou destruição dos ficheiros relevantes, as correspondentes cópias de segurança dos registos estejam disponíveis num curto espaço de tempo.

A UANATACA implementou um procedimento de backup seguro para logs de auditoria, fazendo uma cópia semanal de todos os logs em meio externo. Além disso, uma cópia é mantida em centro de custódia externo.

5.4.6. Localização do sistema de acumulação de logs de auditoria

As informações de auditoria do evento são coletadas internamente e de forma automatizada pelo sistema operacional, software de comunicação de rede e gerenciamento de certificados, além de dados gerados manualmente, que serão armazenados por pessoal devidamente autorizado. Tudo isso compõe o sistema de acumulação de registros de auditoria.

5.4.7. Notificação do evento de auditoria à causa do evento

Quando o sistema de log de auditoria registra um evento, não é necessário enviar uma notificação ao indivíduo, organização, dispositivo ou aplicativo que causou o evento.

5.4.8. Verificação de vulnerabilidade

A análise de vulnerabilidades é coberta pelos processos de auditoria da UANATACA.

As análises de vulnerabilidade devem ser executadas, revisadas e revisadas através do exame desses eventos monitorados. Estas análises deverão ser realizadas periodicamente de acordo com o procedimento interno estabelecido para o efeito.

Os dados de auditoria do sistema são armazenados para serem usados para investigar qualquer incidente e localizar vulnerabilidades.

5.5. Arquivos de informação

A UANATACA garante que toda a informação relativa aos certificados é conservada por um período de tempo adequado, conforme estabelecido na secção 5.5.2desta política.

5.5.1. Tipos de registros arquivados

Os seguintes documentos envolvidos no ciclo de vida do certificado são armazenados pela UANATACA (ou pelas entidades registadoras):

- Todos os dados de auditoria do sistema.
- Todos os dados relativos aos certificados, incluindo contratos com os signatários e dados relativos à sua identificação e localização
- Solicitações de emissão e revogação de certificados.
- Tipo de documento apresentado no pedido de certificado.
- Identidade da Entidade de Registo que aceita o pedido de certificado.
- Número de identificação exclusivo fornecido pelo documento acima.
- Todos os certificados emitidos ou publicados.
- CRLs emitidas ou registros do status dos certificados gerados.
- O histórico das chaves geradas.
- Comunicações entre os elementos da PKI.
- Políticas e Práticas de Certificação
- Todos os dados de auditoria identificados na seção 5.4
- Informações do pedido de certificação.
- Documentação fornecida para justificar solicitações de certificação.
- Informações sobre o ciclo de vida do certificado.

A UANATACA e/ou as Autoridades de Registro conforme o caso, serão responsáveis pelo correto arquivamento de todo este material.

5.5.2. Período de retenção de registros

A UANATACA arquiva os registros acima especificados por pelo menos 15 anos, ou pelo período estabelecido pela legislação vigente.

Em particular, os registros dos certificados revogados estarão acessíveis para consulta gratuita por pelo menos 15 anos ou pelo período estabelecido pela legislação vigente a partir da expiração do certificado ou do término do serviço prestado.

5.5.3. Proteção de arquivos

A UANATACA protege o arquivo para que somente pessoas devidamente autorizadas possam acessá-lo. O arquivo é protegido contra visualização, modificação, exclusão ou qualquer outra manipulação, armazenando-o em um sistema confiável.

A UANATACA garante a correta proteção dos arquivos, designando pessoal qualificado para o seu tratamento e armazenamento em instalações externas seguras.

5.5.4. Procedimentos de backup

A UANATACA dispõe de um centro de armazenamento externo para garantir a disponibilidade das cópias do arquivo eletrônico. Os documentos físicos são armazenados em locais seguros com acesso restrito apenas ao pessoal autorizado.

UANATACA faz, no mínimo, backups incrementais diários de todos os seus documentos eletrônicos e realiza backups completos semanalmente para casos de recuperação de dados.

Além disso, a UANATACA (ou as organizações que desempenham a função de registo) mantém uma cópia dos documentos em papel num local seguro diferente das instalações da própria Autoridade Certificadora.

5.5.5. Requisitos de carimbo de data e hora

Os registros são datados com fonte confiável via NTP.

Não é necessário que essas informações sejam assinadas digitalmente.

5.5.6. Localização do sistema de arquivos

A UANATACA dispõe de um sistema centralizado de recolha de informação sobre a actividade das equipas envolvidas no serviço de gestão de certificados.

5.5.7. Procedimentos para obtenção e verificação de informações de arquivos

A UANATACA possui um procedimento que descreve o processo para verificar se a informação arquivada está correta e acessível. A UANATACA fornece as informações e meios de verificação ao auditor.

5.6. Renovação da chave

Antes que o uso da chave privada da CA expire, uma alteração de chave será realizada. O AC antigo e sua chave privada só serão utilizados para assinatura de LCRs enquanto existirem certificados ativos emitidos pelo referido AC. Um novo AC será gerado com uma nova chave privada e um novo DN. A alteração das chaves de assinante é realizada através da realização de um novo processo de emissão.

Alternativamente, no caso de Autoridades Certificadoras subordinadas, poderá optar pela renovação do certificado com ou sem alteração das chaves, não sendo aplicável o procedimento acima descrito.

5.7. Principais compromissos e recuperação de desastres

5.7.1. Procedimentos de gerenciamento de incidentes e compromissos

A UANATACA desenvolveu políticas de segurança e continuidade de negócio que lhe permitem gerir e recuperar sistemas em caso de incidentes e comprometimento das suas operações, garantindo serviços críticos de revogação e publicação do estado dos certificados.

5.7.2. Corrupção de recursos, aplicativos ou dados

Quando ocorrer um evento de corrupção de recursos, aplicações ou dados, os procedimentos de gestão apropriados serão seguidos de acordo com as políticas de segurança e gestão de incidentes da UANATACA, que incluem escalonamento, investigação e resposta ao incidente. Se necessário, serão iniciados procedimentos de comprometimento de chaves ou recuperação de desastres da UANATACA.

5.7.3. Comprometimento da chave privada da entidade

Em caso de suspeita ou conhecimento do comprometimento da UANATACA, os principais procedimentos de comprometimento serão acionados de acordo com as políticas de segurança, gestão de incidentes e continuidade de negócios, permitindo a recuperação de sistemas críticos, se necessário em uma fonte de dados alternativa.

5.7.4. Continuidade dos negócios após um desastre

A UANATACA restaurará os serviços críticos (suspensão e revogação e publicação de informações sobre o status do certificado) de acordo com o incidente existente e o plano de continuidade de negócios, restaurando a operação normal dos serviços anteriores dentro de 24 horas após o desastre.

A UANATACA dispõe de um centro alternativo se necessário para a implementação dos sistemas de certificação descritos no plano de continuidade de negócios.

5.8. Rescisão do serviço

A UANATACA garante que as possíveis interrupções aos assinantes e terceiros sejam mínimas em consequência da cessação dos serviços do prestador de serviços de certificação. Neste sentido, a UANATACA garante a manutenção contínua dos registos definidos na secção 5.5.1, pelo tempo estabelecido na secção 5.5.2 desta Declaração de Práticas de Certificação.

