Texto de Divulgação (PDS) do Certificado da Autoridade Qualificada de Selagem de Tempo Eletrônico

Índice

Certificado de selo eletrônico de Autoridade Qualificada de Selagem de Tempo Eletrônico

TEXTO DIVULGATIVO - PDS

Este documento contém as informações essenciais a conhecer em relação ao serviço de certificação da Entidade de Certificação ESFIRMA.

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

Informação geral

Controle documental

Classificação de segurança:	Público
Entidade de destino:	ESFIRMA
Versão:	1.6

Controle de versões

Versão	Partes que mudam	Descrição da mudança	Autor da mudança	Data da mudança
1.0	Original	Criação do documento	esFIRMA	7/05/2017
1.4		Subsanaciones	esFIRMA	7/06/2017
1.5	1.1 -1.3 8.6	Mudança de denominação	esFIRMA	6/11/2017
1.6	1.3	Adiciona-se referência ao site da esFIRMA.	esFIRMA	21/04/2023

1. Informação de contato

1.1. Organização responsável

A Entidade de Certificação ESFIRMA, doravante "ESFIRMA", é uma iniciativa de:

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (ESFIRMA) CALLE BARI 39 (EDIF. BINARY BUILDING) 50197 - ZARAGOZA (+34) 976300110

1.2. Contato

Para qualquer consulta, dirijam-se a:

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (ESFIRMA) CALLE BARI 39 (EDIF. BINARY BUILDING) 50197 - ZARAGOZA (+34) 976300110

1.3. Contato para processos de revogação

O processo para solicitar a revogação de um certificado pode ser consultado em . Para qualquer outra consulta a respeito, dirijam-se a:www.esfirma.com

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (ESFIRMA) CALLE BARI 39 (EDIF. BINARY BUILDING) 50197 - ZARAGOZA (+34) 976300110

2. Tipo e finalidade do certificado

Este certificado possui o seguinte OID:

1.3.6.1.4.1.47281.1.5.2	De acordo com a hierarquia de esFIRMA
0.4.0.194112.1.1	De acordo com a política UE (QCP-l)

Os certificados de Autoridade de Selagem Qualificada de Tempo Eletrônico são certificados qualificados de acordo com o artigo 38 e o Anexo III do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014 e cumprem o disposto pelas normas técnicas identificadas com as referências ETSI EN 319 412-3, ETSI EN 319 421 e ETSI EN 319 422.

Esses certificados permitem a assinatura de evidências digitais de tempo eletrônico.

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

a) O campo "uso da chave" está ativado, permitindo-nos realizar as seguintes funções:
    a. Compromisso com o conteúdo (Compromisso de conteúdo, para realizar a função de assinatura eletrônica)
b) No campo "extKeyUsage" está disponível de forma ativada a indicação:
    a. timeStamping" para realizar a função de selagem de tempo eletrônico.
c) No campo "Qualified Certificate Statements" aparece a seguinte declaração:
    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 de Certificação emissora

Esses certificados são emitidos pela ESFIRMA, identificada pelos dados indicados anteriormente.

3. Limites de uso do certificado

3.1. Limites de uso direcionados aos signatários

Deve-se utilizar o serviço de selagem qualificada de tempo eletrônico, fornecido pela ESFIRMA exclusivamente para os usos autorizados no contrato assinado entre ESFIRMA e o ASSINANTE, e que são reproduzidos posteriormente (seção "obrigações dos signatários").

Deve-se utilizar o serviço de selagem de tempo eletrônico de acordo com as instruções, manuais ou procedimentos fornecidos por ESFIRMA.

Deve-se cumprir qualquer lei e regulamentação que possa afetar o uso das ferramentas criptográficas empregadas.

Não se podem adotar medidas de inspeção, alteração ou engenharia reversa dos serviços de selagem de tempo eletrônico da ESFIRMA, sem prévia permissão expressa.

3.2. Limites de uso direcionados aos verificadores

Os certificados são usados para sua própria função e finalidade estabelecida, sem poder ser usados em outras funções e com outras finalidades.

