Texto de divulgação - PDS (PKI Disclosure Statement) para assinatura eletrônica e certificados de autenticação

Informações gerais

Controle documental

Classificação de segurança:	**Público**
Versão:	**3**
Data de edição:	**02/06/2023**
Arquivo:	**PDS-FIRMA_ES_v3**
Código	**PSC-3.1-**

estatuto formal

Preparado por:	**Revisados pela:**	**Aprovado por:**
Nome: Andreia Vargas Data: 02/06/2023	Nome: Alejandro Grande Data: 02/06/23	Nome: Gabriel García Data: 06/06/2023

Controle de versão

Versão	Partes que mudam	Alteração na descrição	Mudança de autor	Alterar data
1,0	Original	Criação de documento	A.C.	22/03/2016
1.1	Completo	Nova versão do documento adicionando todos os perfis de assinatura	DMP	12/05/2017
1.2	2	Novos perfis de certificado são adicionados no QSCD Centralizado	ABD	05/09/2021
2	Completo	Revisão do documento referente à nova versão da Declaração de Práticas de Certificação. Ajuste de acordo com a codificação documental do Sistema de Gestão de Segurança da Informação.	AGB	11/11/2021
3	1.1.1 1.3.1	Atualização da sede social da UANATACA SA Inclusão explicativa de atributos em certificados para identificação de interessados perante Administrações Públicas.	APV	06/06/2023

Índice

INFORMAÇÕES GERAIS 2

CONTROLE DE DOCUMENTOS 2
ESTATUTO FORMAL 2
CONTROLE DE VERSÃO 3

ÍNDICE 4

1. TEXTO DE DIVULGAÇÃO APLICÁVEL À ASSINATURA ELETRÔNICA E CERTIFICADOS DE AUTENTICAÇÃO 7

1.1. INFORMAÇÕES DE CONTATO 7
1.1.1. Organização responsável 7
1.1.2. Contato 7
1.1.3. Emissor de Provedor de Serviços Eletrônicos Confiável 7
1.1.4. Contacto para processos de revogação 8
1.2. TIPOS DE CERTIFICADOS 8
1.3. FINALIDADE DOS CERTIFICADOS 9
1.3.1. Estipulações comuns 10
1.3.2. Certificado Qualificado de Pessoa Física no software 10
1.3.3. Certificado qualificado de assinatura de Pessoa Física no QSCD 11
1.3.4. Certificado Qualificado de Pessoa Física no QSCD 12
1.3.5. Certificado qualificado de pessoa física em HSM centralizado 12
1.3.6. Certificado Qualificado de Pessoa Física em QSCD centralizado 13
1.3.7. Certificado qualificado de assinatura de Pessoa Física no QSCD 14
1.3.8. Certificado Qualificado de Representante Pessoa Física no software 14
1.3.9. Certificado qualificado de assinatura de Representante Pessoa Física no QSCD 15
1.3.10. Certificado qualificado de assinatura do Representante Pessoa Física no QSCD 16
1.3.11. Certificado qualificado de pessoa física Representante de Pessoa Jurídica perante as administrações em software 16
1.3.12. Certificado qualificado de pessoa física Representante de Pessoa Jurídica perante as administrações no QSCD 17
1.3.13. Certidão qualificada de Pessoa Física Representante de Pessoa Jurídica perante as administrações em HSM centralizado 18
1.3.14. Certificado qualificado de Pessoa Física Representante de Pessoa Jurídica perante as administrações em QSCD centralizado 18
1.3.15. Certificado qualificado de pessoa singular Representante de Entidade sem Personalidade Jurídica perante as administrações em software 19