Não obstante o acima exposto, se for o caso, a UANATACA executará todas as ações que sejam necessárias para transferir a um terceiro ou a um depósito notarial, as obrigações de manutenção dos registros especificados durante o período correspondente de acordo com esta Declaração de Práticas de Certificação ou a disposição legal correspondente. .

Antes de terminar os seus serviços, a UANATACA desenvolve um plano de terminação, com as seguintes disposições:

- Fornecer os fundos necessários, incluindo seguro de responsabilidade civil, para continuar a conclusão das atividades de revogação.
- Informará todos os Signatários/Assinantes, Terceiros em quem confiam e outras ACs com quem tenha acordos ou outros tipos de relações da cessação com um aviso mínimo de 6 meses.
- Revogará todas as autorizações às entidades subcontratadas para atuarem em nome da EC no procedimento de emissão de certificados.
- Transferirá suas obrigações relativas à manutenção de informações cadastrais e logs durante o período indicado aos assinantes e usuários.
- Isso destruirá ou desabilitará o uso das chaves privadas da CA.
- Manterá os certificados ativos e o sistema de verificação e revogação até a extinção de todos os certificados emitidos.
- Você executará as tarefas necessárias para transferir as obrigações de manutenção das informações de registro e dos arquivos de registro de eventos durante os respectivos períodos indicados para o assinante e terceiros que dependem de certificados.
- Notificará o Ministério da Energia, Turismo e Agenda Digital, com pelo menos 2 meses de antecedência, da cessação da sua atividade e do destino dos certificados, especificando se a gestão é transferida e para quem ou se a sua validade será extinta.

- Notificará também o Ministério da Energia, Turismo e Agenda Digital da abertura de qualquer processo de falência contra a UANATACA, bem como de qualquer outra circunstância relevante que possa impedir a continuação da atividade.

6. Controles técnicos de segurança

A UANATACA utiliza sistemas e produtos confiáveis, protegidos contra qualquer alteração e que garantem a segurança técnica e criptográfica dos processos de certificação que suportam.

6.1. Geração e instalação de par de chaves

6.1.1. Geração de par de chaves

O par de chaves das entidades certificadoras intermédias "UANATACA CA1 2016" e "UANATACA CA2 2016" são criados pela Autoridade Certificadora raiz "UANATACA ROOT 2016" de acordo com os procedimentos da cerimónia da UANATACA, dentro do perímetro de alta segurança destinado a esta tarefa.

As atividades realizadas durante a cerimônia de geração de chaves foram registradas, datadas e assinadas por todos os participantes da mesma, com a presença de um Auditor CISA. Esses registros são mantidos para fins de auditoria e monitoramento durante um período apropriado determinado pela UANATACA.

Dispositivos com certificações FIPS 140-2 nível 3 e Common Criteria EAL4+ são usados para gerar a chave para as entidades de certificação raiz e intermediárias.

RAIZ DE UANTACA 2016	4.096 bits	25 anos
UANTACA CA1 2016	4.096 bits	13 anos
- Certificados de entidade final	2.048 bits	Até 5 anos
UANTACA CA2 2016	4.096 bits	13 anos
- Certificados de Unidade de Carimbo de Tempo (TSU)	2.048 bits	Até 5 anos
UANTACA CA1 2021	4.096 bits	13 anos
Certificados de entidade final	2.048 bits	Até 5 anos
UANTACA CA2 2021	4.096 bits	13 anos
- Certificados de entidade final	2.048 bits	Até 5 anos

Os documentos Disclosure Text (PKI Disclosure Statement-PDS) de todos os perfis de certificados digitais indicados neste documento estão acessíveis no link http://www.uanataca.com/public/cps/

6.1.1.1. Geração de par de chaves do assinante

As chaves do signatário podem ser geradas por ele mesmo utilizando dispositivos de hardware e/ou software autorizados pela UANATACA.

Como regra geral, as chaves não geradas em um QSCD serão geradas pelo signatário. Não obstante o acima exposto, a UANATACA poderá gerar chaves fora de um QSCD para serem disponibilizadas ao signatário através de métodos seguros que garantam que apenas o signatário tenha acesso às mesmas.

As chaves são geradas usando o algoritmo de chave pública RSA, com comprimento mínimo de 2.048 bits.

6.1.2. Enviando a chave privada ao signatário

Nos certificados num dispositivo de criação de assinatura qualificado, a chave privada é gerada e armazenada devidamente protegida no referido dispositivo qualificado.

Para certificados de software, a chave privada é enviada da seguinte forma:

a) Se a chave privada do signatário for gerada e armazenada no sistema informático que este signatário utiliza ao solicitar o certificado, neste caso a chave privada não é enviada, pois é "autogerada", garantindo assim o controlo exclusivo da chave por o usuário.
b) Caso a chave privada do signatário seja gerada nos sistemas certificados da UANATACA, ela é disponibilizada ao signatário através de mecanismos e protocolos seguros, garantindo que apenas o signatário tenha acesso à mesma, garantindo o controle exclusivo da chave por parte do usuário signatário.

Em ambos os casos, a UANATACA não armazena, guarda, custodia nem tem a capacidade de deduzir a chave privada dos certificados de software.

Nos certificados em HSM Centralizado e em QSCD Centralizado, a chave privada do signatário é gerada em uma área privada do signatário em um HSM remoto. As credenciais de acesso à chave privada são inseridas pelo próprio signatário, não sendo armazenadas nem suscetíveis de dedução ou interceptação pelo sistema remoto de geração e custódia. A chave privada não é enviada ao signatário, ou seja, nunca sai do ambiente de segurança que garante o controle exclusivo da chave privada pelo signatário.

6.1.3. Envio da chave pública ao emissor do certificado

O método de envio da chave pública ao provedor de serviços eletrônicos confiável é o PKCS#10, outra prova criptográfica equivalente ou qualquer outro método aprovado pela UANATACA.

6.1.4. Distribuição da chave pública do prestador de serviços de certificação

As chaves UANATACA são comunicadas a terceiros que confiam nos certificados, garantindo a integridade da chave e autenticando a sua origem, através da sua publicação no Depositário.

Os usuários podem acessar o Repositório para obter chaves públicas e, adicionalmente, em aplicações S/MIME, a mensagem de dados pode conter uma cadeia de certificados, que desta forma são distribuídos aos usuários.

O certificado das Autoridades Certificadoras Raiz e Subordinadas estará disponível aos usuários no site da UANATACA.

6.1.5. Tamanhos de chave

- O comprimento das chaves da Autoridade de Certificação raiz é de 4.096 bits.
- O comprimento da chave da Autoridade de Certificação subordinada é de 4.096 bits.

- O comprimento das chaves dos Certificados de Entidade finais é de no mínimo 2.048 bits.

6.1.6. Geração de parâmetros de chave pública

A chave pública da raiz, das Autoridades de Certificação subordinadas e dos certificados de assinante é criptografada de acordo com a RFC 5280.