Da mesma forma, os certificados devem ser usados apenas de acordo com a lei aplicável, especialmente levando em consideração as restrições de importação e exportação existentes em cada momento.

Os certificados não podem ser utilizados para assinar solicitações de emissão, renovação, suspensão ou revogação de certificados, nem para assinar certificados de chave pública de qualquer tipo, nem assinar listas de revogação de certificados (LRC).

Os certificados não foram projetados, não podem ser destinados e não é autorizado o seu uso ou revenda como equipamentos de controle de situações perigosas ou para usos que requerem ações à prova de falhas, como o funcionamento de instalações nucleares, sistemas de navegação ou comunicações aéreas, ou sistemas de controle de armamento, onde uma falha possa diretamente resultar em morte, lesões pessoais ou danos ambientais graves.

Deve-se levar em consideração os limites indicados nos diversos campos dos perfis de certificados, visíveis no site da ESFIRMA https://www.esfirma.com

O uso de certificados digitais em operações que contrariam este texto de divulgação (PDS) ou os contratos com os assinantes é considerado uso indevido para fins legais apropriados, isentando assim a ESFIRMA, de acordo com a legislação em vigor, de qualquer responsabilidade por este uso indevido dos certificados realizados pelo signatário ou por qualquer terceiro.

Da mesma forma, o assinante será responsável por qualquer responsabilidade que possa resultar do uso fora dos limites e condições de uso estabelecidos neste texto de divulgação, ou nos contratos com os assinantes, bem como de qualquer outro uso indevido do mesmo decorrente desta seção ou que possa ser interpretado como tal de acordo com a legislação em vigor.

4. Obrigações dos assinantes

4.1. Geração de chaves

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

4.2. Solicitação de certificados

O assinante compromete-se a fazer os pedidos, quando necessário, desses certificados de acordo com o procedimento e, se necessário, os componentes técnicos fornecidos pela ESFIRMA, em conformidade com o estabelecido na declaração de práticas de certificação (DPC) e na documentação de operações da ESFIRMA.

4.3. Obrigações de informação

O assinante é responsável por garantir que todas as informações incluídas em seu pedido de certificado sejam precisas, completas para a finalidade do certificado e atualizadas a todo momento.

O assinante deve informar imediatamente a ESFIRMA:

- De qualquer inexatidão detectada no certificado após sua emissão.
- Das mudanças que ocorram nas informações fornecidas e/ou registradas para a emissão do certificado.
- Da perda, roubo, furto ou qualquer outro tipo de perda de controle da chave privada pelo guardião.

4.4. Obrigações de custódia

O assinante compromete-se a guardar todas as informações geradas em sua atividade como entidade de registro.

Custodiar o código de identificação pessoal ou qualquer suporte técnico fornecido pela ESFIRMA, as chaves privadas e, se necessário, as especificações de propriedade da ESFIRMA que lhe forem fornecidas.

Em caso de perda ou roubo da chave privada do certificado, ou caso se suspeite que a chave privada perdeu confiabilidade por qualquer motivo, essas circunstâncias devem ser notificadas imediatamente à ESFIRMA pelo assinante.

4.5. Obrigações de uso correto

Deve-se utilizar o certificado exclusivamente para os usos autorizados na DPC e em qualquer outra instrução, manual ou procedimento fornecido ao assinante.

Deve cumprir qualquer lei e regulamentação que possa afetar seu direito de uso das ferramentas criptográficas empregadas.

Não serão adotadas medidas de inspeção, alteração ou descompilação dos serviços de certificação digital prestados.

Além disso:

a) Que quando qualquer certificado for utilizado, e enquanto o certificado não tiver expirado, não tiver sido suspenso ou revogado, esse certificado será aceito e estará operacional.

b) Que não atua como entidade de certificação e, portanto, se compromete a não utilizar as chaves privadas correspondentes às chaves públicas contidas nos certificados com o propósito de assinar qualquer certificado.

c) Que em caso de comprometimento da chave privada, seu uso fica imediata e permanentemente suspenso.

4.6. Transações proibidas

Indica-se a obrigação de não utilizar as chaves privadas, os certificados ou qualquer outro suporte técnico fornecido pela ESFIRMA na realização de qualquer transação proibida pela lei aplicável.