1.3.16. Certificado qualificado de pessoa singular Representante de Entidade sem Personalidade Jurídica perante as administrações no QSCD 20
1.3.17. Certificado qualificado de pessoa singular Representante de Entidade sem Personalidade Jurídica perante as administrações em HSM centralizado 20
1.3.18. Certificado qualificado de pessoa singular Representante de Entidade sem Personalidade Jurídica perante as administrações em QSCD centralizado 21
1.3.19. Certificado Qualificado de Funcionário Público de Nível Médio 22
1.3.20. Certificado de autenticação eletrônica para Funcionário Público Alto Nível 22
1.3.21. Certificado qualificado de assinatura de Funcionário Público de Alto Nível 23
1.3.22. Certificado qualificado de assinatura de Funcionário Público de Alto Nível no QSCD centralizado 23
1.4. LIMITES DE USO DE CERTIFICADO 25
1.4.1. Limites de uso direcionados aos signatários 25
1.4.2. Limites de uso voltados para verificadores 25
1.5. OBRIGAÇÕES DOS ASSINANTES 27
1.5.1. Geração de chave 27
1.5.2. Solicitação de Certificado 27
1.5.3. Obrigações de informação 27
1.6. OBRIGAÇÕES DOS SIGNATÁRIOS 28
1.6.1. Obrigações de custódia 28
1.6.2. Obrigações de uso correto 28
1.7. OBRIGAÇÕES DOS VERIFICADORES 29
1.7.1. Decisão informada 29
1.7.2. Requisitos de verificação de assinatura eletrônica 29
1.7.3. Confie em um certificado não verificado 30
1.7.4. Efeito da verificação 30
1.7.5. Uso correto e atividades proibidas 30
1.7.6. Cláusula de indenização 31
1.8. OBRIGAÇÕES DA UANATACA 32
1.8.1. Em relação à prestação do serviço de certificação digital 32
1.8.2. Em relação às verificações de registro 32
1.8.3. Períodos de conservação 33
1.9. GARANTIAS LIMITADAS E ISENÇÃO DE GARANTIAS 33
1.9.1. Garantia UANATACA para serviços de certificação digital 33
1.9.2. Exclusão de garantia 34
1.10. ACORDOS APLICÁVEIS E CPS 35
1.10.1. Acordos aplicáveis 35
1.10.2. Declaração de Práticas de Certificação 35
1.11. REGRAS DE CONFIANÇA PARA ASSINATURAS DE LONGA DURAÇÃO 35
1.12. POLÍTICA DE PRIVACIDADE 35

1.13. POLÍTICA DE PRIVACIDADE 36
1.14. POLÍTICA DE REEMBOLSO 36
1.15. REGULAMENTOS APLICÁVEIS E JURISDIÇÃO COMPETENTE 37
1.16. LINK COM A LISTA DE PROVEDORES DE SERVIÇOS ELETRÔNICOS CONFIÁVEIS E QUALIFICADOS 37
1.17. DIVISIBILIDADE DE CLÁUSULAS, SOBREVIVÊNCIA, ACORDO TOTAL E NOTIFICAÇÃO 37

1. ASSINATURA ELETRÔNICA E CERTIFICADOS DE AUTENTICAÇÃO

Este documento contém as informações essenciais que você deve saber em relação ao serviço de certificação do Provedor de Serviços Eletrônicos Confiável UANATACA.

1.1. Informação de contato

1.1.1. Organização responsável

O Provedor de Serviços Eletrônicos de Confiança Uanataca, SA, doravante "UANATACA", é uma iniciativa de:

UANATACA, SA
AVENIDA MERIDIANA, 350 3º ANDAR 08027 BARCELONA
TELEFONE: 935 272 290
E-MAIL: INFO@UANATACA.COM

1.1.2. Contato

Para qualquer dúvida, entre em contato:

UANATACA, SA
E-MAIL: INFO@UANATACA.COM
TELEFONE: 935 272 290

1.1.3. Provedor de serviços eletrônicos confiável do emissor

Os certificados descritos neste documento são emitidos pela UANATACA, identificados pelos dados acima indicados.

