Texto de Divulgação (PDS) dos certificados emitidos às Administrações Públicas

Índice

1.1. CONTROLO DE DOCUMENTOS 4
1.2. CONTROLO DE VERSÕES 4

2. INFORMAÇÃO 7

1.1. ORGANIZAÇÃO RESPONSÁVEL 7
1.2. CONTACTO 7
1.3. CONTACTO PARA PROCESSOS DE REVOGAÇÃO 7

3. TIPO E FINALIDADE DO CERTIFICADO 8

3.1. CERTIFICADOS QUALIFICADOS DE FUNCIONÁRIO PÚBLICO 8
3.2. CERTIFICADOS DE FUNCIONÁRIO PÚBLICO COM PSEUDÓNIMO 8
3.3. CERTIFICADOS DE CARTÃO 8
3.4. CERTIFICADOS CLOUD 9
3.5. CERTIFICADOS PARA AUTENTICAÇÃO 9
3.6. CERTIFICADOS DE ASSINATURA AVANÇADA 9
3.7. CERTIFICADOS PARA ASSINATURA QUALIFICADA 9
3.8. CERTIFICADOS ELETRÓNICOS QUALIFICADOS 9
3.9. CERTIFICADOS AVANÇADOS DE SELO 10
3.10. TIPOS DE CERTIFICADOS 10
3.11. AUTORIDADE CERTIFICADORA EMITIDORA 11
3.12. VALIDAÇÃO DE CERTIFICADOS 11

4. LIMITES DE UTILIZAÇÃO DE CERTIFICADOS 13

4.1. LIMITES DE UTILIZAÇÃO DIRECIONADOS A SINALIZADORES 13
4.2. LIMITES DE UTILIZAÇÃO DIRECIONADOS PARA VERIFICADORES 13

5. OBRIGAÇÕES DOS SUBSCRITORES 15

5.1. GERAÇÃO DE CHAVES 15
5.2. PEDIDO DE CERTIFICADOS 15
5.3. VERACIDADE DA INFORMAÇÃO 15
5.4. OBRIGAÇÕES DE CUSTÓDIA 16

6. OBRIGAÇÕES DOS SIGNATÁRIOS E CRIADORES DE SELOS 17

6.1. OBRIGAÇÕES DE CUSTÓDIA 17
6.2. OBRIGAÇÕES DE USO CORRETO 17
6.3. TRANSAÇÕES PROIBIDAS 18

7. OBRIGAÇÕES DOS VERIFICADORES 19

7.1. DECISÃO INFORMADA 19
7.2. REQUISITOS DE VERIFICAÇÃO DE ASSINATURA 19
7.3. CONFIAR NUM CERTIFICADO NÃO VERIFICADO 20

7.4. EFEITO DA VERIFICAÇÃO 20
7.5. USO ADEQUADO E ATIVIDADES PROIBIDAS 20
7.6. CLÁUSULA DE INDEMNIZAÇÃO 21

8. OBRIGAÇÕES DA ESFIRMA 22

8.1. NO QUE DIZ RESPEITO À PRESTAÇÃO DE CERTIFICAÇÃO DIGITAL 22
8.2. EM RELAÇÃO ÀS VERIFICAÇÕES DE REGISTO 22
8.3. PERÍODOS DE RETENÇÃO 23

9. GARANTIAS LIMITADAS E RENÚNCIAS DE GARANTIAS 24

9.1. GARANTIA ESFIRMA PARA SERVIÇOS DE CERTIFICAÇÃO DIGITAL 24
9.2. EXCLUSÃO DA GARANTIA 25

10. ACORDOS E CPO APLICÁVEIS 27

10.1. ACORDOS APLICÁVEIS 27
10.2. CPD 27

11. POLÍTICA DE PRIVACIDADE 28

12. POLÍTICA DE PRIVACIDADE 29

13. POLÍTICA DE REEMBOLSO 30

14. LEGISLAÇÃO APLICÁVEL, JURISDIÇÃO COMPETENTE E REGIME DE REIVINDICAÇÕES E LITÍGIOS 31

14.1. ACREDITAÇÕES E SELOS DE QUALIDADE 31
14.2. LIGAÇÃO PARA A LISTA DE PRESTADORES 31
14.3. SEPARABILIDADE DOS TERMOS, SOBREVIVÊNCIA, ACORDO TOTAL E NOTIFICAÇÃO 32

TEXTO INFORMATIVO - PDS

Este documento contém a informação essencial a conhecer relativamente ao serviço de certificação do Organismo de Certificação ESFIRMA.