Os serviços de certificação digital (e os de selagem de tempo eletrônico) fornecidos pela ESFIRMA não foram projetados nem permitem sua utilização ou revenda como equipamentos de controle de situações perigosas, ou para usos que exijam ações à prova de falhas, como a operação de instalações nucleares, sistemas de navegação ou comunicação aérea, sistemas de controle de tráfego aéreo ou sistemas de controle de armamento, nos quais um erro poderia diretamente causar a morte, danos físicos ou danos ambientais graves.

5. Obrigações dos verificadores

5.1. Decisão informada

ESFIRMA informa ao verificador que tem acesso a informações suficientes para tomar uma decisão informada no momento de verificar um certificado e confiar nas informações contidas nesse certificado.

Adicionalmente, o verificador reconhecerá que o uso do Registro e das Listas de Revogação de Certificados (doravante, "as LRCs" ou "as CRLs") da ESFIRMA, são regidos pela DPC da ESFIRMA e se comprometerá a cumprir os requisitos técnicos, operacionais e de segurança descritos na mencionada DPC.

5.2. Requisitos de verificação do selo de tempo

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

- É necessário utilizar o software apropriado para a verificação de um selo de tempo com os algoritmos e comprimentos de chaves autorizados no certificado e/ou executar qualquer outra operação criptográfica, e estabelecer a cadeia de certificados na qual se baseia o selo de tempo a ser verificado, uma vez que este é verificado utilizando essa cadeia de certificados.

- É necessário garantir que a cadeia de certificados identificada seja a mais adequada para o carimbo de tempo que está sendo verificado, pois um carimbo de tempo pode se basear em mais de uma cadeia de certificados, e é decisão do verificador garantir o uso da cadeia mais adequada para verificá-la.

- É necessário verificar o estado de revogação dos certificados da cadeia com as informações fornecidas ao Registro de ESFIRMA (com LRCs, por exemplo) para determinar a validade de todos os certificados da cadeia de certificados, pois apenas pode ser considerado corretamente verificado um selo de tempo se todos e cada um dos certificados da cadeia forem corretos e estiverem em vigor.

- É necessário garantir que todos os certificados da cadeia autorizam o uso da chave privada pelo assinante do certificado, pois existe a possibilidade de que alguns dos certificados incluam limites de uso que impeçam a confiança no selo de tempo que é verificado. Cada certificado da cadeia possui um indicador que faz referência 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 o selo de tempo eletrônico.

5.3. Confiança em um certificado não verificado

Se o verificador confiar em um certificado não verificado, assumirá todos os riscos decorrentes dessa ação.

5.4. Uso correto e atividades proibidas

O verificador compromete-se a não utilizar nenhum tipo de informação sobre o estado dos certificados ou qualquer outro tipo fornecido pela ESFIRMA, na realização de qualquer transação proibida pela lei aplicável à referida transação.

O verificador compromete-se a não inspecionar, interferir ou realizar engenharia reversa da implementação técnica dos serviços públicos de selagem de tempo eletrônico ou de certificação da ESFIRMA, sem prévio consentimento por escrito.

Adicionalmente, o verificador se obriga a não comprometer intencionalmente a segurança dos serviços públicos de selagem de tempo eletrônico e de certificação da ESFIRMA.

Os serviços de selagem de tempo eletrônico e de certificação digital fornecidos pela ESFIRMA não foram projetados nem permitem a utilização ou revenda, como equipamentos de controle de situações perigosas ou para usos que exijam ações à prova de falhas, como a operação de instalações nucleares, sistemas de navegação ou comunicação aérea, sistemas de controle de tráfego aéreo, ou sistemas de controle de armamento, onde um erro poderia causar a morte, danos físicos ou danos ambientais graves.

5.5. Cláusula de indenização

O terceiro que confia no certificado compromete-se a manter a ESFIRMA isenta de qualquer dano decorrente de qualquer ação ou omissão que resulte em responsabilidade, dano ou perda, despesa de qualquer tipo, incluindo as judiciais e de representação legal em que possa incorrer, pela publicação e uso do certificado, quando ocorrer uma das seguintes causas:

- Incumprimento das obrigações do terceiro que confia no certificado.
- Confiança temerária em um certificado, de acordo com as circunstâncias.