1.1.4. Contacto para processos de revogação

Para qualquer dúvida, entre em contato:

UANATACA, SA
E-MAIL: INFO@UANATACA.COM
TELEFONE: 935 272 290

1.2. Tipos de certificados

Os seguintes certificados emitidos pela UANATACA estão qualificados de acordo com o artigo 28 e Anexo I do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014 e cumprem o disposto nos regulamentos técnicos identificados com o referência ETSI EN 319 411-2. A UANATACA atribuiu a cada tipo de certificado um identificador de objeto (OID), para identificação pelas aplicações, que são detalhados a seguir:

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 no QSCQ*
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*
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*
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*
	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*

1.3. Finalidade dos certificados

1.3.1. Estipulações comuns

Os certificados qualificados descritos neste documento e emitidos em software e HSM Centralizado, garantem a identidade do assinante e da pessoa indicada no certificado, permitindo a geração da "assinatura eletrónica avançada baseada num certificado eletrónico qualificado".

Os certificados qualificados descritos neste documento e emitidos em QSCD e QSCD Centralizada, funcionam com dispositivos qualificados de criação de assinaturas, de acordo com os artigos 29 e 51 do Regulamento (UE) 910/2014, e cumprem o disposto na norma técnica de o Instituto Europeu de Normas de Telecomunicações, identificado com a referência EN 319 411-2 . Estes certificados qualificados garantem a identidade do signatário, permitindo 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.

Sem prejuízo do anterior, qualquer tipo de certificado eletrónico qualificado, quando emitido para identificação de interessados perante as Administrações Públicas, deverá conter como atributos **a sua 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.

1.3.2. 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 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:

a) 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

1.3.3. 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.

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

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

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

a) 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)

1.3.4. 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.

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

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

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

a) 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

1.3.5. 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 o OID 0.4.0.194112.1.0, que está declarado no certificado. Os certificados de pessoas singulares emitidos em HSM Centralizado são certificados qualificados de acordo com o disposto no artigo 28.º do Regulamento (UE) 910/2014 eIDAS.

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:

a) 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

1.3.6. 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.

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

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

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

a) 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

1.3.7. 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.

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

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

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

a) 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)

1.3.8. 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 que é emitido para assinatura e autenticação eletrónica avançada de pessoa singular ou representante de entidade, emitido em software de acordo com o disposto no artigo 28.º do Regulamento (UE) 910/2014 eIDAS, e que cumpre o disposto no os regulamentos técnicos do European Telecommunications Standards Institute, identificados com a referência EN 319 411-2 .

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:

a) 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

1.3.9. 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.

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

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

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

a) 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)

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

Este certificado possui o OID 1.3.6.1.4.1.47286. 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.

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

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

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

a) 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)

1.3.11. 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.

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:

a) 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

1.3.12. 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.

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:

a) 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

1.3.13. Certificado qualificado de Pessoa Física Representante de Pessoa Jurídica perante as administrações em HSM centralizado

Este certificado possui o OID 1.3.6.1.4.1.47286.1.7.5. 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.

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:

a) 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

1.3.14. 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 em QSCD remoto é um certificado qualificado de acordo com o disposto nos artigos 28 do Regulamento (UE) 910/2014 eIDAS.

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:

a) 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

1.3.15. 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.

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:

a) 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

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

Este certificado possui o OID 1.3.6.1.4.1.47286.1.8.2.2. 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.

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

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

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

a) 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

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

Este certificado possui o OID 1.3.6.1.4.1.47286.1.8.5. 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.

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:

a) 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

1.3.18. 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 em QSCD remoto é um certificado qualificado de acordo com o disposto nos artigos 28 do Regulamento (UE) 910/2014 eIDAS.

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

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

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

a) 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

1.3.19. Certificado Qualificado de Funcionário Público de Nível Médio

Este certificado possui o OID 1.3.6.1.4.1.47286.1.4.1. 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.

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:

a) 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

1.3.20. 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.

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

a) 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

1.3.21. 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.

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:

a) 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)

1.3.22. 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 emitido em QSCD remoto é um certificado qualificado de acordo com o disposto nos artigos 28 do Regulamento (UE) 910/2014 eIDAS.

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:

a) 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. Limites de uso de certificados

1.4.1. Limites de uso direcionados aos signatários

O signatário deverá utilizar o serviço de certificação de certificados prestado pela UANATACA, exclusivamente para os usos autorizados no contrato celebrado entre a UANATACA e o ASSINANTE, e que são reproduzidos posteriormente (seção "obrigações dos signatários").

