Texto de Divulgação - PDS (Declaração de Divulgação PKI) da Autoridade Qualificada de Carimbo de Tempo Eletrônico

Control documental

Clasificación de seguridad:	**Público**
Versión:	**2**
Fecha edición:	**11/11/2021**
Fichero:	**PDS - TSA_v2.docx**
Código	**PSC-3.3-**

Estado formal

Preparado por:	**Revisado por:**	**Aprobado por:**
Nombre: Alejandro Grande Fecha: 11/11/2021	Nombre: Albert Borrás Fecha: 12/11/2021	Nombre: Gabriel García Fecha: 16/11/2021

Control de versiones

Versión	Partes que cambian	Descripción cambio	Autor cambio	Fecha cambio
1.0	Original	Creación del documento	DMP	23/06/2017
2	Completo	Revisión del documento respecto de la nueva versión de la Declaración de Prácticas de Certificación. Ajuste de acuerdo con la codificación documental del Sistema de Gestión de la Seguridad de la Información.	AGB	11/11/2021

Índice _

TEXTO DE DIVULGAÇÃO APLICÁVEL À AUTORIDADE QUALIFICADA SELO ELETRÔNICO CERTIFICADO DE CARIMBO DE HORA ELETRÔNICA

Este documento contém as informações essenciais a saber em relação ao serviço de certificação da Entidade Certificadora UANATACA.

Este documento segue a estrutura definida no Anexo A da norma ETSI EN 319 411-1, de acordo com as indicações da secção 4.3.4 da norma ETSI EN 319 412-5.

1. Informação de contato

1.1. Organização responsável

A Entidade Certificadora UANATACA, doravante "UANATACA", é uma iniciativa de:

UANATACA, SA
RUA RIERA DE CAN TODÀ, 24-26, 6º, 1ª
08024 BARCELONA
TELEFONE: 935 272 290

1.2. Contato

Para qualquer dúvida, entre em contato:

UANATACA, SA
RUA RIERA DE CAN TODÀ, 24-26, 6º, 1ª
08024 BARCELONA
TELEFONE: 935 272 290
E-MAIL: INFO@UANATACA.COM

1.3. Contacto para processos de revogação

Para qualquer dúvida, entre em contato:

UANATACA, SA
RUA RIERA DE CAN TODÀ, 24-26, 6º, 1ª
08024 BARCELONA
TELEFONE: 935 272 290
E-MAIL: INFO@UANATACA.COM

2. Tipo e finalidade do certificado

Este certificado possui o seguinte OID:

1.3.6.1.4.1.47286.1.5	De acordo com a hierarquia UANATACA
0.4.0.194112.1. 3	De acordo com a política da UE (QCP-l-qscd)

Os certificados da Autoridade Qualificada de Carimbo da Hora Eletrónico são certificados qualificados de acordo com o artigo 38.º e Anexo III 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 as referências ETSI EN 319 412-3, ETSI EN 319 421 e ETSI EN 319 422.

Estes certificados permitem a assinatura de provas digitais de hora eletrónica.

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. Compromisso com o conteúdo (Compromisso de conteúdo , para desempenhar a função de assinatura eletrônica)
b) No campo “extKeyUsage” está disponível a seguinte indicação de forma ativada:
    a. “timeStamping” para realizar a função de carimbo de data/hora eletrônico.
c) A seguinte declaração aparece no campo “Declarações de certificado qualificado”:
    a. qCCompliance (0.4.0.1862.1.1), que informa que o certificado é emitido como qualificado.
d) O campo “Aviso ao usuário” descreve o uso deste certificado.

2.1. Entidade Emissora de Certificação

Estes certificados são emitidos pela UANATACA, identificados através dos dados acima indicados.

3. Limites de uso de certificados

3.1. Limites de uso direcionados aos signatários

O serviço qualificado de carimbo de hora eletrónico, prestado pela UANATACA, deverá ser utilizado exclusivamente para os usos autorizados no contrato celebrado entre a UANATACA e o ASSINANTE, e que se reproduzem posteriormente (secção "obrigações dos signatários").