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

1.1. Controlo de documentos

Classificação de Segurança	PÚBLICO
Versão	2.2

1.2. Controlo de Versões

Versão	Alterações	Descrição	Autor	Data
1.0	Original	Criação de documentos	esFIRMA	28/04/2016
1.4		Correções	esFIRMA	07/06/2017
1.5		Alteração do nome e referência aos regulamentos	esFIRMA	06/11/2017
2.0		Inclusão de todos os certificados referentes ao Governo Geral Espanhol	esFIRMA	03/06/2020
2.1		Revisão da Lei 6/2020	esFIRMA	08/04/2021

2.2	(1.3)	Foi adicionada uma referência ao site da esFIRMA.	esFIRMA	21/04/2023
2.3		Acrescentou referência ao procedimento de resolução de litígios	esFIRMA	15/07/2026

2. Informação

2.1. Organização responsável

O Organismo de Certificação ESFIRMA, doravante designado "ESFIRMA", é uma iniciativa de:

SERVIÇOS PÚBLICOS PARA A ADMINISTRAÇÃO SA (ESFIRMA) CALLE BARI 39 (EDIF. EDIFÍCIO BINÁRIO) 50197 - ZARAGOZA (+34) 976300110

2.2. Contacto

Para quaisquer questões, por favor contacte:

SERVIÇOS PÚBLICOS PARA A ADMINISTRAÇÃO SA (ESFIRMA) CALLE BARI 39 (EDIF. EDIFÍCIO BINÁRIO) 50197 - ZARAGOZA (+34) 976300110

2.3. Contacto para processos de revogação

O processo para solicitar a revogação de um certificado pode ser encontrado em www.esfirma.com. Para quaisquer questões adicionais, por favor contacte:

SERVIÇOS PÚBLICOS PARA A ADMINISTRAÇÃO SA (ESFIRMA) CALLE BARI 39 (EDIF. EDIFÍCIO BINÁRIO) 50197 - ZARAGOZA (+34) 976300110

3. Tipo e finalidade do certificado

3.1. Certificados qualificados de funcionário público

Estes certificados são qualificados de acordo com o artigo 28 e o anexo I do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, e cumprem as disposições dos regulamentos técnicos identificados com a referência ETSI EN 319 411-2.

Estes certificados permitem que os seus titulares sejam identificados como pessoal ao serviço da Administração Pública, ligando-os a esta, de acordo com os requisitos estabelecidos no Artigo 43 da Lei 40/2015, de 1 de outubro, sobre o Regime Jurídico do Setor Público, para a assinatura eletrónica do pessoal ao serviço das Administrações Públicas.

3.2. Certificados de funcionário público com pseudónimo

Estes certificados permitem identificar os seus titulares como pessoal ao serviço da Administração Pública, ligando-os a esta, conforme previsto pelo Artigo 43.2 da Lei 40/2015, de 1 de outubro, sobre o Regime Jurídico do Setor Público, para a assinatura eletrónica de pessoal ao serviço das Administrações Públicas, pessoal que, por razões de segurança pública, só deve ser identificado pelo número de identificação profissional ou outro pseudónimo de um funcionário público, conforme indicado no Anexo I, parágrafo c) do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014, e no Artigo 6.1.a) da Lei 6/2020, de 11 de novembro, que regula certos aspetos dos serviços fiduciários eletrónicos.

3.3. Certificados de cartão

Os certificados que utilizam cartão funcionam com um dispositivo qualificado de criação de assinatura eletrónica, de acordo com o Anexo II do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014.

3.4. Certificados Cloud

Estes certificados são geridos centralmente.

3.5. Certificados para autenticação

Os certificados com a função de identificação garantem a identidade do assinante e do signatário.

3.6. Certificados de Assinatura Avançada

Certificados com função de assinatura permitem a geração da "assinatura eletrónica avançada" baseada num certificado qualificado sem a participação conjunta de um dispositivo qualificado de criação de assinatura.

3.7. Certificados para assinatura qualificada

Certificados com função de assinatura permitem a geração da "assinatura eletrónica qualificada"; ou seja, a assinatura eletrónica avançada baseada num certificado qualificado quando gerada utilizando um dispositivo qualificado, portanto, de acordo com as disposições do Artigo 25.2 do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, terá efeito legal equivalente ao de uma assinatura manuscrita.