6.1.7. Verificação de qualidade de parâmetros de chave pública

- Comprimento do módulo = 4096 bits
- Algoritmo de geração de chave: rsagen1
- Funções criptográficas resumidas: SHA256.

6.1.8. Geração de chaves em aplicações informáticas ou bens de capital

Todas as chaves são geradas em bens de capital, conforme indicado na seção 6.1.1.

6.1.9. Principais finalidades de uso

Os usos das chaves para os certificados CA são exclusivamente para assinatura de certificados e CRLs.

Os usos das chaves dos certificados da entidade final são exclusivamente para assinatura digital, não repúdio e criptografia de dados.

6.2. Proteção de chave privada

6.2.1. Padrões de módulos criptográficos

Em relação aos módulos que gerenciam chaves UANATACA e assinantes de certificados de assinatura eletrônica, é garantido o nível exigido pelos padrões indicados nas seções anteriores.

6.2.2. Controle por mais de uma pessoa (n de m) sobre a chave privada

É necessário um controle multipessoal para ativação da chave privada AC. No caso desta Declaração de Práticas de Certificação, existe especificamente uma política **de 3 em cada 6** pessoas para ativação de chave.

Os dispositivos criptográficos são protegidos fisicamente conforme determinado neste documento.

6.2.3. Garantia de chave privada

A UANATACA não armazena cópias utilizáveis por meios próprios das chaves privadas dos signatários.

6.2.4. Backup de chave privada

A UANATACA faz uma cópia de segurança das chaves privadas das CAs que permitem a sua recuperação em caso de desastre, perda ou deterioração das mesmas. Tanto a geração da cópia como a sua recuperação requerem a participação de pelo menos duas pessoas.

Esses arquivos de recuperação são armazenados em armários à prova de fogo e na central de custódia externa.

Chaves geradas em um dispositivo de software: a UANATACA não pode fazer backups das chaves, pois não tem acesso às mesmas. O signatário pode fazer um backup.

Chaves geradas no QSCD: não podem ser feitos backups das chaves, pois não podem ser exportadas do QSCD.

Chaves geradas em HSM Centralizado e QSCD Centralizado: Só é possível fazer backups de um bloob criptografado com a chave Security World do HSM utilizado, sendo sua descriptografia impossível sem a utilização de credenciais que somente o titular do certificado conhece.

6.2.5. Arquivo de chave privada

As chaves privadas das ECs ficam arquivadas por um período de **10 anos** após a emissão do último certificado. Eles serão armazenados em arquivos seguros e à prova de fogo e no centro de custódia externo. Será necessária pelo menos a colaboração de duas pessoas para recuperar a chave privada das CAs no dispositivo criptográfico inicial.
Somente no caso de certificados de criptografia o assinante poderá armazenar a chave privada pelo tempo que considerar adequado. Neste caso a UANATACA manterá também uma cópia da chave privada associada ao certificado de encriptação.

UANATACA não arquiva chaves de certificados emitidas em software.

6.2.6. Inserindo a chave privada no módulo criptográfico

As chaves privadas são geradas diretamente nos módulos criptográficos de produção da UANATACA.

As chaves privadas da Autoridade Certificadora são armazenadas criptografadas nos módulos criptográficos de produção da UANATACA.

6.2.7. Método de ativação de chave privada

A chave privada UANATACA é ativada mediante a execução do procedimento de inicialização segura correspondente do módulo criptográfico, por pessoas autorizadas de acordo com esta Declaração de Práticas de Certificação.

As chaves AC são ativadas por um processo m de n (3 de 6). A ativação das chaves privadas da AC Intermediária é gerenciada com o mesmo processo m de n que as chaves da AC.

6.2.8. Método de desativação de chave privada

Para desativar a chave privada UANATACA serão seguidos os passos descritos no manual do administrador do equipamento criptográfico correspondente.

6.2.9. Método de destruição de chave privada

Antes da destruição das chaves, será emitida a revogação do certificado das chaves públicas a elas associadas.

Os dispositivos que possuem qualquer parte das chaves privadas UANATACA armazenadas serão fisicamente destruídos ou reinicializados em um nível baixo. Para eliminá-lo, siga os passos descritos no manual do administrador do equipamento criptográfico.

Finalmente, as cópias de backup serão destruídas com segurança. Em relação às chaves privadas dos signatários, serão seguidos os procedimentos estabelecidos no plano de rescisão.

6.2.10. Classificação de módulos criptográficos

Consulte a seção 6.2.1

6.3. Outros aspectos importantes do gerenciamento de pares

6.3.1. Arquivo de chave pública

A UANATACA arquiva suas chaves públicas rotineiramente, de acordo com o disposto na seção 5.5deste documento.

6.3.2. Períodos de uso de chaves públicas e privadas

Os períodos de utilização das chaves são determinados pela duração do certificado, após o qual não podem continuar a ser utilizadas.

A título de exceção e caso exista, a chave privada de desencriptação pode continuar a ser utilizada mesmo após a expiração do certificado.

6.4. Dados de ativação

6.4.1. Geração e instalação de dados de ativação

Os dados de ativação dos dispositivos que protegem as chaves privadas da UANATACA são gerados de acordo com o disposto na secção 6.2.2e os procedimentos da cerimónia de chaves.

A criação e distribuição dos referidos dispositivos são registradas.

Da mesma forma, UANATACA gera dados de ativação com segurança.

6.4.2. Proteção de dados de ativação

Os dados de ativação dos dispositivos que protegem as chaves privadas das Autoridades Certificadoras raiz e subordinadas são protegidos pelos titulares dos cartões de administrador dos módulos criptográficos, conforme consta no documento de cerimónia de chaves.

O signatário do certificado é responsável por proteger sua chave privada, com uma ou mais senhas tão completas e complexas quanto possível. O signatário deve lembrar-se da(s) senha(s).

6.5. Controles de segurança do computador

A UANATACA utiliza sistemas confiáveis para oferecer seus serviços de certificação. A UANATACA realizou controlos e auditorias informáticas com o objectivo de estabelecer uma gestão adequada dos seus activos informáticos com o nível de segurança exigido na gestão dos sistemas de certificação electrónica.

No que diz respeito à segurança da informação, a UANATACA aplica os controlos do esquema de certificação de sistemas de gestão de informação ISO 27001.

Os equipamentos utilizados são inicialmente configurados com os perfis de segurança adequados pelo pessoal dos sistemas da UANATACA, nos seguintes aspectos:

- Configurações de segurança do sistema operacional.
- Configurações de segurança do aplicativo.
- Dimensionamento correto do sistema.
- Configuração e permissões do usuário.
- Configuração de eventos de log.
- Plano de backup e recuperação.
- Configurações de antivírus.
- Requisitos de tráfego de rede.

6.5.1. Requisitos técnicos específicos de segurança informática

Cada servidor UANATACA inclui as seguintes funcionalidades:

- Controlo de acessos aos serviços de Autoridades Certificadoras subordinadas e gestão de privilégios.
- Aplicar a separação de funções para gerenciamento de privilégios.
- Identificação e autenticação de funções associadas a identidades.
- Arquivo de histórico de assinantes, Autoridades de Certificação subordinadas e dados de auditoria.
- Auditoria de eventos relacionados à segurança.
- Autodiagnóstico de segurança relacionado aos serviços das Autoridades Certificadoras subordinadas.
- Mecanismos de recuperação chave e sistema de Autoridades Certificadoras subordinadas.