O serviço de carimbo de hora eletrônico deverá ser utilizado de acordo com as instruções, manuais ou procedimentos fornecidos pela UANATACA.

Você deve cumprir todas as leis e regulamentos que possam afetar o uso das ferramentas criptográficas que utiliza.

Nenhuma medida de inspeção, alteração ou engenharia reversa poderá ser tomada nos serviços de carimbo eletrônico de data e hora da UANATACA sem autorização prévia e expressa.

3.2. 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 legislação aplicável, especialmente tendo em conta as restrições de importação e exportação existentes em qualquer momento.

Os certificados não podem ser usados para assinar solicitações de emissão, renovação, suspensão ou revogação de certificados, nem para assinar certificados de chave pública de qualquer tipo, nem para assinar listas de revogação de certificados (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 (PDS), 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 do certificados realizados pelo signatário ou por terceiros.

Da mesma forma, qualquer responsabilidade que possa surgir da sua utilização fora dos limites e condições de utilização incluídos neste texto de divulgação, ou nos contratos com assinantes, bem como qualquer outra utilização indevida do mesmo derivado será imputável ao assinante deste documento. seção ou que possa ser interpretado como tal com base na legislação vigente.

4. Obrigações dos assinantes

4.1. Geração de chave

O assinante autoriza a UANATACA a gerar as chaves privada e pública para a emissão deste certificado.

4.2. Solicitação de certificado

O assinante obriga-se a solicitar, quando necessário, estes certificados 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 UANATACA documentação de operações.

4.3. 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 custodiante.

4.4. Obrigações de custódia

O assinante é obrigado a salvaguardar toda a informação gerada na sua atividade como entidade de registo.

Para salvaguardar o código de identificação pessoal ou qualquer suporte técnico fornecido pela UANATACA, as chaves privadas e, se necessário, as especificações de propriedade da UANATACA que são fornecidas.

Em caso de perda ou roubo da chave privada do certificado, ou no caso de se suspeitar que a chave privada perdeu fiabilidade por qualquer motivo, tais circunstâncias deverão ser imediatamente notificadas à UANATACA através do assinante.

4.5. Obrigações de uso correto

O certificado deverá ser utilizado exclusivamente para utilizações autorizadas na DPC e em quaisquer outras instruções, manuais ou procedimentos fornecidos ao assinante.

Você deve cumprir todas as leis e regulamentos que possam afetar seu direito de usar as ferramentas criptográficas utilizadas.

Não poderão ser adotadas medidas para fiscalizar, alterar ou descompilar os serviços de certificação digital prestados.

Além do mais:

a) Que quando for utilizado qualquer certificado, e enquanto o certificado não tiver expirado, não tiver sido suspenso ou revogado, o referido certificado terá sido aceite e estará operacional.

b) Que não atua como entidade certificadora e, portanto, está obrigada 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, seu uso será suspenso imediata e permanentemente.

4.6. Transações proibidas

É indicada a obrigação de não utilizar chaves privadas, certificados ou qualquer outro suporte técnico fornecido pela UANATACA na realização de qualquer transação proibida pela lei aplicável.

Os serviços de certificação digital (e serviços de carimbo eletrônico do tempo) prestados pela UANATACA não foram concebidos nem permitem sua utilização ou revenda como equipamentos de controle de situações perigosas, ou para usos que exijam ações à prova de erros, como a operação de instalações nucleares , sistemas de navegação aérea ou de comunicação, sistemas de controlo de tráfego aéreo ou sistemas de controlo de armas, nos quais um erro pode causar diretamente a morte, danos físicos ou danos ambientais graves.

5. Obrigações dos verificadores

5.1. 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.

5.2. Requisitos de verificação de carimbo de data/hora

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 o software apropriado para verificar um carimbo de data/hora 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 o carimbo de data/hora a ser verificado, uma vez que este é verificado usando esta cadeia de certificados.

- É necessário garantir que a cadeia de certificados identificada é a mais adequada para o carimbo temporal que está sendo verificado, uma vez que um carimbo temporal pode ser baseado em mais de uma cadeia de certificados, sendo decisão do verificador garantir a utilização da cadeia mais adequada. para verificação.

