

PDS

PKI Disclosure Statement

CÓDIGO DO DOCUMENTO	ICERT-INDI-PDS
VERSÃO	3.2
DATA	21/09/2021

SUMÁRIO

1. INTRODUÇÃO	3
2. CONTACTOS	3
3. TIPOS DE CERTIFICADOS, VALIDAÇÃO E UTILIZAÇÃO	4
4. LIMITES DE CONFIANÇA	5
5. OBRIGAÇÕES DO TITULAR	5
6. OBRIGAÇÕES DO REQUERENTE, SE DIFERENTE DO TITULAR	6
7. ESTADO DE VALIDADE DOS CERTIFICADOS.....	8
8. GARANTIA LIMITADA E EXCLUSÃO/LIMITAÇÃO DE RESPONSABILIDADE	8
9. ACORDOS APLICÁVEIS, POLÍTICAS E DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO	9
10. POLÍTICA DE PRIVACIDADE	9
11. POLÍTICAS DE REEMBOLSO	9
12. LEI APLICÁVEL ÀS RECLAMAÇÕES E À RESOLUÇÃO DE LITÍGIOS.....	10
13. ARQUIVOS, LICENÇAS E MARCAS, AUDITORIAS	10

1. Introdução

O presente PKI-Disclosure-Statement (PDS) cumpre o pedido de publicação contemplado na norma europeia ETSI EN 319 411-1, relativa ao serviço de certificação oferecido pela Qualified Trust Service Provider InfoCert SpA. (doravante “**InfoCert**” ou “**QTSP**”) e destina-se a fornecer ao requerente do serviço as informações técnicas necessárias para a sua utilização.

O Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 "relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno, que revoga a Diretiva 1999/93/CE" é referido como "**Regulamento eIDAS**".

O presente documento é adicionado às Condições Gerais de Contrato como parte integrante da documentação contratual da InfoCert.

A publicação deste PDS não substitui a publicação da Declaração de Práticas de Certificação (CPS) onde constam informações mais detalhadas, disponível no site web da InfoCert, no endereço:

<https://www.firma.infocert.it/documentazione/>.

2. Contactos

InfoCert S.p.A. – N.º fiscal para efeitos de IVA 07945211006
Qualified Trust Service Provider
Piazza Sallustio, 9
00187 - Roma

Sede operacional
Piazza Luigi da Porto 3
35131 Pádua

Telefone: +39 06836691 - Fax: +39 06 23328861
Call Center Assinatura Digital: consultar o link <https://help.infocert.it/contatti/>
Web: <http://www.firma.infocert.it/>
e-mail: firma.digitale@legalmail.it

É possível pedir a **revogação** utilizando o formulário específico publicado no site web da InfoCert e enviando-o por correio eletrónico certificado, carta registada ou por fax acompanhado da fotocópia de um documento de identidade válido. Também é possível requerer a revogação diretamente no serviço de registo competente, de acordo com os termos das condições gerais de contrato. A InfoCert reserva-se o direito de fazer verificações adicionais sobre a identidade do requerente.

A **suspensão** pode ser pedida diretamente online no site web da InfoCert, utilizando o código secreto atribuído na altura do registo.

3. Tipos de certificados, validação e utilização

A InfoCert emite certificados qualificados de acordo com a norma europeia **ETSI EN 319 411** e outras normas relacionadas. Os certificados são oferecidos ao público (empresas privadas, organismos públicos, profissionais, particulares, etc.), nas condições publicadas no site web do QTSP ou das Autoridades de Registo (RA).

O algoritmo utilizado para assinar os certificados pode ser selecionado entre os seguintes:

- sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)]
- ecdsa-with-SHA256 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)]
- ecdsa-with-SHA384 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)]
- ecdsa-with-SHA512 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)].

As assinaturas e certificados são verificáveis através do produto **GoSign**, que poderá ser descarregado gratuitamente do site da InfoCert.

4. Limites de confiança

A InfoCert emite:

- **certificados qualificados a pessoas singulares**, para assinatura eletrónica avançada ou qualificada;
- **certificados qualificados de selo eletrónico a pessoas coletivas**, também para conformidade com a Diretiva PSD2

Além disso, a InfoCert fornece serviços de assinatura remota em QSCD (Qualified Electronic Signature Creation Device), gerando e gerindo chaves e certificados para o signatário.

Detalhes e políticas podem ser encontrados nas Declarações de Práticas de Certificação disponíveis no endereço <https://www.firma.infocert.it/documentazione>.

O período de validade de cada certificado está indicado no próprio certificado e pode variar desde um mínimo de uma hora a um máximo de três anos e três meses.

É proibida a utilização do certificado fora dos limites e dos contextos especificados na CPS e nos contratos e, de qualquer forma, violando os limites de uso e de valor (*key usage, extended key usage, user notice*) indicados no certificado.