As funcionalidades expostas são realizadas através de uma combinação de sistema operacional, software PKI, proteção física e procedimentos.

6.5.2. Avaliação do nível de segurança informática

A autoridade certificadora e os pedidos de registro utilizados pela UANATACA são confiáveis.

6.6. Controles técnicos do ciclo de vida

6.6.1. Controles de desenvolvimento de sistemas

As aplicações são desenvolvidas e implementadas pela UANATACA de acordo com os padrões de desenvolvimento e controle de mudanças.

Os aplicativos possuem métodos para verificação de integridade e autenticidade, bem como a exatidão da versão a ser utilizada.

6.6.2. Controles de gerenciamento de segurança

A UANATACA desenvolve as atividades necessárias à formação e sensibilização dos colaboradores em matéria de segurança. Os materiais utilizados para treinamento e os documentos que descrevem os processos são atualizados após sua aprovação por um grupo de gestão de segurança. No desempenho desta função existe um plano de formação anual.

A UANATACA exige, através de contrato, medidas de segurança equivalentes de qualquer fornecedor externo envolvido no trabalho de serviços eletrónicos confiáveis.

6.6.2.1. Classificação e gestão de informações e ativos

A UANATACA mantém um inventário de bens e documentação e um procedimento de gestão deste material para garantir a sua utilização.

A política de segurança da UANATACA detalha os procedimentos de gestão da informação onde esta é classificada de acordo com o seu nível de confidencialidade.

Os documentos estão catalogados em três níveis: NÃO CLASSIFICADOS, USO INTERNO e CONFIDENCIAL.

6.6.2.2. Operações de gestão

A UANATACA dispõe de um procedimento adequado de gestão e resposta a incidentes, através da implementação de um sistema de alerta e da geração de relatórios periódicos.

O processo de gestão de incidentes é desenvolvido detalhadamente no documento de segurança da UANATACA.

A UANATACA documentou todo o procedimento relativo às funções e responsabilidades do pessoal envolvido no controle e manipulação dos elementos contidos no processo de certificação.

6.6.2.3. Apoie o tratamento e a segurança

Todas as mídias são tratadas de forma segura de acordo com os requisitos da classificação da informação. A mídia que contém dados confidenciais é destruída com segurança se não for necessária novamente.

Planejamento do sistema

O departamento de Sistemas da UANATACA mantém um registro das capacidades dos equipamentos. Em conjunto com a aplicação do controle de recursos de cada sistema, pode-se prever um possível redimensionamento.

Relatórios de incidentes e resposta

A UANATACA possui um procedimento de monitoramento de incidentes e sua resolução onde são registradas as respostas e uma avaliação econômica que envolve a resolução do incidente.

Procedimentos operacionais e responsabilidades

A UANATACA define atividades, atribuídas a pessoas com um papel de confiança, diferente das pessoas encarregadas de realizar operações diárias que não são confidenciais.

6.6.2.4. Gerenciamento do sistema de acesso

A UANATACA faz todos os esforços razoáveis para confirmar que o sistema de acesso está limitado a pessoas autorizadas.

Em particular:

AC Geral

- Controles baseados em firewalls, antivírus e IDS estão disponíveis em alta disponibilidade.
- Os dados sensíveis são protegidos através de técnicas criptográficas ou controles de acesso com forte identificação.
- A UANATACA possui um procedimento documentado para gerenciamento de registros e cancelamentos de usuários e política de acesso detalhada em sua política de segurança.
- A UANATACA possui procedimentos para garantir que as operações sejam realizadas respeitando a política da função.
- Cada pessoa tem uma função associada a ela para realizar operações de certificação.
- Os funcionários da UANATACA são responsáveis por suas ações através do compromisso de confidencialidade firmado com a empresa.

Geração de certificado

A autenticação para o processo de emissão é realizada através de um sistema de m de n operadores para ativação da chave privada UANATACA.

Gerenciamento de revogação

A revogação será feita através de autenticação forte às aplicações de um administrador autorizado. Os sistemas de log gerarão evidências que garantam o não repúdio da ação realizada pelo administrador da UANATACA.

Status de revogação

A aplicação de status de revogação possui controle de acesso baseado em autenticação com certificados ou identificação de dois fatores para evitar tentativas de modificação das informações de status de revogação.

6.6.2.5. Gerenciamento do ciclo de vida de hardware criptográfico

A UANATACA garante que o hardware criptográfico utilizado para assinatura dos certificados não seja manipulado durante o transporte, inspecionando o material entregue.

O hardware criptográfico é transportado em suportes preparados para evitar qualquer manipulação.

UANATACA registra todas as informações pertinentes do dispositivo para adicionar ao catálogo de ativos.

O uso de hardware de assinatura de certificado criptográfico requer o uso de pelo menos dois funcionários de confiança.

A UANATACA realiza testes periódicos para garantir o correto funcionamento do dispositivo.

O dispositivo de hardware criptográfico é manuseado apenas por pessoal confiável.

A chave de assinatura privada UANATACA armazenada no hardware criptográfico será excluída assim que o dispositivo for removido.

A configuração do sistema UANATACA, bem como suas modificações e atualizações, são documentadas e controladas.

As alterações ou atualizações são autorizadas pelo responsável pela segurança e estão refletidas nas respectivas atas de trabalho. Estas configurações serão feitas por pelo menos duas pessoas de confiança.

6.7. Controles de segurança de rede

UANATACA protege o acesso físico aos dispositivos de gerenciamento de rede e possui uma arquitetura que ordena o tráfego gerado com base em suas características de segurança, criando seções de rede claramente definidas. Essa divisão é feita através do uso de firewalls.

As informações confidenciais transferidas por redes não seguras são criptografadas usando protocolos SSL ou sistema VPN com autenticação de dois fatores.

6.8. Controles de engenharia de módulos criptográficos

Os módulos criptográficos estão sujeitos aos controles de engenharia previstos nas normas indicadas ao longo desta seção.

Os algoritmos de geração de chaves usados são comumente aceitos para o uso pretendido.

Todas as operações criptográficas da UANATACA são realizadas em módulos com certificações FIPS 140-2 nível 3.

6.9. Fontes de tempo

UANATACA possui um procedimento coordenado de sincronização de horário via NTP, que acessa dois serviços independentes:

- A primeira sincronização é com um serviço baseado em antenas e receptores GPS que permite um nível de confiança do STRATUM 1 (com dois sistemas em alta disponibilidade).
- O segundo tem uma sincronização complementar, via NTP, com o Real Instituto e Observatório da Marinha (ROA).