Da mesma forma, o signatário compromete-se a utilizar o serviço de certificação digital de acordo com as instruções, manuais ou procedimentos fornecidos pelo UANATACA.

O signatário deve cumprir quaisquer leis e regulamentos que possam afetar seu direito de uso das ferramentas criptográficas que utiliza.

O signatário não poderá adotar medidas de inspeção, alteração ou engenharia reversa dos serviços de certificação digital da UANATACA, sem prévia autorização expressa.

1.4.2. Limites de uso voltados para verificadores

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 tidos em conta os limites indicados nos vários campos dos perfis de certificados, visíveis no site da UANATACA (https://www.uanataca.com).

A utilização de certificados digitais em operações que contrariem este texto de divulgação, ou os contratos com assinantes, é considerada utilização indevida para os efeitos legais cabíveis, isentando assim a UANATACA, com base na legislação em vigor, de qualquer responsabilidade por esta utilização indevida dos certificados efetuados. pelo signatário ou por qualquer terceiro.

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 surgir do seu uso fora dos limites e condições de uso incluídos neste texto de divulgação, ou nos contratos com assinantes, bem como qualquer outro uso indevido do mesmo derivado desta seção ou que possa ser interpretado como tal com base sobre a regulamentação aplicável.

1.5. Obrigações dos assinantes

1.5.1. Geração de chave

O assinante autoriza a UANATACA a gerir, de acordo com os métodos e procedimentos correspondentes, a emissão das chaves privadas e públicas para os signatários, e solicita em seu nome a emissão do certificado de acordo com as políticas de certificação da UANATACA.

1.5.2. Solicitação de certificado

O assinante obriga-se a solicitar certificados qualificados de acordo com o procedimento e, se necessário, os componentes técnicos fornecidos pela UANATACA, de acordo com o estabelecido na declaração de práticas de certificação (DPC) e na documentação de operações da UANATACA.

1.5.3. Obrigações de informação

O assinante é responsável por garantir que todas as informações incluídas em sua solicitação de certificado sejam precisas, completas para a finalidade do certificado e sempre atualizadas.

O assinante deverá informar imediatamente a UANATACA:

- De qualquer imprecisão detectada no certificado após sua emissão.
- Das alterações ocorridas nas informações fornecidas e/ou registradas para emissão do certificado.
- Perda, roubo, furto ou qualquer outro tipo de perda de controle da chave privada por parte do signatário.

1.6. Obrigações dos signatários

1.6.1. Obrigações de custódia

O signatário compromete-se a salvaguardar o código de identificação pessoal ou qualquer suporte técnico fornecido pela UANATACA, as chaves privadas e, se necessário, as especificações propriedade da UANATACA que lhe sejam fornecidas.

Em caso de perda ou roubo da chave privada do certificado, ou caso o signatário suspeite que a chave privada perdeu fiabilidade por qualquer motivo, tais circunstâncias deverão ser imediatamente notificadas à Autoridade de Registo de referência ou à UANATACA.

1.6.2. Obrigações de uso correto

O signatário deverá utilizar o serviço de certificação de certificados de pessoa física emitidos em DCCF (QSCD) fornecido pela UANATACA, exclusivamente para usos autorizados na DPC e em quaisquer outras instruções, manuais ou procedimentos fornecidos ao assinante.

O signatário deverá cumprir quaisquer leis e regulamentos que possam afetar seu direito de uso das ferramentas criptográficas utilizadas.

O signatário não poderá adotar medidas de fiscalização, alteração ou descompilação dos serviços de certificação digital prestados.

O signatário reconhecerá:

a) Que quando você usa qualquer certificado, e desde que o certificado não tenha expirado ou tenha sido suspenso ou revogado, você aceitou esse certificado e ele está operacional.

b) Que não atua como entidade certificadora e, portanto, compromete-se a não utilizar as chaves privadas correspondentes às chaves públicas contidas nos certificados para efeitos de assinatura de qualquer certificado.

c) Que se a chave privada for comprometida, você deverá cessar imediata e permanentemente seu uso e proceder de acordo com este documento.