Os registos de eventos relacionados com a emissão de certificados são conservados durante, pelo menos, 20 (vinte) anos, no sistema de conservação InfoCert, abrangido pela legislação vigente em Itália.

5. Obrigações do Titular

O **Titular** deve respeitar as cláusulas constantes da CPS e das condições gerais de contrato e, nomeadamente:

- ler a documentação contratual e qualquer outra documentação de informação suplementar;
- seguir os procedimentos de identificação adotados pela Autoridade de Certificação (CA), conforme descritos na CPS;

- fornecer todas as informações necessárias para a identificação acompanhadas, quando solicitado, por documentação adequada;
- utilizar o seu par de chaves apenas para os fins e das formas previstas na CPS;
- assinar o pedido de registo e certificação, aceitando as condições gerais de contrato que disciplinam o fornecimento do serviço, nos formulários analógicos ou eletrónicos preparados pela CA.
- até à data de expiração do certificado, informar imediatamente a CA ou a RA nos seguintes casos:
 - se o seu dispositivo de assinatura foi perdido, roubado ou estiver danificado;
 - se perdeu o controlo exclusivo da sua chave privada devido, por exemplo, a violação dos dados de ativação (por exemplo do PIN) do seu dispositivo de assinatura;
 - se algumas das informações constantes do seu certificado estiverem incorretas ou já não forem válidas;
- proteger a confidencialidade das credenciais necessárias para utilizar os dispositivos ou os serviços de assinatura, não as comunicando ou revelando a terceiros e mantendo-as sob seu controlo exclusivo;
- Deixar imediata e permanentemente de utilizar esta chave possivelmente violada, salvo para a descodificação da própria chave;
- Assegurar-se de que a chave privada deixa de ser utilizada pelo assinante, caso o requerente seja informado de que o certificado do assinante foi revogado ou que a CA foi violada.

O fornecimento e utilização de uma ligação à Internet e de todas as ferramentas necessárias (hardware e software) são da responsabilidade do requerente.

6. Obrigações do Requerente, se diferente do Titular

O **Requerente**, se diferente do Titular, deve respeitar as cláusulas constantes da CPS e das condições gerais de contrato e, nomeadamente:

- ler a documentação contratual e qualquer outra documentação de informação suplementar;
- seguir os procedimentos de identificação adotados pelo QTSP;

- fornecer todas as informações necessárias para a identificação acompanhadas, quando solicitado, por documentação adequada;
- assinar o pedido de registo e certificação, aceitando as condições contratuais que disciplinam o fornecimento do serviço, nos formulários analógicos ou eletrónicos preparados pela CA;
- Identificar e comunicar ao TSP o procedimento informático por meio do qual serão enviados os documentos a submeter ao procedimento de assinatura remota e à ativação das chaves de assinatura por parte do Titular;
- Suportar os custos do serviço de assinatura remota e indicar, através de documentos e procedimentos específicos, as entidades Titulares às quais os certificados deverão ser concedidos;
- indicar o tipo de sistema de autenticação escolhido para ativar o procedimento de assinatura remota;
- caso pretenda pedir a revogação ou suspensão do certificado do Titular, assinar o formulário específico de pedido de revogação ou suspensão disponibilizado pelo QTSP;
- informar o Titular das obrigações decorrentes do certificado, fornecer informações corretas e verdadeiras sobre a identidade do Titular e seguir os processos e indicações do QTSP e/ou da AR;
- se o Titular for pessoa coletiva, fornecer ao QTSP as seguintes informações:
 - Apelido e nome do Requerente;
 - Código TIN ou código análogo de identificação do Requerente (código fiscal para o contexto italiano);
 - Dados do documento de identificação apresentado para a identificação do Requerente, tais como tipo, número, entidade emissora e data de emissão do documento;
 - endereço de correio eletrónico para enviar ao Requerente as comunicações do QTSP;
 - Nome do Titular pessoa coletiva;
 - VAT Code ou NTR (número fiscal para efeitos de IVA ou número de Registo de Empresa para os assinantes italianos);
- quando as chaves são geradas num dispositivo do Assinante, o Requerente deve enviar um pedido específico em formato PKCS#10 assinado pelo Requerente. Se o dispositivo de assinatura não for colocado à disposição pelo QTSP, o Requerente deve assegurar que o dispositivo respeite as normas em vigor, apresentando

documentação específica e estando sujeito a auditorias periódicas realizadas pelo QTSP.

7. Estado de validade dos certificados

Quem quer que utilize informações contidas nos certificados deverá verificar que os certificados não estejam suspensos ou revogados.

As informações sobre o estado dos certificados estão disponíveis consultando a lista de certificados revogados (CRL) publicada pela CA na url indicada no próprio certificado ou através do serviço OCSP. A verificação da validade dos certificados pode ser feita através do produto GoSign, que pode ser descarregado gratuitamente do site da InfoCert.

