In.Te.S.A. S.p.A.

Qualified Trust Service Provider

Manual de Operação para os procedimentos de assinatura eletrónica qualificada remota em âmbito bancário e financeiro

Código documento: MO_REMBAN OID: 1.3.76.21.1.50.110

Redação: Antonio Raia

Aprovação: Franco Tafini

Data de emissão: 01/07/2019

Versão: 04

Assinado por:
ANTONIO RAIA

Organização: IN.TE.S.A. S.p.A.

VERSÕES

Versão n.º: 04		***Data Revisão:***	***01/07/2019***
Descrição das alterações:	Alteração dos dados da empresa e logótipo Atualização de definições e referências normativas Atualização layout gráfico Introdução procedimento de assinatura para Cliente Prospect (I.2.3)		
Motivos:	Atualizações das normas: Regulamento (UE) 910/2014 (eIDAS), Decreto Legislativo 179/2016 (RGPD) Alterações organizativas do TSP Novo procedimento para aquisição de cliente		
Versão n.º: 03		***Data da Revisão:***	***13/06/2012***
Descrição das alterações:	Extensão do manual ao âmbito financeiro (Instituições de Pagamento) além do bancário		
Motivos:	Atualização		
Versão n.º: 02		***Data da Revisão:***	***02/04/2012***
Descrição das alterações:	B.4.2. - Introduzido sistema de reconhecimento da identidade do Titular (Verificação adequada) sem a presença física do mesmo. C.5. - Introduzidas modalidades do sistema de reconhecimento da identidade do Titular (Verificação adequada). F.1.3. - Inserido limite de uso padrão. G. - Inserida modalidade de comunicação por e-mail das confirmações operativas.		
Motivos:	Atualização		
Versão n.º: 01		***Data da Revisão:***	***01/11/2011***
Descrição das alterações:	nenhuma		
Motivos:	primeira publicação		

Índice

Referências legais

Texto Único - DPR 445/00 e posteriores modificações e adendas	Decreto do Presidente da República n.º 445 de 28 de dezembro de 2000. *"Texto único das disposições legislativas e regulamentares em matéria de documentação administrativa"*. De ora em diante indicado também apenas como *TU*.
CAD - DLGS 82/05 e posteriores modificações e adendas	Decreto-lei n.º 82 de 7 de março de 2005. "*Código da administração digital*". De ora em diante indicado também apenas como *CAD*.
DPCM 22/02/2013 *Novas Regras Técnicas* e posteriores modificações e adendas	Decreto do Presidente do Conselho de Ministros de 22 de fevereiro de 2013 *"Regras técnicas em matéria de geração, aposição e verificação das assinaturas eletrónicas avançadas, qualificadas e digitais, nos termos dos artigos 20.º parágrafo 3, 24.º parágrafo 4, 28.º parágrafo 3,* *32.º parágrafo 3 alínea b), 35.º parágrafo 2, 36.º parágrafo 2, e 71.º (do CAD, ndr).* De ora em diante indicado também apenas como *DPCM*.
Regulamento (UE) n. 910/2014 (eIDAS) e posteriores modificações e adendas	Regulamento UE) n. 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 e que revoga a diretiva 1999/93/CE. De ora em diante indicado também apenas como *Reg. eIDAS*.
RGPD Regulamento Geral sobre a Proteção de Dados e posteriores modificações e adendas	REGULAMENTO (UE) 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, e que revoga a diretiva 95/46/CE (regulamento geral sobre a proteção de dados) De ora em diante indicado também apenas como *RGPD*.
DETERMINAÇÃO N.º 147/2019 e posteriores modificações e adendas	Linhas de orientação com as "Regras Técnicas e Recomendações relativas à criação de certificados eletrónicos qualificados, assinaturas e selos eletrónicos qualificados e selos temporais eletrónicos qualificados. De ora em diante indicado também apenas como *DETERMINAÇÃO*.