- Falta de verificação do estado de um certificado, para determinar se ele não está suspenso ou revogado.
- Falta de verificação da totalidade das medidas de garantia prescritas na DCP ou restante das normas de aplicação.

ESFIRMA não se responsabilizará em nenhum caso por qualquer perda de informações criptografadas que não possam ser recuperadas.

6. Obrigações da ESFIRMA

6.1. Em relação à prestação de certificação digital

ESFIRMA se compromete a:

a) Emitir, entregar, administrar, suspender, revogar e renovar certificados, de acordo com as instruções fornecidas pelo assinante, nos casos e pelos motivos descritos na DPC da ESFIRMA.

b) Executar os serviços com os meios técnicos e materiais adequados e com pessoal que cumpra as condições de qualificação e experiência estabelecidas na DPC.

c) Cumprir os níveis de qualidade do serviço, em conformidade com o estabelecido na DPC, nos aspectos técnicos, operacionais e de segurança.

d) Notificar o assinante, com antecedência, a data de expiração dos certificados.

e) Comunicar às terceiras pessoas que o solicitarem, 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 do registro

ESFIRMA se compromete a emitir certificados com base nos dados fornecidos pelo assinante, podendo realizar as verificações que considerar apropriadas.

No caso em que a ESFIRMA detectar erros nos dados que devem ser incluídos nos certificados ou que justifiquem esses dados, poderá realizar as alterações que considerar necessárias antes de emitir o certificado ou suspender o processo de emissão e gerir com o assinante o incidente correspondente. Caso a ESFIRMA corrija os dados sem gestão prévia do incidente correspondente com o assinante, deverá notificar os dados finalmente certificados ao assinante.

ESFIRMA reserva-se o direito de não emitir o certificado, quando considerar que a justificação documental seja insuficiente para a correta identificação e autenticação do assinante e/ou do domínio.

As obrigações anteriores ficarão suspensas nos casos em que o assinante atuar como autoridade de registro e possuir os elementos técnicos correspondentes à geração de chaves, emissão de certificados e gravação de dispositivos de assinatura corporativos.

6.3. Períodos de conservação

ESFIRMA arquiva os registros correspondentes às solicitações de emissão e revogação de certificados por pelo menos 15 anos.

ESFIRMA armazena as informações dos logs por um período entre 1 e 15 anos, dependendo do tipo de informação registrada.

7. Garantias limitadas e rejeição de garantias

7.1. Garantia da ESFIRMA pelos serviços de certificação digital

ESFIRMA garante ao assinante:

- Que não há erros de fato nas informações contidas nos certificados, conhecidos ou realizados pela Entidade de Certificação.

- Que não há erros de fato nas informações contidas nos certificados, devido à falta de diligência adequada na gestão do pedido de certificado ou na sua criação.

- Que os certificados cumprem com todos os requisitos materiais estabelecidos na DPC.

- Que os serviços de revogação e o uso do depósito cumprem todos os requisitos materiais estabelecidos na DPC.

ESFIRMA garante ao terceiro que confia no certificado:

- Que a informação contida ou incorporada por referência no certificado está correta, exceto quando indicado o contrário.

- Em caso de certificados publicados no depósito, que o certificado foi emitido ao assinante e domínio identificado no mesmo e que o certificado foi aceito.

- Que na aprovação do pedido de certificado e na emissão do certificado, todos os requisitos materiais estabelecidos na DPC foram cumpridos.

- A rapidez e segurança na prestação dos serviços, especialmente dos serviços de revogação e depósito.

Adicionalmente, ESFIRMA garante ao assinante e a terceiros que confiam no certificado:

- Que o certificado contém as informações que devem constar em um certificado qualificado de selo eletrônico, 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 selos qualificados de tempo de acordo com o artigo 42 deste mesmo Regulamento.

- Que, no caso de gerar as chaves privadas do assinante, mantém-se a confidencialidade durante o processo.