8. Garantia limitada e exclusão/limitação de responsabilidade

Os certificados qualificados são fornecidos em conformidade com este documento e as condições gerais de contrato. Todos os pormenores técnicos necessários estão determinados na CPS.

A InfoCert é responsável pelos possíveis danos causados diretamente, com dolo ou por negligência, a qualquer pessoa singular ou coletiva, em consequência do incumprimento das obrigações referidas no Regulamento (UE) N.º 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 e da falta de adoção, por parte da InfoCert, de todas as medidas aptas a evitar o referido dano.

No caso citado no parágrafo anterior, o Requerente ou o Titular terão o direito de obter, a título de ressarcimento dos danos sofridos diretamente em consequência do comportamento referido no parágrafo anterior, um montante que, em todo caso, não poderá ser superior aos valores máximos previstos para cada sinistro e por ano, no art. 3.º, alínea 7, do Regulamento anexo à Determinação AgID 185/2017.

O reembolso não poderá ser solicitado se a não fruição for imputável à utilização imprópria do serviço de certificação ou ao gestor da rede de telecomunicações, ou então derivante de caso fortuito, força maior ou causas de qualquer maneira não imputáveis à InfoCert.

9. Acordos aplicáveis, políticas e declarações de práticas de certificação

Os acordos, os termos e condições aplicáveis ao serviço do QTSP e as CSPs estão publicados no site web da InfoCert, no endereço <https://firma.infocert.it/documentazione>.

10. Política de privacidade

As informações relativas ao Assinante e ao Requerente que são adquiridas pela CA durante o exercício das suas atividades típicas devem ser consideradas, salvo consentimento expresso, confidenciais e não publicáveis, com exceção daquelas explicitamente destinadas a uso público: *chave pública, certificado (se solicitado pelo Assinante), datas de revogação e de suspensão do certificado*.

Em particular, os dados pessoais são tratados pela InfoCert em conformidade com o Decreto Legislativo italiano de 30 de junho de 2003, n.º 196 e o Regulamento Europeu 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, totalmente vinculativo a partir de 25 de maio de 2018.

11. Políticas de reembolso

O Titular é obrigado a informar o QTSP da sua decisão de rescisão do contrato através de uma declaração explícita que deve ser enviada, antes do termo do período de rescisão, por correio eletrónico certificado para o endereço: *richieste.rimborso@legalmail.it* ou por carta registada com aviso de receção dirigida a InfoCert S.p.A., Direção Geral e Administrativa, Via Marco e Marcelliano, 45 00147 Roma. Para este efeito pode utilizar, por conveniência, o formulário de rescisão disponível no site, acedendo ao seguinte link: <https://www.InfoCert.it/pdf/Modulo-di-recesso-tipo.pdf>.

Sem prejuízo do custo de devolução do possível dispositivo de assinatura a ser suportado pelo Titular e/ou Requerente, o QTSP reembolsará os pagamentos já efetuados. Tais reembolsos serão efetuados para a conta bancária corrente utilizada na transação inicial,

a menos que o Titular tenha indicado expressamente outros dados bancários; em todo o caso, o Titular não suportará quaisquer custos na sequência do reembolso em questão.

12. Lei aplicável às reclamações e à resolução de litígios

A prestação do serviço de certificação e selos temporais é regulada pelas leis em vigor em Itália. Para tudo o que aqui não estiver expressamente previsto, remete-se para o Código Civil italiano e para as outras leis aplicáveis.

Salvo disposição em contrário nas condições gerais de contrato, todos os litígios decorrentes ou relacionados com a interpretação e execução do presente acordo serão submetidos à jurisdição exclusiva dos tribunais competentes de Roma.

Se o cliente for um consumidor, quaisquer litígios relativos ao contrato celebrado pelo consumidor estarão sujeitos à jurisdição territorial inapelável do órgão jurisdicional do local de residência ou de domicílio do mesmo consumidor.

13. Arquivos, licenças e marcas, auditorias

A CA não efetua verificações relativas à utilização de marcas registadas mas pode recusar a geração ou pode pedir a revogação de um certificado envolvido numa disputa.

A verificação de conformidade com o Regulamento (UE) n.º 910/2014 de 23/07/2014, conforme as normas ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, foi realizada pela CSQA Certificazioni S.r.l, de acordo com o esquema de avaliação eIDAS definido por ACCREDIA, em conformidade com as normas ETSI EN 319 403 e ISO/IEC 17065:2012.

A InfoCert apresentou o relatório de conformidade à Agência para a Itália Digital - AgID que confirmou a presença da InfoCert como Prestador qualificado de serviços de confiança, de acordo com o Regulamento (UE) n.º 910/2014 de 23/07/2014, na Trusted List.

A lista das CAs italianas de confiança (Trusted List) pode ser visualizada no site <https://eidas.agid.gov.it/TL/TSL-IT.xml>