Definições e acrónimos

AgID	*Agenzia per l'Italia Digitale* ("Agência para a Itália Digital", antiga CNIPA e DigitPA) - *www.agid.gov.it*. Organismo de Vigilância nos termos do Reg. UE 910/2014 (eIDAS). De ora em diante denominada também apenas *Agência*.
QTSP *Qualified Trust Service Provider.* *Certificador Acreditado*	*Prestador de Serviços de Confiança Qualificado*. Pessoa singular ou coletiva que presta um ou mais serviços de confiança qualificados. Anterior *Certificador Acreditado*, nos termos do CAD. No presente documento é o QTSP In.Te.S.A. S.p.A.
Serviço de Confiança Qualificado	Serviço eletrónico fornecido por um QTSP e que consiste nos elementos referidos no Art. 3.º, ponto 16) e 17) do Reg. UE 910/2014 (eIDAS). No presente documento é o QTSP In.Te.S.A. S.p.A. que presta os serviços qualificados de assinatura eletrónica e de selo temporal eletrónico e outros serviços associados a estes últimos.
Certificado Qualificado de assinatura eletrónica	Atestado eletrónico que associa os dados de validação da assinatura eletrónica a uma pessoa singular e confirma, pelo menos, o seu nome ou pseudónimo. É emitido por um prestador de serviços de confiança e satisfaz os requisitos estabelecidos no anexo I do Reg. UE 910/2014 (eIDAS)
Chave Privada	O elemento do par de chaves assimétricas, usado pelo Titular, através do qual a assinatura digital é aposta no documento eletrónico.
Chave Pública	O elemento do par de chaves assimétricas que se pretende tornar público, com o qual se verifica a assinatura digital no documento informático.
CRL	Lista dos Certificados Revogados, Certificate Revocation List, uma lista que apresenta os certificados revogados ou suspensos, que já não sejam considerados válidos pelo Certificador que os emitiu.
OCSP	Online Certificate Status Protocol: serviço de verificação do estado de validade do Certificado, de acordo com o protocolo OCSP.

Documento informático	O documento eletrónico que contém a representação informática de atos, factos ou dados juridicamente relevantes
AEQ - Assinatura Eletrónica Qualificada *AD - Assinatura Digital*	Assinatura eletrónica criada por um dispositivo qualificado de criação de assinaturas eletrónicas e que se baseia num certificado qualificado de assinatura eletrónica. Em Itália, corresponde à *Assinatura Digital* definida no CAD, Art. 1.º, parágrafo 1, ponto s): Assinatura eletrónica qualificada baseada num sistema de chaves criptográficas, uma pública e uma privada, correlacionadas entre si, que permite ao Titular, através da chave privada, e ao destinatário, através da chave pública, respetivamente, explicitar e verificar a proveniência e a integridade de um documento informático ou de um conjunto de documentos informáticos.
Assinatura Remota	Procedimento especial de assinatura eletrónica qualificada ou de assinatura digital, gerada em HSM protegido e gerido sob a responsabilidade do certificador acreditado, que permite garantir o controlo exclusivo das chaves privadas por parte dos titulares das mesmas.
HSM - Hardware Security Module	Dispositivos para a criação da assinatura eletrónica qualificada, se estiverem em conformidade com os requisitos do Anexo II do Reg. (UE) 910/2014. Também chamados *Dispositivos de Assinatura*.
Qualified Electronic Time Stamp (Selo Temporal Qualificado)	*Selo Temporal Eletrónico Qualificado* Dados em formato eletrónico que vinculam outros dados em formato eletrónico a uma hora específica, criando uma prova de que esses outros dados existiam nesse momento. Satisfaz os requisitos estabelecidos pelo Art. 42.º do Reg. eIDAS
CA - Certification Authority	Autoridade que emite os certificados para a assinatura eletrónica.
RA - Registration Authority	*Autoridade de Registo*: entidade que, encarregada pelo QTSP, tem a responsabilidade de registar e verificar as informações (em especial a identidade do Titular) necessárias para que o QTSP emita o Certificado Qualificado.
Registo dos Certificados	A combinação de um ou mais arquivos informáticos, realizada pelo Certificador, que contém todos os Certificados emitidos.
Requerente	A pessoa singular que requer o Certificado.
Titular	A pessoa singular a quem é emitido o certificado e que está autorizada a utilizá-lo para aplicar a sua assinatura digital.
Cliente *Cliente Prospect*	É o Cliente (ou potencial cliente, chamado Prospect) do Banco/Instituição Financeira.
Referência Temporal	Informação que contém a data e a hora, que é associada a um ou mais documentos informáticos.
TSA - Time Stamping Authority	Autoridade que emite os selos temporais eletrónicos.

A. Introdução

O presente documento constitui o *Manual de Operação para os procedimentos de assinatura eletrónica qualificada remota* (de ora em diante, *Manual de Operação* ou também apenas *MO*) do QTSP In.Te.S.A. S.p.A.