1.7. Obrigações dos verificadores

1.7.1. Decisão informada

A UANATACA informa ao verificador que tem acesso a informação suficiente para tomar uma decisão informada ao verificar um certificado e confiar na informação contida no referido certificado.

Além disso, o verificador reconhecerá que a utilização do Registro e das Listas de Revogação de Certificados (doravante, "os LRCs" ou "as LCRs) da UANATACA, são regidos pela DPC da UANATACA e se comprometerá a cumprir os requisitos técnicos, operacionais e segurança descritas na referida DPC.

1.7.2. Requisitos de verificação de assinatura eletrônica

A verificação será normalmente executada automaticamente pelo software verificador e, em qualquer caso, de acordo com a DPC, com os seguintes requisitos:

- É necessário utilizar software adequado para verificar uma assinatura eletrônica com os algoritmos e comprimentos de chave autorizados no certificado e/ou executar qualquer outra operação criptográfica, e estabelecer a cadeia de certificados na qual se baseia a assinatura eletrônica a ser verificada, uma vez que que a assinatura eletrônica seja verificada usando esta cadeia de certificados.
- É necessário garantir que a cadeia de certificados identificada é a mais adequada para a assinatura eletrónica que está a ser verificada, uma vez que uma assinatura eletrónica pode basear-se em mais do que uma cadeia de certificados, cabendo ao verificador garantir a utilização da cadeia mais adequada. para verificar isso.
- É necessário verificar o estado de revogação dos certificados da cadeia com as informações fornecidas ao Registro UANATACA (com LRCs, por exemplo) para determinar a validade de todos os certificados da cadeia de certificados, pois apenas

um pode ser considerado corretamente verificado. assinatura eletrônica se todos e cada um dos certificados da cadeia estiverem corretos e válidos.

- É necessário garantir que todos os certificados da cadeia autorizam a utilização da chave privada pelo titular do certificado e pelo signatário, uma vez que existe a possibilidade de alguns dos certificados incluírem limites de utilização que impeçam a confiança na assinatura eletrónica que é criada. verificar. Cada certificado da cadeia possui um indicador que se refere às condições de uso aplicáveis, para revisão pelos verificadores.
- É necessário verificar tecnicamente a assinatura de todos os certificados da cadeia antes de confiar no certificado utilizado pelo signatário.

1.7.3. Confie em um certificado não verificado

Se o verificador confiar num certificado não verificado, assumirá todos os riscos derivados desta ação.

1.7.4. Efeito da verificação

Em virtude da correta verificação dos certificados de pessoa física emitidos no DCCF (QSCD), de acordo com este texto informativo, o verificador pode confiar na identificação e, quando aplicável, na chave pública do signatário, dentro das limitações de uso correspondentes, a gerar mensagens criptografadas.

1.7.5. Uso correto e atividades proibidas

O verificador compromete-se a não utilizar qualquer tipo de informação sobre o estado dos certificados ou qualquer outro tipo que tenha sido fornecido pela UANATACA, na realização de qualquer operação proibida pela lei aplicável à referida operação.

O verificador compromete-se a não inspecionar, interferir ou fazer engenharia reversa na implementação técnica dos serviços de certificação pública da UANATACA, sem consentimento prévio por escrito.

Além disso, o verificador compromete-se a não comprometer intencionalmente a segurança dos serviços públicos de certificação da UANATACA.

Os serviços de certificação digital prestados pela UANATACA não foram concebidos nem permitem a utilização ou revenda, como equipamentos de controlo de situações perigosas ou para utilizações que exijam ações à prova de erros, como a operação de instalações nucleares, sistemas de navegação ou comunicação aérea. , sistemas de controle de tráfego aéreo ou sistemas de controle de armas, onde um erro pode causar morte, danos físicos ou graves danos ambientais.