3.8. Certificados eletrónicos qualificados

Estes certificados são 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 as disposições dos regulamentos técnicos identificados com a referência ETSI EN 319 411-2.

Estes certificados permitem que os seus titulares sejam identificados como Administrações Públicas, de acordo com os requisitos estabelecidos no Artigo 40 da Lei 40/2015, de 1 de outubro, sobre o Regime Jurídico do Setor Público, que incluirá o número de identificação fiscal e o respetivo nome, bem como, quando aplicável, a identidade do titular no caso de selos eletrónicos dos órgãos administrativos.

3.9. Certificados Avançados de Selo

Os certificados com função de assinatura permitem a geração do "selo eletrónico avançado" baseado num certificado qualificado sem a intervenção conjunta de um dispositivo qualificado de criação de assinatura.

3.10. Tipos de certificados

Certificado	**Apoio**	**Perfil**	**OIDs**
Funcionário público de alto nível, para assinatura	Cartão	Assinatura	● 1.3.6.1.4.1.47281.1.1.1 ● 0.4.0.194112.1.2 ● 2.16.724.1.3.5.7.1
Funcionário público de nível médio, para assinatura	HSM Centralizado	Assinatura	● 1.3.6.1.4.1.47281.1.1.4 ● 0.4.0.194112.1.0 ● 2.16.724.1.3.5.7.2
Funcionário público de alto nível, para autenticação	*Cartão*	*Autent*	● *1.3.6.1.4.1.47281.1.1.5* ● *0.4.0.2042.1.2* ● *2.16.724.1.3.5.7.1*

Certificado	Apoio	Perfil	OIDs
Funcionário público com pseudónimo de alto nível, para assinatura	Cartão	Assinatura	• 1.3.6.1.4.1.47281.1.3.1 • 0.4.0.194112.1.2 • 2.16.724.1.3.5.4.1
Funcionário público com pseudónimo de nível médio, para assinatura	HSM Centralizado	Assinatura	• 1.3.6.1.4.1.47281.1.3.4 • 0.4.0.194112.1.0 • 2.16.724.1.3.5.4.2
Funcionário público com pseudónimo de alto nível, para autenticação	*Cartão*	*Autent*	• *1.3.6.1.4.1.47281.1.3.5* • *0.4.0.2042.1.2* • *2.16.724.1.3.5.4.1*

Certificado	Apoio	Perfil	OIDs
Selo eletrónico, nível médio	Software	Assinatura	• 1.3.6.1.4.1.47281.1.2.2 • 0.4.0.194112.1.2 • 2.16.724.1.3.5.6.2
Selo eletrónico, nível médio, centralizado	HSM Centralizado	Assinatura	• 1.3.6.1.4.1.47281.1.2.4 • 0.4.0.194112.1.2 • 2.16.724.1.3.5.6.2

3.11. Autoridade Certificadora Emitidora

Estes certificados são emitidos pela ESFIRMA, identificados pelos dados indicados acima.

3.12. Validação de certificados

As listas de certificados revogados e serviços OCSP podem ser encontradas no site da esFIRMA e nos URLs indicados em cada um dos certificados.

4. Limites de utilização dos certificados

4.1. Limites de utilização direcionados a sinalizadores

O signatário e o criador dos selos devem utilizar o serviço de certificação fornecido pela esFIRMA exclusivamente para os usos autorizados no contrato assinado entre a esFIRMA e o ASSINANTE, e que são reproduzidos abaixo.

Da mesma forma, o signatário e o criador dos selos são obrigados a utilizar o serviço de certificação digital de acordo com as instruções, manuais ou procedimentos fornecidos pela esFIRMA.

O signatário e o criador do selo devem cumprir quaisquer leis e regulamentos que possam afetar o seu direito de utilizar as ferramentas criptográficas que utilizam.

O signatário e o criador do selo não podem adotar medidas de inspeção, alteração ou engenharia reversa dos serviços digitais de certificação da esFIRMA sem permissão prévia e expressa.

4.2. Limites de utilização direcionados para verificadores

Os certificados são usados para a sua própria função e propósito estabelecido, e não podem ser usados para outras funções ou para outros fins.

De igual modo, os certificados devem ser usados apenas de acordo com a legislação aplicável, especialmente tendo em conta as restrições à importação e exportação em vigor em cada momento.