- A responsabilidade da Entidade de Certificação, dentro dos limites estabelecidos. Em nenhum caso, a ESFIRMA será responsável por caso fortuito ou força maior.

7.2. Exclusão da garantia

ESFIRMA rejeita qualquer outra garantia diferente da anterior que não seja legalmente exigível.

Especificamente, ESFIRMA não garante nenhum software utilizado por qualquer pessoa para assinar, verificar assinaturas, criptografar, descriptografar ou utilizar de outra forma qualquer certificado digital emitido pela ESFIRMA, exceto nos casos em que haja uma declaração escrita em sentido 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 ESFIRMA e a empresa assinante dos certificados.

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

- DPC, que regula a emissão e utilização dos certificados.

8.2. DPC

Os serviços de certificação e de carimbo de tempo da ESFIRMA são regulados tecnicamente e operacionalmente pela DPC da ESFIRMA, pelas suas atualizações posteriores, bem como por documentação complementar.

A DPC e a documentação de operações são modificadas periodicamente no Registro e podem ser consultadas na página da Internet: https://www.esfirma.com

8.3. Política de privacidade

ESFIRMA não pode divulgar nem pode ser obrigada a divulgar informações confidenciais em relação a certificados sem um pedido específico prévio que provenha de:

a) A pessoa em relação à qual a ESFIRMA tem o dever de manter as informações confidenciais, ou

b) Uma ordem judicial, administrativa ou qualquer outra prevista na legislação vigente.

No entanto, o assinante aceita que determinadas informações, pessoais e de outros tipos, fornecidas no pedido de certificados, sejam incluídas nos seus certificados e no

mecanismo de verificação do estado dos certificados, e que as informações mencionadas não sejam confidenciais, por imperativo legal.

ESFIRMA não cede a nenhuma pessoa os dados entregues especificamente para a prestação do serviço de certificação.

8.4. Política de privacidade

ESFIRMA possui uma política de privacidade na seção 9.4 da DPC e regulamentação específica de privacidade em relação ao processo de registro, confidencialidade do registro, proteção do acesso às informações pessoais e consentimento do usuário.

Além disso, considera-se que a documentação justificativa da aprovação do pedido deve ser preservada e devidamente registrada, com garantias de segurança e integridade durante o prazo de 15 anos a partir do vencimento do certificado, mesmo em caso de perda antecipada de validade por revogação.

8.5. Política de reembolso

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

8.6. Lei aplicável e jurisdição competente

As relações com a ESFIRMA serão regidas pela lei espanhola em matéria de serviços de confiança vigente em cada momento, bem como pela legislação civil e comercial no que for aplicável.

A jurisdição competente é a indicada na Lei 1/2000, de 7 de janeiro, de Julgamento Civil.

Em caso de discrepância entre as partes, as partes tentarão a resolução amigável prévia. Para esse fim, as partes devem enviar uma comunicação à esFIRMA por qualquer meio

que deixe registro no endereço de contato indicado no ponto de informação de contato desta PDS.

Se as partes não chegarem a um acordo a respeito, qualquer uma delas poderá submeter o conflito à jurisdição civil, sujeito aos Tribunais do domicílio social deESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA.

8.7. Acreditações e selos de qualidade

Sem estipulação.

8.8. Vinculação com a lista de prestadores

https://sedeaplicaciones.minetur.gob.es/Prestadores/

8.9. Divisibilidade das cláusulas, sobrevivência, acordo integral e notificação

As cláusulas do presente texto de divulgação são independentes entre si, motivo pelo qual, se qualquer cláusula for considerada inválida ou inaplicável, o restante das cláusulas das PDS continuarão sendo aplicáveis, exceto acordo expresso em contrário das partes.

Os requisitos contidos nas seções 9.6.1 (Obrigações e responsabilidade), 8 (Auditoria de conformidade) e 9.3 (Confidencialidade) da DPC da ESFIRMA continuarão vigentes após a terminação do serviço.

Este texto contém a vontade completa e todos os acordos entre as partes.

As partes notificam-se mutuamente de fatos através de um procedimento de envio de email para o endereço info@esfirma.com