6.10. Mudança de status de um Dispositivo Seguro de Criação de Assinatura (QSCD)

A UANATACA, no caso de alteração do estatuto de certificação dos dispositivos qualificados de criação de assinaturas (QSCD), procederá da seguinte forma:

1. A UANATACA dispõe de uma lista de vários QSCD certificados, bem como de uma estreita relação com os fornecedores dos referidos dispositivos, de forma a garantir alternativas a uma eventual perda do estatuto de certificação dos dispositivos QSCD.
2. Em caso de término do prazo de validade ou perda da certificação, a UANATACA não utilizará o referido QSCD para emissão de novos certificados digitais, seja em novas emissões ou eventualmente em possíveis renovações.
3. Procederemos imediatamente à mudança para dispositivos QSCD com certificação válida.
4. Caso se comprove que um dispositivo QSCD nunca o foi, por falsificação ou qualquer outro tipo de fraude, a UANATACA procederá imediatamente à notificação aos seus clientes e ao órgão regulador, revogando os certificados digitais emitidos nestes dispositivos e substituindo-os por emitindo-os em QSCDs válidos

7. Perfis de certificados e listas de certificados revogados

7.1. Perfil de certificado

Todos os certificados qualificados emitidos ao abrigo desta política cumprem a norma X.509 versão 3 e RFC 3739 e os diferentes perfis descritos na norma EN 319 412 .
A documentação relativa aos perfis da norma EN 319 412 pode ser solicitada à UANATACA.

7.1.1. Número da versão

UANATACA emite certificados X.509 Versão 3

7.1.2. Extensões de certificado

As extensões do certificado estão detalhadas nos documentos de perfil acessíveis no site da UANATACA (https://web.uanataca.com/).

Dessa forma, é possível manter versões mais estáveis da Declaração de Práticas de Certificação e isolá-las de ajustes frequentes nos perfis.

7.1.3. Identificadores de objeto de algoritmo (OIDs)

O identificador de objeto do algoritmo de assinatura é:

- 1.2.840.113549.1.1.11 sha256Com criptografia RSA

O identificador do objeto do algoritmo de chave pública é:

- 1.2.840.113549.1.1.1 criptografia rsa

7.1.4. Formato do nome

Os certificados devem conter as informações necessárias à sua utilização, conforme determinado pela política correspondente.

7.1.5. Restrições de nome

Os nomes contidos nos certificados estão restritos a X.500 “Nomes Distintos”, que são únicos e inequívocos.

7.1.6. Identificador de objeto (OID) de tipos de certificado

Todos os certificados incluem um identificador da política de certificados sob a qual foram emitidos, de acordo com a estrutura indicada no ponto 1.2.1

7.2. Perfil da lista de revogação de certificados

7.2.1. Número da versão

As LCR emitidas pela UANATACA são da versão 2.

7.2.2. Perfil OCSP

De acordo com o padrão IETF RFC 6960.

8. Auditoria de conformidade

A UANATACA comunicou o início da sua actividade como prestadora de serviços de certificação pelo Órgão Nacional de Supervisão e está sujeita às revisões de controlo que este órgão considere necessárias.

8.1. Frequência de auditoria de conformidade

A UANATACA realiza anualmente uma auditoria de conformidade, além das auditorias internas que realiza a seu critério ou a qualquer momento, por suspeita de descumprimento de alguma medida de segurança.

8.2. Identificação e qualificação do auditor

As auditorias são realizadas por uma empresa de auditoria externa independente que demonstra competência técnica e experiência em segurança informática, segurança de sistemas de informação e auditorias de conformidade de serviços de certificação de chaves públicas e elementos relacionados.

8.3. Relacionamento do auditor com a entidade auditada

As empresas de auditoria são de reconhecido prestígio com departamentos especializados na realização de auditorias informáticas, pelo que não existe conflito de interesses que possa distorcer a sua atuação em relação à UANATACA.

8.4. Lista de elementos sujeitos a auditoria

A auditoria verifica em relação à UANATACA:

a) Que a entidade possua um sistema de gestão que garanta a qualidade do serviço prestado.

b) Que a entidade cumpre os requisitos da Declaração de Práticas de Certificação e demais documentação relativa à emissão dos diversos certificados digitais.
c) Que a Declaração de Práticas de Certificação e demais documentação legal relacionada estejam em conformidade com o acordado pela UANATACA e com o estabelecido na regulamentação vigente.
d) Que a entidade gere adequadamente os seus sistemas de informação

Em particular, os elementos sujeitos a auditoria serão os seguintes:

a) Processos de Autoridades Certificadoras, Autoridades de Registro e elementos relacionados.
b) Sistemas de informação.
c) Proteção do centro de processamento de dados.
d) Documentos.

8.5. Ações a serem tomadas como resultado de uma falta de conformidade

Uma vez recebido pela administração o relatório da auditoria de conformidade realizada, as deficiências encontradas são analisadas com a empresa que realizou a auditoria e são desenvolvidas e executadas medidas corretivas para solucionar tais deficiências.

Caso a UANATACA não consiga desenvolver e/ou executar as medidas corretivas ou se as deficiências encontradas representarem uma ameaça imediata à segurança ou integridade do sistema, deverá notificar imediatamente o Comitê de Segurança da UANATACA, que poderá executar as seguintes ações:

- Cessar temporariamente as operações.
- Revogue a chave da Autoridade de Certificação e regenere a infraestrutura.
- Encerre o serviço da Autoridade de Certificação.
- Outras ações complementares que se fizerem necessárias.

8.6. Tratamento de relatórios de auditoria

Os relatórios dos resultados da auditoria são entregues ao Comitê de Segurança da UANATACA no prazo máximo de 15 dias após a execução da auditoria.

9. Requisitos comerciais e legais

9.1. Cotações

9.1.1. Taxa de emissão ou renovação de certificado

A UANATACA poderá estabelecer uma taxa pela emissão ou renovação de certificados, da qual, quando aplicável, os assinantes serão oportunamente informados.

9.1.2. Taxa de acesso ao certificado

A UANATACA não estabeleceu nenhuma taxa de acesso aos certificados.

9.1.3. Taxa de acesso às informações de status do certificado

A UANATACA não estabeleceu nenhuma taxa para acesso às informações sobre o status dos certificados.

9.1.4. Tarifas para outros serviços

Nenhuma estipulação.

9.1.5. Politica de reembolso

Nenhuma estipulação.

9.2. Capacidade financeira

A UANATACA dispõe de recursos económicos suficientes para manter as suas operações e cumprir as suas obrigações, bem como para enfrentar o risco de responsabilidade por danos , conforme estabelecido na ETSI EN 319 401-1 7.12 c), em relação à gestão da cessação dos serviços e plano de rescisão.

9.2.1. Cobertura do seguro

A UANATACA dispõe de uma garantia de cobertura suficiente de responsabilidade civil, através de um seguro de responsabilidade civil profissional, que mantém de acordo com a regulamentação em vigor aplicável.

9.2.2. Outros ativos

Nenhuma estipulação.

9.2.3. Cobertura de seguro para assinantes e terceiros que dependem de certificados

A UANATACA dispõe de garantia suficiente de cobertura de responsabilidade civil, através de seguro de responsabilidade civil profissional, para serviços eletrónicos de confiança, com um mínimo segurado de 6.000.000 euros.