Os certificados não podem ser usados para assinar pedidos 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 (LRCs).

Os certificados não foram concebidos, não podem ser usados nem estão autorizados para uso ou revenda como equipamentos de controlo de situações perigosas ou para usos que exijam ações de segurança em falhas, como a operação de instalações nucleares, sistemas de navegação aérea ou comunicações, ou sistemas de controlo de armas, onde uma falha possa levar diretamente à morte, Danos pessoais ou danos ambientais graves.

Devem ser tidos em conta os limites indicados nos vários campos dos perfis de certificados, visíveis no site da ESFIRMA.

O uso de certificados digitais em transações que contrariem este texto de divulgação (PDS), ou contratos com subscritores, é considerado uso impróprio para fins legais adequados, pelo que a ESFIRMA está isenta, de acordo com a legislação vigente, de qualquer responsabilidade por este uso impróprio dos certificados feito pelo signatário ou por qualquer terceiro.

O fornecedor esFIRMA não tem acesso aos dados sobre os quais pode ser aplicado o uso de um certificado. Assim, e como consequência desta impossibilidade técnica de aceder ao conteúdo da mensagem, não é possível para a esFIRMA emitir qualquer avaliação sobre esse conteúdo, pelo que o assinante, o signatário ou o criador dos selos assume qualquer responsabilidade decorrente do conteúdo associado à utilização de um certificado.

Da mesma forma, o assinante será responsável por qualquer responsabilidade que possa surgir do uso do mesmo fora dos limites e condições de uso estabelecidos neste texto de divulgação, ou nos contratos com os subscritores, bem como de qualquer outro uso indevido do mesmo derivado desta secção ou que possa ser interpretado como tal de acordo com a legislação vigente.

5. Obrigações dos subscritores

5.1. Geração de chaves

Nos certificados de cartão, o assinante autoriza o signatário a gerar as suas chaves privadas e públicas dentro de um dispositivo qualificado de criação de assinatura eletrónica, e solicita, em nome do signatário, a emissão do certificado ao esFIRMA.

Nos certificados cloud, o assinante autoriza o signatário a gerar as suas chaves privadas e públicas, e solicita, em nome do signatário, a emissão do certificado ao esFIRMA.

Nos certificados eletrónicos de selo, o assinante autoriza a esFIRMA a gerar as chaves, privadas e públicas, para uso pelos criadores do selo, e solicita em seu nome a emissão do certificado eletrónico de selo.

5.2. Pedido de certificados

O subscritor compromete-se a fazer pedidos, quando necessário, para estes certificados de acordo com o procedimento e, se necessário, os componentes técnicos fornecidos pela ESFIRMA, de acordo com as disposições da declaração de práticas de certificação (CPD) e da documentação operacional da ESFIRMA.

5.3. Veracidade da informação

O assinante é responsável por garantir que toda a informação incluída na sua candidatura ao certificado é precisa, completa para efeitos do certificado e está sempre atualizada.

O assinante deve informar imediatamente a ESFIRMA:

- Quaisquer imprecisões detetadas no certificado após a sua emissão.

- Quaisquer alterações que ocorram na informação fornecida e/ou registada para a emissão do certificado.

5.4. Obrigações de custódia

O assinante compromete-se a salvaguardar toda a informação gerada na sua atividade enquanto entidade de registo.

6. Obrigações dos signatários e criadores de selos

6.1. Obrigações de custódia

O signatário ou criador dos selos compromete-se a proteger o código de identificação pessoal, as chaves privadas, quando o cartão ou qualquer outro suporte técnico fornecido pela esFIRMA e, se necessário, as especificações detidas pela esFIRMA que forem fornecidas.

No caso de perda ou roubo da chave privada do certificado, ou no caso de suspeitar que a chave privada perdeu fiabilidade por qualquer motivo, tais circunstâncias devem ser imediatamente notificadas diretamente à esFIRMA ou através do assinante.

6.2. Obrigações de uso correto

O signatário ou criador dos selos deve utilizar o serviço de certificação fornecido pela esFIRMA, exclusivamente para os usos autorizados no DPC e em quaisquer outras instruções, manuais ou procedimentos fornecidos ao assinante.

O signatário ou criador dos selos tem de cumprir quaisquer leis e regulamentos que possam afetar o seu direito de utilizar as ferramentas criptográficas utilizadas.