1.7.6. Cláusula de indenização

O terceiro que se baseie no certificado compromete-se a isentar a UANATACA de qualquer dano decorrente de qualquer ação ou omissão que resulte em responsabilidade, dano ou perda, despesas de qualquer espécie, incluindo custos judiciais e de representação legal que possam ser incorridos, para a publicação e uso do certificado, quando ocorrer alguma 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.
- Falta de verificação de todas as medidas de garantia prescritas no DCP ou outros regulamentos aplicáveis.

1.8. Obrigações da UANATACA

1.8.1. Em relação à prestação do serviço de certificação digital

A UANATACA está obrigada a:

a) Emitir, entregar, gerenciar, suspender, reativar, revogar e renovar certificados, de acordo com as instruções fornecidas pelo assinante e/ou signatário, nos casos e pelos motivos descritos na DPC da UANATACA.
b) Executar os serviços com meios técnicos e materiais adequados e com pessoal que reúna as condições de qualificação e experiência estabelecidas na DPC.
c) Cumprir os níveis de qualidade de serviço, de acordo com o estabelecido na DPC, nos aspectos técnicos, operacionais e de segurança.
d) Notificar o subscritor e o signatário, antes da data de expiração dos certificados, da possibilidade de renovação dos mesmos, bem como da suspensão, levantamento desta suspensão ou revogação dos certificados, quando tais circunstâncias ocorrerem.
e) Comunicar aos terceiros que o solicitem o estado dos certificados, de acordo com o estabelecido na DPC para os diferentes serviços de verificação de certificados.

1.8.2. Em relação às verificações de registro

A UANATACA obriga-se a emitir certificados com base nos dados fornecidos pelo assinante, para os quais poderá realizar as verificações que considerar oportunas quanto à identidade e demais informações pessoais e complementares dos assinantes e, quando for o caso, dos signatários.

Estas verificações podem incluir a justificação documental fornecida e quaisquer outros documentos e informações relevantes fornecidos pelo assinante e/ou signatário.

Caso a UANATACA detecte erros nos dados que devem constar dos certificados ou que justifiquem esses dados, poderá efetuar as alterações que julgar necessárias antes da emissão do certificado ou suspender o processo de emissão e gerir o incidente correspondente com o assinante. Caso a UANATACA corrija os dados sem gestão prévia

do incidente correspondente com o assinante, deverá notificar o assinante dos dados finalmente certificados.

A UANATACA reserva-se o direito de não emitir o certificado quando considerar que a justificação documental é insuficiente para a correta identificação e autenticação do assinante e/ou signatário.

As obrigações acima serão suspensas nos casos em que o assinante atue como autoridade de registro e possua os elementos técnicos correspondentes à geração de chaves, emissão de certificados e gravação de dispositivos de assinatura corporativa.

1.8.3. Períodos de conservação

A UANATACA arquiva os registros correspondentes aos pedidos de emissão e revogação de certificados há pelo menos 15 anos.

A UANATACA armazena a informação de registo por um período entre 1 e 15 anos, dependendo do tipo de informação registada, de acordo com o disposto nas suas políticas e procedimentos.

1.9. Garantias limitadas e isenção de garantias

1.9.1. Garantia UANATACA para serviços de certificação digital

A UANATACA garante 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 DPC.
- Que os serviços de revogação e utilização do depósito cumpram todos os requisitos materiais estabelecidos na DPC.

A UANATACA garante 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 repositório, que o certificado foi emitido ao assinante e signatário nele identificado e que o certificado foi aceite.
- Que na aprovação do pedido de certificado e na emissão do certificado foram cumpridos todos os requisitos materiais estabelecidos na DPC.
- 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 qualificado para assinatura contém a informação que um certificado qualificado deve conter, de acordo com o disposto no artigo 28.º do Regulamento (UE) 910/2014, em cumprimento do disposto nos regulamentos técnicos identificados com a referência ETSI EN 319. 411-2.
- 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. Em nenhum caso a UANATACA será responsável por acontecimentos imprevisíveis e em casos de força maior.

1.9.2. Exclusão de garantia

A UANATACA rejeita qualquer outra garantia diferente da anterior que não seja juridicamente exigível.