9.3. Confidencialidade

9.3.1. Informação confidencial

As seguintes informações são mantidas confidenciais pela UANATACA:

- Solicitações de certificados, aprovadas ou negadas, bem como todas as demais informações pessoais obtidas para emissão e manutenção de certificados, exceto as informações indicadas na seção seguinte.
- Chaves privadas geradas e/ou armazenadas pelo provedor de serviços de certificação.
- Logs de transações, incluindo logs completos e logs de auditoria de transações.
- Registros de auditoria interna e externa, criados e/ou mantidos pela Autoridade Certificadora e seus auditores.
- Continuidade de negócios e planos de emergência.
- Planos de segurança.
- Documentação de operações, arquivamento, monitoramento e outros análogos.

- Todas as demais informações identificadas como “Confidenciais”.

9.3.2. Informações não confidenciais

As seguintes informações são consideradas não confidenciais:

- Certificados emitidos ou em processo de emissão.
- A vinculação do assinante a um certificado emitido pela Autoridade Certificadora.
- O nome e apelido da pessoa singular identificada no certificado, bem como qualquer outra circunstância ou dado pessoal do titular, caso seja significativo em função da finalidade do certificado.
- O endereço de correio eletrónico da pessoa singular identificada no certificado, ou o endereço de correio eletrónico atribuído pelo subscritor, se for significativo com base na finalidade do certificado.
- Os usos e limites econômicos descritos no certificado.
- O período de validade do certificado, bem como a data de emissão do certificado e a data de validade.
- O número de série do certificado.
- Os diferentes estados ou situações do certificado e a data de início de cada um deles, especificamente: geração e/ou entrega pendente, válido, revogado, suspenso ou expirado e o motivo que causou a mudança de estado.
- As listas de certificados revogados (CLRs), bem como as demais informações de status de revogação.
- As informações contidas nos depósitos de certificados.
- Qualquer outra informação que não esteja indicada na seção anterior.

9.3.3. Divulgação de informações sobre suspensão e revogação

Consulte a seção anterior.

9.3.4. Divulgação Legal de Informações

A UANATACA divulga informações confidenciais apenas nos casos legalmente previstos.

Especificamente, os registros que garantem a confiabilidade dos dados contidos no certificado serão divulgados caso seja necessário comprovar a certificação em processo judicial, mesmo sem o consentimento do titular do certificado.

A UANATACA indicará estas circunstâncias na política de privacidade prevista na seção 9.4.

9.3.5. Divulgação de informações a pedido de seu titular

A UANATACA inclui, na política de privacidade prevista na seção 9.4, requisitos para permitir a divulgação das informações do assinante e, quando aplicável, da pessoa física identificada no certificado, diretamente a ele ou a terceiros.

9.3.6. Outras circunstâncias de divulgação de informações

Nenhuma estipulação.

9.4. Proteção de dados pessoais

A UANATACA garante o cumprimento da regulamentação em vigor em matéria de protecção de dados pessoais, reflectida no Regulamento Europeu n.º 2016/679 sobre Protecção Geral de Dados e, em geral, em qualquer regulamentação nacional que possa ser aplicável.

Em conformidade com o mesmo, a UANATACA documentou nesta Declaração de Práticas de Certificação os aspectos e procedimentos de segurança e organizacionais, de forma a garantir que todos os dados pessoais a que tem acesso estão protegidos contra perda, destruição, dano, falsificação e tratamento ilícito ou não autorizado. .

Todas as informações necessárias relativas ao tratamento de dados pessoais realizado pela UANATACA são detalhadas a seguir:

Responsável pelo tratamento

Uanataca, SA

NIF : A66721499

Endereço : Avenida Meridiana, nº 350, 3º andar, 08027, Barcelona.

Dados cadastrais : Junta Comercial de Barcelona, conforme registro datado de 15 de março de 2016, no tomo 45264, fólio 6, folha B 482242, registro 1.

Oficial de Proteção de Dados

Telefone : (+34) 93 527 22 90

E-mail : legal@uanataca.com

Objetivo do tratamento

A UANATACA trata os dados pessoais fornecidos para a realização dos serviços eletrónicos solicitados, nomeadamente a emissão de certificados eletrónicos, tudo de acordo com o disposto na Declaração de Práticas de Certificação (DPC) da UANATACA, que se encontra disponível no seguinte link: https: / /www.uanataca.com/public/cps/ .

As finalidades do tratamento de dados relacionadas com o SERVIÇO são as seguintes:

- Identificação de assinantes e/ou signatários de certificados eletrônicos.
- Emissão e gestão de certificados eletrónicos.
- Gestão do ciclo de vida do certificado (suspensão, renovação, reativação e revogação).
- Comunicações relacionadas ao serviço.
- Custódia e manutenção do arquivo referente ao certificado eletrônico.
- Gestão administrativa, contábil e de faturamento derivada da contratação.

Legitimação do tratamento

A legitimação do tratamento de dados pessoais para Prestação de Serviços de Confiança para emissão de certificados eletrónicos baseia-se na celebração de contrato dos serviços solicitados, onde o utilizador dele faça parte.

Dados processados e conservação

As categorias de dados pessoais tratados pela UANATACA, a título de exemplo, mas não limitativo, incluem:

- Dados de identificação: nome, apelido e número de identidade oficial.
- Dados profissionais: organização, departamento e/ou cargo.
- Dados de contacto: morada postal, email e telefone.
- Dados relativos à identidade ou identificação dos usuários: fotografias e/ou quando aplicável o padrão biométrico facial, para poder realizar o processo de identificação por vídeo UANATACA.

Os dados pessoais serão conservados até ao final da relação contratual e posteriormente, durante os prazos legalmente exigidos de acordo com cada caso. Regra geral, os dados pessoais relativos ao SERVIÇO serão conservados durante 15 anos a contar da expiração do certificado ou do fim do serviço prestado.

Da mesma forma, as provas dos processos de identificação serão conservadas durante 15 anos, exceto as provas incompletas que serão conservadas por um período mínimo de 5 anos.

Os dados pessoais serão armazenados nas instalações seguras da UANATACA localizadas em Espanha e Itália.

Transferência de dados

Os dados poderão ser disponibilizados a terceiros, no território da União Europeia, para a prestação de serviços contratados pelo utilizador (por exemplo fornecedores de alojamento de dados (CPD), serviços de apoio à identificação, empresas do grupo, etc.), tudo isto sob a proteção do correspondente contrato de tratamento de dados pessoais, garantindo sempre medidas de segurança adequadas que garantam a devida proteção dos dados pessoais dos utilizadores.

Sem prejuízo do acima exposto, regra geral, os dados pessoais apenas serão cedidos a terceiros por obrigação legal.

Como regra geral, não serão realizadas transferências internacionais .

Direitos de uso

Os utilizadores poderão exercer os seus direitos de confirmação, acesso, retificação, eliminação, cancelamento, limitação, oposição e portabilidade.

- Confirmação . Todos os utilizadores têm o direito de obter a confirmação se a UANATACA está a tratar dados pessoais que lhes digam respeito.