O signatário ou criador dos selos não pode adotar medidas para inspecionar, alterar ou descompilar os serviços digitais de certificação prestados.

O signatário ou criador dos selos deve deixar de usar a chave privada em caso de comprometimento da chave, revogação ou comprometimento das chaves da CA.

O signatário ou criador dos selos reconhecerá:

a) Que quando usar qualquer certificado, e desde que o certificado não tenha expirado ou sido revogado, terá aceite esse certificado e estará operacional.

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

6.3. Transações proibidas

O signatário ou criador dos selos compromete-se a não utilizar as suas chaves privadas, certificados, cartões ou qualquer outro suporte técnico fornecido pela esFIRMA na realização de qualquer transação proibida pela lei aplicável.

Os serviços digitais de certificação (e os serviços de carimbo eletrónico temporal) fornecidos pela ESFIRMA não foram concebidos e não permitem a sua utilização ou revenda como equipamentos de controlo de situações perigosas, nem para usos que exijam ações à prova de erros, como a operação de instalações nucleares, sistemas de navegação aérea ou comunicação, sistemas de controlo de tráfego aéreo ou sistemas de controlo de armamento, onde um erro pode causar diretamente a vida, danos físicos ou danos ambientais graves.

7. Obrigações dos verificadores

7.1. Decisão informada

A ESFIRMA informa o verificador que tem acesso a informação suficiente para tomar uma decisão informada no momento da verificação de um certificado e para confiar na informação contida nesse certificado.

Além disso, o verificador deve reconhecer que a utilização das Listas de Registo e Revogação de Certificados da ESFIRMA (doravante designadas como "as LRCs" ou "as CRLs") é regida pela DPC da ESFIRMA e compromete-se a cumprir os requisitos técnicos, operacionais e de segurança descritos na referida DPC.

7.2. Requisitos de Verificação de Assinatura

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

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

Uma assinatura eletrónica é considerada corretamente verificada se todos os certificados da cadeia estiverem corretos e atualizados.

- É necessário garantir que todos os certificados na cadeia autorizam o uso da chave privada pelo assinante do certificado, uma vez que existe a possibilidade de alguns dos certificados incluirem limites de utilização que impeçam a confiança na verificação da assinatura eletrónica. Cada certificado na cadeia tem um indicador que se refere às condições de utilização aplicáveis, para revisão pelos verificadores.
- É necessário verificar tecnicamente a assinatura de todos os certificados na cadeia antes de confiar no certificado utilizado pelo signatário ou criador do selo.

7.3. Confiar num certificado não verificado

Se o verificador depender de um certificado não verificado, assumirá todos os riscos decorrentes desta ação.

7.4. Efeito da verificação

Em virtude da verificação correta destes certificados, de acordo com este texto informativo (PDS), o verificador pode confiar na identificação e, quando apropriado, na chave pública do signatário.

7.5. Uso Adequado e Atividades Proibidas

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

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

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

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

7.6. Cláusula de indemnização

O terceiro que confia no certificado compromete-se a isentar a ESFIRMA de quaisquer danos resultantes de qualquer ação ou omissão que resulte em responsabilidade, dano ou perda, despesas de qualquer tipo, incluindo despesas legais e de representação legal que possam ser incorridas, pela publicação e utilização do certificado, quando ocorrer qualquer uma das seguintes causas:

- Incumprimento das obrigações do terceiro que se baseia no certificado.
- Confiança imprudente num certificado, tendo em conta as circunstâncias.
- Falha em verificar o estado de um certificado, para determinar que não está suspenso ou revogado.
- Falha em verificar todas as medidas de segurança prescritas no DCP ou noutras regulamentações de implementação.

A ESFIRMA não será responsável pelos danos causados nos termos indicados no Artigo 11 da Lei 6/2020, de 11 de novembro, que regula certos aspetos dos serviços eletrónicos de trust.

8. Obrigações de ESFIRMA

8.1. No que diz respeito à prestação de certificação digital

A ESFIRMA compromete-se a:

a) Emitir, entregar, administrar e revogar certificados, de acordo com as instruções fornecidas pelo subscritor, nos casos e pelas razões descritas no DPC ESFIRMA.

b) Realizar os serviços com os meios técnicos e materiais adequados, e com pessoal que cumpra as qualificações e condições de experiência estabelecidas no DPC.

c) Cumprir os níveis de qualidade do serviço, de acordo com o que está estabelecido no DPC, nos aspetos técnicos, operacionais e de segurança.

d) Notifique o assinante, com antecedência, da data de validade dos certificados.

e) Comunique aos terceiros que o solicitem o estado dos certificados, de acordo com o que está estabelecido no DPC para os diferentes serviços de verificação de certificados.