- 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. carimbo de data / hora se cada certificado da cadeia estiver correto e atual.

- É necessário garantir que todos os certificados da cadeia autorizam a utilização da chave privada pelo titular do certificado, uma vez que existe a possibilidade de alguns dos certificados incluírem limites de utilização que impedem a confiança no carimbo temporal que é verificado. 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 para carimbo de data/hora eletrônico.

5.3. Confie em um certificado não verificado

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

5.4. 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 públicos de carimbo temporal eletrônico ou certificação da UANATACA, sem consentimento prévio por escrito.

Além disso, o verificador compromete-se a não comprometer intencionalmente a segurança dos serviços públicos de carimbo de data/hora eletrônico ou certificação da UANATACA.

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

5.5. 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.

A UANATACA não será responsável em nenhum caso por qualquer perda de informação criptografada que não possa ser recuperada.

6. Obrigações da UANATACA

6.1. Em relação à disponibilização de certificação digital

A UANATACA está obrigada a:

a) Emitir, entregar, gerir, suspender, revogar e renovar certificados, de acordo com as instruções fornecidas pelo assinante, 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 assinante, com antecedência, sobre a data de vencimento dos certificados.

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.

6.2. 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.

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 do domínio.

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.

6.3. 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.

7. Garantias limitadas e isenção de garantias

7.1. Garantia UANATACA para serviços de certificação digital

A UANATACA garante ao assinante:

- Que não existem erros factuais na informação contida nos certificados, conhecidos ou cometidos pela Entidade 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 domínio 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 contém as informações que um certificado de selo eletrônico qualificado deve conter, de acordo com o Anexo III do Regulamento UE 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014, e com as indicações adicionais para a criação de selo eletrônico qualificado carimbos temporais nos termos do artigo 42.º deste mesmo Regulamento.

- Que, caso sejam geradas as chaves privadas do assinante, a sua confidencialidade seja mantida durante o processo.

- A responsabilidade da Entidade Certificadora, com os limites estabelecidos. Em nenhum caso a UANATACA será responsável por acontecimentos imprevisíveis e em casos de força maior.

7.2. 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.

8. Acordos e políticas

8.1. Acordos aplicáveis

Os acordos aplicáveis a este certificado são os seguintes:

- Contrato de serviços de certificação, que regula a relação entre a UANATACA e a empresa subscritora dos certificados.

- Condições gerais de serviço incorporadas no texto de divulgação do certificado ou PDS.

- DPC, que regulamenta a emissão e utilização de certificados.

8.2. DPC

Os serviços de certificação e carimbo temporal da UANATACA são regulados técnica e operacionalmente pela DPC da UANATACA, pelas suas atualizações posteriores, bem como por 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 .

8.3. 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 em vigor.

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.

8.4. 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 comprove 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, inclusive tudo em caso de perda antecipada de validade. por revogação. .

8.5. Politica de reembolso

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

8.6. Lei aplicável e jurisdição competente

As relações com a UANATACA serão regidas pela legislação espanhola sobre serviços de confiança em vigor em cada momento, bem como pela legislação civil e comercial na medida do aplicável.

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

Em caso de desacordo entre as partes, as partes tentarão uma resolução amigável prévia. Para o efeito, as partes deverão enviar uma comunicação à UANATACA por qualquer meio que deixe registo para o endereço de contacto indicado no ponto de contacto deste PDS.

Caso as partes não cheguem a acordo a este respeito, qualquer uma delas poderá submeter o conflito à jurisdição civil, sujeito aos Tribunais da sede da UANATACA.

8.7. Acreditações e selos de qualidade

Nenhuma estipulação.

8.8. Link com a lista de fornecedores

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

8.9. 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 "Obrigações e Responsabilidade", "Auditoria de Conformidade" e "Confidencialidade" da DPC UANATACA continuarão em vigor após o término do serviço.

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

As partes notificam-se mutuamente dos factos através de procedimento de envio de e-mail para o endereço info@uanataca.com