- Acesso e retificação . Os utilizadores têm o direito de aceder a todos os seus dados pessoais, bem como solicitar a retificação daqueles que sejam inexatos ou erróneos.

- Exclusão e cancelamento . Os utilizadores poderão solicitar a eliminação/cancelamento dos dados quando, entre outros motivos, os mesmos não sejam necessários para as finalidades para as quais foram recolhidos.

- Limitação e oposição . O usuário poderá solicitar a limitação do tratamento para que os seus dados pessoais não sejam aplicados às operações correspondentes. Em determinadas circunstâncias e por motivos relacionados com a sua situação particular, o utilizador poderá opor-se ao tratamento dos dados, ficando a UANATACA obrigada a cessar o tratamento dos mesmos, salvo por motivos legítimos imperiosos, ou ao exercício ou defesa de eventuais reclamações.

- Portabilidade . Os interessados poderão solicitar que os seus dados pessoais lhes sejam enviados ou transmitidos a outro responsável, em formato eletrónico estruturado e de uso corrente.

Para exercer os seus direitos, os utilizadores podem enviar um pedido para o endereço de correio eletrónico ou escrever para o endereço: Avenidada meridiana, nº 350, 3ª planta, 08027, Barcelona. Neste pedido deverão anexar uma cópia do seu documento de identidade e indicar claramente o direito que pretendem exercer.

9.5. Direito de propriedade intelectual

9.5.1. Propriedade do certificado e informações de revogação

Apenas a UANATACA goza de direitos de propriedade intelectual sobre os certificados que emite, sem prejuízo dos direitos dos assinantes, titulares de chaves e terceiros, a quem concede licença não exclusiva para reprodução e distribuição de certificados, gratuitamente, desde que a reprodução é completo e não altera nenhum elemento do certificado, sendo necessário em relação às assinaturas digitais e/ou sistemas de criptografia no âmbito de utilização do certificado, e de acordo com a documentação que os vincula.

Além disso, os certificados emitidos pela UANATACA contêm um aviso legal sobre a sua titularidade.

As mesmas regras se aplicam ao uso de informações de revogação de certificado.

9.5.2. Propriedade da Declaração de Práticas de Certificação

Somente a UANATACA goza de direitos de propriedade intelectual sobre esta Declaração de Práticas de Certificação.

9.5.3. Propriedade das informações do nome

O assinante e, quando aplicável, a pessoa física identificada no certificado, retém todos os direitos, se houver, sobre a marca, produto ou nome comercial contido no certificado.

O assinante é o proprietário do nome distinto (DN) do certificado, composto pelas informações especificadas na seção 3.1.1.

9.5.4. Propriedade da chave

Os pares de chaves pertencem aos assinantes dos certificados.

Quando uma chave é dividida em partes, todas as partes da chave são propriedade do proprietário da chave.

9.6. Obrigações e responsabilidade civil

9.6.1. Obrigações da UANATACA

A UANATACA garante, sob a sua inteira responsabilidade, que cumpre todos os requisitos estabelecidos na Declaração de Práticas de Certificação, responsabilizando-se pelo cumprimento dos procedimentos descritos, de acordo com as indicações contidas neste documento.

A UANATACA fornece serviços eletrônicos confiáveis de acordo com esta Declaração de Práticas de Certificação.

A UANATACA informa o subscritor dos termos e condições relativos à utilização do certificado, do seu preço e das suas limitações de utilização, através de um contrato de subscritor que incorpora por referência os textos de divulgação (PDS) de cada um dos certificados adquiridos.

O documento de texto de divulgação, também denominado PDS [17], está em conformidade com o conteúdo do Anexo A da ETSI EN 319 411-1 v1.1.1 (2016-02), um documento que pode ser transmitido por meios eletrónicos, utilizando um meio de comunicação duradouro no tempo e em linguagem compreensível.

A UANATACA vincula os assinantes, titulares de chaves e terceiros que confiem nos certificados, através do referido texto de divulgação ou PDS, em linguagem escrita e compreensível, com os seguintes conteúdos mínimos:

- Prescrições para atendimento ao disposto nas seções 4.5.3, 9.2, 9.6.7, 9.6.8, 9.6.9e 9.6.10.
- Indicação da política aplicável, indicando que os certificados não são emitidos ao público.

[17]"Declaração de divulgação de PKI" ou declaração de divulgação de PKI aplicável.

- Demonstração de que as informações contidas no certificado estão corretas, salvo notificação em contrário por parte do assinante.
- Consentimento para publicação do certificado no repositório e acesso de terceiros ao mesmo.
- Consentimento para o armazenamento da informação utilizada para o registo do assinante e para a transferência dessa informação a terceiros, em caso de cessação das operações da Autoridade Certificadora sem revogação de certificados válidos.
- Limites de uso de certificados, incluindo aqueles estabelecidos na seção 1.4.2
- Informações sobre como validar um certificado, incluindo o requisito de verificar o estado do certificado e as condições sob as quais o certificado pode ser razoavelmente confiável, o que é aplicável quando o assinante atua como um terceiro que depende do certificado.
- Como é garantida a responsabilidade financeira da Autoridade Certificadora.
- Limitações de responsabilidade aplicáveis, incluindo utilizações pelas quais a Autoridade Certificadora aceita ou exclui a sua responsabilidade.
- Período de arquivamento de informações de solicitação de certificado.
- Período de arquivamento do log de auditoria.
- Procedimentos de resolução de litígios aplicáveis.
- Lei aplicável e jurisdição competente.
- Se a Autoridade Certificadora foi declarada em conformidade com a política de certificação e, se aplicável, de acordo com qual sistema.

9.6.2. Garantias oferecidas a assinantes e terceiros que dependem de certificados

A UANATACA, na documentação que a vincula aos assinantes e terceiros que dependem de certificados, estabelece e rejeita garantias e limitações de responsabilidade aplicáveis.

A UANATACA garante, no mínimo, ao assinante:

- Que não existem erros factuais nas informações contidas nos certificados, conhecidos ou cometidos pela Autoridade Certificadora .
- Que não existem erros factuais nas informações contidas nos certificados, por falta de diligência na gestão do pedido de certificado ou na sua criação.

- Que os certificados atendam a todos os requisitos materiais estabelecidos na Declaração de Práticas de Certificação.
- Que os serviços de revogação e a utilização do Repositório cumpram todos os requisitos materiais estabelecidos na Declaração de Práticas de Certificação.

A UANATACA garantirá, no mínimo, ao terceiro que confia no certificado:

- Que as informações contidas ou incorporadas por referência no certificado são corretas, salvo indicação em contrário.
- No caso de certificados publicados no Depositário, que o certificado tenha sido emitido ao assinante nele identificado e que o certificado tenha sido aceite, nos termos da secção 4.4.
- Que na aprovação do pedido de certificado e na emissão do certificado foram atendidos todos os requisitos materiais estabelecidos na Declaração de Práticas de Certificação.
- A rapidez e segurança na prestação de serviços, especialmente serviços de revogação e depósito.