8.2. Em relação às verificações de registo

A ESFIRMA compromete-se a emitir certificados com base nos dados fornecidos pelo subscritor, para os quais poderá realizar as verificações que considerar adequadas.

No caso de a ESFIRMA detetar erros nos dados que devem ser incluídos nos certificados ou que justifiquem esses dados, pode fazer as alterações que considerar necessárias antes de emitir o certificado ou suspender o processo de emissão e gerir o incidente correspondente com o assinante. No caso de a ESFIRMA corrigir os dados sem gerir previamente o incidente

correspondente ao assinante, deve notificá-lo dos dados finalmente certificados.

A ESFIRMA reserva-se o direito de não emitir o certificado quando considerar que a justificação documental é insuficiente para a identificação e autenticação corretas do assinante.

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

8.3. Períodos de retenção

A ESFIRMA mantém informações relativas aos serviços prestados de acordo com o Artigo 24.2.h) do Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, por pelo menos 15 anos a contar da expiração do certificado ou do fim do serviço prestado.

A ESFIRMA armazena informação de registo por um período entre 1 e 15 anos, dependendo do tipo de informação registada.

9. Garantias Limitadas e Isenções de Garantias

9.1. Garantia ESFIRMA para serviços de certificação digital

A ESFIRMA garante ao assinante:

- Que não existem erros factuais na informação contida nos certificados, conhecidos ou emitidos pelo Organismo Certificador.

- Que não existem erros factuais na informação contida nos certificados, devido à falta de diligência devida na gestão da candidatura do certificado ou na criação do mesmo.

- Que os certificados cumpram todos os requisitos materiais estabelecidos no DPC.

- Que os serviços de revogação e a utilização do depósito cumpram todos os requisitos materiais estabelecidos no DPC.

A ESFIRMA garante ao terceiro que depende do certificado:

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

- No caso de certificados publicados no depósito, que o certificado foi emitido ao subscritor identificado e que o certificado foi aceite.

- Que, na aprovação do pedido de certificado e na emissão do certificado, todos os requisitos materiais estabelecidos no DPC foram cumpridos.

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

Além disso, a ESFIRMA garante ao assinante e ao terceiro que depende do certificado:

- Que o certificado contém a informação que um certificado qualificado deve conter, de acordo com o Anexo I do Regulamento da UE 910/2014.
- Que, no caso de gerar as chaves privadas do assinante ou, quando apropriado, da pessoa física identificada no certificado, a sua confidencialidade é mantida durante o processo.
- Responsabilidade do Organismo de Certificação, dentro dos limites estabelecidos. Em nenhum caso a ESFIRMA será responsável por acontecimentos fortuitos e em caso de força maior.
- A chave privada da autoridade certificadora utilizada para emitir certificados não foi comprometida, a menos que a esFIRMA não tenha comunicado o contrário, segundo o DPC.
- Não originou nem introduziu declarações falsas ou erradas na informação de qualquer certificado, nem deixou de incluir as informações necessárias fornecidas pelo assinante e validadas pelo esFIRMA no momento da emissão do certificado.
- Todos os certificados cumprem os requisitos formais e de conteúdo do DPC, incluindo todos os requisitos legais atuais e aplicáveis.
- Está sujeita aos procedimentos operacionais e de segurança definidos no CPD.

9.2. Exclusão da Garantia

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

Especificamente, o ESFIRMA não garante qualquer software utilizado por qualquer pessoa para assinar, verificar assinaturas, encriptar, desencriptar ou utilizar qualquer certificado digital

emitida pela ESFIRMA, exceto nos casos em que exista declaração escrita em contrário.

10. Acordos e DPCs Aplicáveis

10.1. Acordos Aplicáveis

Os acordos aplicáveis a este certificado são os seguintes:

- Contrato de serviços de certificação, que regula a relação entre a ESFIRMA e a Administração Pública/Entidade Jurídica que subscreve os certificados.

- Termos Gerais de Serviço incorporados neste texto de Divulgação de Certificado ou PDS.

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

10.2. CPD

Os serviços de certificação da ESFIRMA são regulados técnica e operacionalmente pelo CPD da ESFIRMA, pelas suas atualizações subsequentes, bem como por documentação complementar.