O conteúdo deste Manual de Operação está em conformidade com o estabelecido pelas regras técnicas contidas no *Decreto do Presidente do Conselho de Ministros de 22 de fevereiro de 2013* (de ora em diante *DPCM*) e pelo *Decreto Legislativo 7 de março de 2005, n.º 82, com o "Código da Administração Digital"* como posteriormente alterado e completado (de ora em diante "*CAD*") e está em conformidade com o *Regulamento UE 910/2014* (de ora em diante, *Reg. eIDAS*).

Para tudo o que não for expressamente previsto no presente Manual de Operação, consultar as normas em vigor e futuras que regulam a matéria em questão.

Este documento descreve as regras e os procedimentos operativos do *QTSP In.Te.S.A. S.p.A.* (de ora em diante, *QTSP INTESA, Certificador* ou também apenas *INTESA*) para a emissão dos certificados qualificados, a geração e a verificação da assinatura eletrónica qualificada e os procedimentos do serviço de selo temporal em conformidade com a norma em vigor quando este é gerido no âmbito de projetos bancários ou financeiros.

Nesta tipologia de projetos, as entidades bancárias ou financeiras, fornecedores dos serviços de homebanking e das aplicações de balcão, funcionarão também como Local Registration Authority (de ora em diante, LRA) por conta do QTSP INTESA. Em seguida, estas entidades bancárias ou financeiras serão chamadas com o termo *Banco* ou *Instituição de Pagamento* (ou também apenas *Banco / Instituição*).

Neste contexto, os Titulares de um Certificado Qualificado são apenas os sujeitos identificados pelo mesmo Banco/Instituição que, em virtude de um acordo específico com o QTSP INTESA, está autorizado a desempenhar a função de Registration Authority.

Enfatiza-se, portanto, que todos os processos de assinatura de documentos objeto do presente Manual de Operação serão implementados exclusivamente no âmbito de aplicações bancárias ou financeiras.

As atividades descritas no presente Manual de Operação são realizadas em conformidade com o Reg. UE 910/2014 (eIDAS).

A.1. Propriedade intelectual

O presente Manual de Operação é de exclusiva propriedade da In.Te.S.A. S.p.A., que é Titular de todos os respetivos direitos intelectuais.

O conteúdo deste documento relativo ao desempenho das atividades QTSP encontra-se abrangido por direitos de propriedade intelectual.

A.2. Validade

O conteúdo deste documento aplica-se ao QTSP INTESA (ou seja, às suas infraestruturas logísticas e técnicas, bem como ao seu pessoal), aos Titulares dos certificados emitidos por este e a quem os utiliza para verificar a autenticidade e a integridade dos documentos nos quais seja aposta uma assinatura eletrónica qualificada, utilizando também usando os selos temporais qualificadas emitidas pelo QTSP INTESA, e ao Banco/Instituição de pagamento na qualidade de Local Registration Authority.

O uso das chaves e dos respetivos certificados emitidos é regulado pelo disposto no Artigo 5.º, parágrafo 4, do DPCM, que estabelece que as chaves de criação e verificação de assinatura e os respetivos serviços são diferenciados de acordo com os seguintes tipos:

a) chaves de assinatura, destinadas à criação e verificação de assinaturas apostas ou associadas a documentos;
b) chaves de certificação, destinadas à criação e verificação de assinaturas apostas em certificados qualificados, informações sobre o estado de validade do certificado ou a assinatura de certificados relativos a chaves de selo temporal eletrónico;
c) chaves de marcação temporal, destinadas à criação e verificação dos selos temporais.

B. Generalidades

O objetivo deste documento é descrever, em termos gerais, os procedimentos e respetivas regras que regem a emissão de certificados qualificados por parte do QTSP INTESA.

As regras e procedimentos mencionados acima decorrem do cumprimento das atuais normas de referência, cujo cumprimento permite que a INTESA seja incluída na lista de certificadores acreditados.

Assim, para cumprir as normas mencionadas, será necessário envolver várias entidades que serão melhor identificadas mais à frente no documento.

B.1. Dados de identificação da versão do Manual de Operação

O presente documento constitui a versão n.º *04* do *Manual de Operação para os procedimentos de assinatura eletrónica qualificada remota em âmbito bancário e financeiro,* emitido em conformidade com o Art. 40.º do DPCM.

O identificador de objeto deste documento é **1.3.76.21.1.50.110**.

O presente Manual de Operação é publicado e pode ser consultado por via telemática:

- para o endereço da internet do QTSP, *https://www.intesa.it/e-trustcom/*
- para o endereço da internet da Agência para a Itália Digital, *www.agid.gov.it*
- no âmbito do site institucional do Banco/Instituição.

Nota: a publicação de versões atualizadas do presente Manual de Operação só poderá ser feita mediante autorização prévia da Agência para a Itália Digital.