Adicionalmente, a UANATACA garante ao assinante e ao terceiro que confia no certificado:

- Que o certificado contenha a informação que um certificado qualificado deve conter, de acordo com o disposto na Lei 6/2020, de 11 de novembro.
- Que, caso sejam geradas as chaves privadas do assinante ou, se for o caso, da pessoa singular identificada no certificado, a sua confidencialidade seja mantida durante o processo.
- A responsabilidade da Autoridade Certificadora, com os limites estabelecidos.

9.6.3. Isenção de outras garantias

A UANATACA rejeita qualquer outra garantia que não seja legalmente exigível, exceto as contempladas na seção 9.6.2.

9.6.4. Limitação de responsabilidades

A UANATACA limita a sua responsabilidade à emissão e gestão de certificados e pares de chaves de assinante fornecidos pela Autoridade Certificadora.

9.6.5. Cláusulas de indenização

9.6.5.1. Cláusula de indenização do assinante

A UANATACA inclui no contrato com o assinante uma cláusula pela qual o assinante se obriga a isentar a Autoridade Certificadora de qualquer dano decorrente de qualquer ação ou omissão que resulte em responsabilidade, dano ou perda, despesa de qualquer tipo, incluindo as judiciais e legais representação que possa ser incorrida, em razão da publicação e utilização do certificado, quando ocorrer alguma das seguintes causas:

- Falsidade ou declaração errada feita pelo usuário do certificado.
- Erro do usuário do certificado ao fornecer os dados da solicitação, caso a ação ou omissão tenha envolvido fraude ou negligência com relação à Autoridade Certificadora ou a qualquer pessoa que confie no certificado.
- Deixar de proteger a chave privada, de utilizar um sistema confiável ou de manter as precauções necessárias para evitar o comprometimento, perda, divulgação, modificação ou uso não autorizado da referida chave.
- Utilização pelo assinante de um nome (incluindo nomes comuns, endereços de correio eletrónico e nomes de domínio), ou outra informação constante do certificado, que viole direitos de propriedade intelectual ou industrial de terceiros.

9.6.5.2. Cláusula de indenização de terceiros que depende do certificado

A UANATACA inclui no texto de divulgação ou PDS, cláusula pela qual o terceiro que confia no certificado se compromete a isentar a Autoridade Certificadora de qualquer dano decorrente de qualquer ação ou omissão que resulte em responsabilidade, dano ou perda, despesas de qualquer espécie, incluindo despesas judiciais e de representação legal que possam ser incorridas, para a publicação e utilização da certidão, quando ocorrer qualquer uma das seguintes causas:

- Incumprimento das obrigações do terceiro que depende do certificado.
- Confiança imprudente num certificado, dadas as circunstâncias.
- Falha na verificação do status de um certificado para determinar se ele não está suspenso ou revogado.

9.6.6. Caso fortuito e força maior

A UANATACA não será responsável em nenhum caso por situações que surjam do acaso e em casos de força maior.

Entende-se por acontecimento fortuito aquela situação ou acontecimento impossível de prever, ou que, se previsto, é inevitável no que diz respeito à sua mitigação. Adicionalmente, entende-se por força maior a situação ou evento inevitável para tornar efetivas as suas circunstâncias, imprevisíveis e extraordinárias na sua origem, emanadas de um ambiente estranho e irresistível.

Portanto, a UANATACA não será responsável em caso algum por situações de guerra, desastres naturais, funcionamento disfuncional de serviços eléctricos, redes ou infra-estruturas informáticas, por motivos não imputáveis à UANATACA.

9.6.7. Lei aplicável

A UANATACA estabelece, no contrato de subscrição e no texto de divulgação ou PDS, que a lei aplicável à prestação de serviços, incluindo a política e práticas de certificação, é a Lei Espanhola.

9.6.8. Divisibilidade, sobrevivência, acordo integral e cláusulas de notificação

A UANATACA estabelece, no contrato de adesão, e no texto de divulgação ou PDS, cláusulas de divisibilidade, sobrevivência, plena concordância e notificação:

- De acordo com a cláusula de divisibilidade, a invalidade de uma cláusula não afetará o restante do contrato.
- Ao abrigo da cláusula de sobrevivência, determinadas regras continuarão a aplicar-se após a cessação da relação jurídica que regula o serviço entre as partes. Para o efeito, a Autoridade Certificadora assegura que pelo menos os requisitos constantes das secções 9.6.1(Obrigações e responsabilidade), 8(Auditoria de conformidade) e 9.3(Confidencialidade), permanecem em vigor após o término do serviço e as condições gerais de emitir/usar.

- Pela cláusula de contrato integral, entender-se-á que o documento legal que regulamenta o serviço contém o testamento completo e todos os acordos entre as partes.
- De acordo com a cláusula de notificação, será estabelecido o procedimento pelo qual as partes se notificarão mutuamente dos fatos.

9.6.9. Cláusula de Jurisdição Competente

A UANATACA estabelece, no contrato de subscrição e no texto de divulgação ou PDS, uma cláusula de jurisdição competente, indicando que a jurisdição judicial internacional corresponde aos juízes espanhóis.

A jurisdição territorial e funcional será determinada em virtude das normas de direito internacional privado e das normas de direito processual aplicáveis.

9.6.10. Resolução de conflitos

A UANATACA estabelece, no contrato de subscrição, e no texto de divulgação ou PDS, os procedimentos de mediação e resolução de conflitos aplicáveis.

10. Anexo I - Siglas

EBA	Autoridade Bancária Europeia
A.C.	Autoridade de Certificação
AC	Autoridade de Certificação. Autoridade de Certificação
R.A.	Autoridade de Registro
NCA	Autoridade Nacional Competente (PSD2)
CP	Política de Certificado
CPS	Declaração de práticas de certificação. Declaração de práticas de certificação
CRL	Lista de revogação de certificados. Lista de certificados revogados
RSE	Solicitação de assinatura de certificado. Solicitação de assinatura de certificado
DES	Padrão de criptografia de dados. Padrão de criptografia de dados
PSD2	Diretiva Serviços de Pagamento
D. N.	Nome Distinto. Nome distintivo dentro do certificado digital
DSA	Algoritmo de Assinatura Digital. Padrão de algoritmo de assinatura
DCCF	Dispositivo qualificado de criação de assinatura
QSCD	Dispositivo qualificado de criação de assinatura. Dispositivo qualificado de criação de assinatura
FIPS	Publicação padrão de processamento de informações federais
ISO	Organização Internacional para Padronização. Organismo internacional de padronização
LDAP	Protocolo leve de acesso a diretórios. Protocolo de acesso ao diretório
OCSP	Protocolo de status de certificado on-line. Protocolo de acesso ao status do certificado
OID	Identificador de Objeto. Identificador de objeto
PA	Autoridade Política. Autoridade Política
computador	Política de Certificação
ALFINETE	Número de identificação pessoal. Número de identificação pessoal
PKI	Infraestrutura de chave pública. Infraestrutura de chave pública
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de criptografia
SHA	Algoritmo Hash Seguro. Algoritmo Hash Seguro
SSL	Camada de soquetes seguros
TCP/IP	Controle de transmissão. Protocolo/Protocolo de Internet