O CPD e a documentação das operações são periodicamente modificados e podem ser consultados no site: https://www.esfirma.com

11. Política de Privacidade

A ESFIRMA não pode divulgar nem pode ser obrigada a divulgar qualquer informação confidencial relativa a certificados sem um pedido específico prévio de:

a) A pessoa relativamente a quem o ESFIRMA tem o dever de manter a informação confidencial, ou

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

No entanto, o subscritor concorda que certas informações, pessoais ou não, fornecidas na candidatura do certificado, serão incluídas nos seus certificados e no mecanismo de verificação do estado do certificado, e que essas informações não serão confidenciais, conforme exigido por lei.

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

O tratamento desses dados por terceiros para o fim de prestar um serviço à esFIRMA, incluindo, mas não se limitando a, ocorre no âmbito de uma ordem de processamento referida no artigo 28 REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 sobre a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação destes dados e à revogação da Diretiva 95/46/CE (Regulamento Geral de Proteção de Dados) e do artigo 33 da Lei Orgânica 3/2018, de 5 de dezembro, sobre a Proteção de Dados Pessoais e Garantia dos Direitos Digitais (LOPDGDD), em virtude da qual está em conformidade com os requisitos do RGPD e da LOPDGDD, e garante a proteção dos direitos do sujeito aos dados.

12. Política de Privacidade

A ESFIRMA tem uma política de privacidade na secção 9.4 do DPC, e um regulamento específico de privacidade relativo ao processo de registo, confidencialidade do registo, proteção do acesso a informações pessoais e consentimento dos utilizadores.

A informação referida na secção 7.3 deverá ser mantida nos períodos indicados, devidamente registada e com garantias de segurança e integridade.

13. Política de Reembolso

A ESFIRMA não reembolsará o custo do serviço de certificação em circunstância alguma.

14. Legislação aplicável, jurisdição competente e regime de reclamações e litígios

As relações com a ESFIRMA serão regidas pela legislação espanhola sobre serviços fiduciários em vigor em todos os momentos, bem como pela legislação civil e comercial, conforme aplicável.

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

Em caso de divergência entre as partes, estas devem tentar um acordo amigável prévio. Para tal, as partes devem enviar uma comunicação à esFIRMA, preenchendo o formulário de reclamação e sugestão disponível no site da esFIRMA por qualquer dos meios aí indicados. A queixa será tratada de acordo com os procedimentos internos para a resolução de queixas, recursos e litígios.

Se as partes não chegarem a acordo a este respeito, qualquer uma delas pode submeter a disputa à jurisdição civil, sujeita aos Tribunais da sede registada da ESFIRMA.

14.1. Acreditações e selos de qualidade

A EsFIRMA possui a qualificação "compatível com eIDAS" para os seguintes serviços:

a) Serviço para a emissão de certificados eletrónicos qualificados para assinaturas eletrónicas
b) Serviço para a emissão de certificados eletrónicos qualificados com selo eletrónico
c) Serviço para a emissão de certificados eletrónicos qualificados para autenticação de websites
d) Serviço de emissão de selos eletrónicos qualificados por tempo

14.2. Ligação para a lista de prestadores

A EsFIRMA é um prestador qualificado de serviços de certificação e, por isso, faz parte da Lista de Prestadores Qualificados (TSL) mantida pelo supervisor nacional e que pode ser obtida no seguinte endereço:
https://sedeaplicaciones.minetur.gob.es/Prestadores/

A EsFIRMA está incluída na "Lista de Trusts" da União Europeia como Prestadora qualificada de
Serviços Eletrónicos de Confiança:
https://webgate.ec.europa.eu/tl-browser/#/tl/ES/27

14.3. Separabilidade dos termos, sobrevivência, acordo total e notificação

As disposições deste texto de divulgação (PDS) são independentes umas das outras, pelo que, se alguma cláusula for considerada inválida ou inexequível, as restantes cláusulas do PDS continuarão a aplicar-se, salvo acordo expresso em contrário entre as partes.

Os requisitos contidos nas secções "Obrigações e Responsabilidade", "Auditoria de Conformidade" e "Confidencialidade" do DPC da ESFIRMA permanecerão em vigor após a cessação do serviço.

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

As partes notificam-se mutuamente dos factos através de um procedimento enviado por email para a morada info@esfirma.com