Especificamente, a UANATACA não garante nenhum software utilizado por qualquer pessoa para assinar, verificar assinaturas, criptografar, descriptografar ou de outra forma utilizar qualquer certificado digital emitido pela UANATACA, exceto nos casos em que haja declaração escrita em contrário.

1.10. Acordos aplicáveis e CPD

1.10.1. Acordos aplicáveis

Os acordos aplicáveis aos certificados são os seguintes:

- Contrato de serviços de certificação, que regula a relação entre a UANATACA e o subscritor dos certificados.
- Condições gerais de serviço incorporadas neste documento.
- Declaração de Práticas de Certificação, que regulamenta a emissão e utilização de certificados.

1.10.2. Declaração de práticas de certificação

Os serviços de confiança da UANATACA são regulados técnica e operacionalmente pela Declaração de Práticas de Certificação (DPC) da UANATACA, pelas suas atualizações posteriores, bem como pela documentação complementar.

A DPC e a documentação operacional são periodicamente modificadas no Cadastro e podem ser consultadas na página da Internet: https://www.uanataca.com .

1.11. Regras de confiança para assinaturas de longa duração

A UANATACA informa aos solicitantes de certificados que não oferece um serviço que garanta a confiabilidade da assinatura eletrônica de um documento ao longo do tempo.

1.12. Política de Privacidade

A UANATACA não pode divulgar e não pode ser forçada a divulgar qualquer informação confidencial relativa a certificados sem um pedido prévio específico de:

a) A pessoa sobre quem a UANATACA tem o dever de manter a informação confidencial, ou
b) Ordem judicial, administrativa ou qualquer outra prevista na legislação vigente.

No entanto, o assinante concorda que determinadas informações, pessoais ou não, fornecidas no pedido de certificado, serão incluídas nos seus certificados e no mecanismo de verificação do estado dos certificados, e que as referidas informações não são confidenciais por imperativo legal.

A UANATACA não transfere os dados fornecidos especificamente para a prestação do serviço de certificação a nenhuma pessoa.

1.13. Política de privacidade

UANATACA possui uma política de privacidade na seção 9.4 da DPC, e regulamentos específicos de privacidade em relação ao processo de registro, à confidencialidade do registro, à proteção do acesso às informações pessoais e ao consentimento do usuário.

Da mesma forma, prevê-se que a documentação que comprova a aprovação do pedido deverá ser conservada e devidamente registrada e com garantias de segurança e integridade por um período de 15 anos a partir do vencimento do certificado, mesmo em caso de perda antecipada de validade devido à revogação.

1.14. Politica de reembolso

A UANATACA não reembolsará em nenhum caso o custo do serviço de certificação.

1.15. Regulamentos aplicáveis e jurisdição competente

As relações com a UANATACA serão regidas pelas disposições do Regulamento (UE) 910/2014 eIDAS, pelas leis espanholas e, especialmente, por todas aquelas que decorrem da sua política de cumprimento.

O foro competente é o indicado na Lei 1/2000, de 7 de janeiro, de Processo Civil.

1.16. Vinculação com a lista de Provedores de Serviços Eletrônicos Confiáveis e Qualificados

http://www.minetur.gob.es/telecomunicaciones/es-es/servicios/firmaelectronica/paginas/prestadores.aspx

1.17. Divisibilidade de cláusulas, sobrevivência, acordo total e notificação

As cláusulas deste texto de divulgação são independentes entre si, razão pela qual, caso alguma cláusula seja considerada inválida ou inaplicável, as restantes cláusulas do PDS continuarão a ser aplicáveis, salvo acordo expresso em contrário entre as partes.

Os requisitos contidos nas seções 9.6.1 (Obrigações e responsabilidade), 8 (Auditoria de conformidade) e 9.3 (Confidencialidade) da DPC UANATACA continuarão em vigor após o término do serviço nos termos nela previstos.

Este texto contém o testamento completo e todos os acordos entre as partes.

As partes notificam-se mutuamente dos factos através de procedimento de correio eletrónico para os seguintes endereços:

- info@uanataca.com, em nome da UANATACA
- O endereço eletrônico, indicado pelo assinante no contrato com a UANATACA.