B.2. Dados de identificação do QTSP – Qualified Trust Service Provider

O QTSP (*Prestador de Serviços de Confiança Qualificado*) é a sociedade ***In.Te.S.A. S.p.A.***, da qual em seguida são apresentados os dados de identificação.

Denominação social	**In.Te.S.A. S.p.A.**
Endereço da sede legal	**Strada Pianezza, 289** **10151 Turim**
Representante Legal	**Diretor Geral**
Registo das Empresas de Turim	**N.º Inscrição 1692/87**
N.º IVA:	**05262890014**
N.º de telefone (central)	**+39.011.19216.111**
Site	**www.intesa.it**
Endereço de correio eletrónico	**marketing@intesa.it**
Endereço (URL) registo dos certificados	**ldap://x500.e-trustcom.intesa.it**
ISO Object Identifier (OID)	**1.3.76.21.1**

O pessoal responsável pelas atividades de certificação, em conformidade com o Art. 38.º do DPCM, é composto pelas figuras seguintes:

a) Responsável pela segurança.
b) Responsável pelo serviço de certificação e selo temporal.
c) Responsável pela condução técnica dos sistemas.
d) Responsável pelos serviços técnicos e logísticos.
e) Responsável pelas verificações e inspeções (auditorias).

As figuras acima pertencem todas à organização do QTSP INTESA.

B.3. Responsabilidade do Manual de Operação

A responsabilidade do presente Manual de Operação, nos termos do Art. 40.º, parágrafo 3, alínea c) do DPCM, é da Certification Authority INTESA, que cuida da sua redação e publicação.

Com o objetivo de recolher eventuais observações e pedidos de esclarecimentos, a INTESA preparou os seguintes instrumentos:

um endereço de correio eletrónico: *marketing@intesa.it*

um contacto telefónico: +39 011.192.16.111

um serviço de Help Desk para as chamadas em Itália 800.80.50.93

para as chamadas para o estrangeiro +39 02.871.193.396

B.4. Entidades envolvidas nos processos

Dentro da estrutura do QTSP são identificadas entidades que participam nos processos relativos à emissão dos certificados.

Estas entidades operam em conformidade com as regras e processos implementados pelo QTSP realizando, na parte que lhes compete, as atividades que lhes foram atribuídas.

B.4.1. Certification Authority (CA)

A INTESA, operando em conformidade com as disposições do DPCM, CAD e Reg. eIDAS, realiza as atividades de Qualified Trust Service Provider. Estas atividades incluem serviços de confiança qualificados para a criação, verificação e validação de assinaturas eletrónicas, selos eletrónicos ou selos temporais qualificados.

Os dados de identificação do QTSP INTESA são indicados no parágrafo anterior *B.2*.

B.4.2. Local Registration Authority (LRA)

Para o tipo específico de serviço oferecido (assinatura eletrónica qualificada remota no campo das aplicações bancárias e financeiras) descrito neste Manual de Operação, o QTSP INTESA exige o desempenho das funções de Registration Authority no Banco/Instituição que adquiriu o serviço.

A LRA compromete-se a realizar as seguintes atividades:

- Identificação do Titular;
- Registo do Titular.

O Banco/Instituição, no exercício da função de Registration Authority, deve garantir que a atividade de reconhecimento seja realizada em conformidade com a legislação em vigor e com as disposições deste Manual de Operação.

Em particular, o Banco/Instituição, em conformidade com a legislação de combate ao branqueamento de capitais, pode identificar o Titular (*verificação adequada*), mesmo que este último não se apresente fisicamente numa agência.

Neste caso, o Banco/Instituição deverá:

- verificar a identidade por meio de documentos, dados ou informações adicionais, como documentos públicos, documentos particulares autenticados, certificados utilizados para a criação de uma assinatura eletrónica qualificada associada a documentos eletrónicos ou através de uma declaração da Autoridade Consular Italiana;
- aplicar medidas adicionais para a verificação dos documentos fornecidos, como, por exemplo, certificados de confirmação de uma instituição de crédito ou financeira sujeita à diretiva;
- utilizar a documentação que comprova que o relatório de financiamento provém de uma conta em nome do cliente.

C. Obrigações

C.1. Obrigações do Prestador de Serviços de Confiança Qualificado (QTSP)

No exercício da sua atividade, o Prestador de Serviços de Confiança Qualificado (também conhecido como *Certificador Acreditado*) opera em conformidade com as disposições de:

- Decreto Legislativo n.º 82 de 7 de março de 2005 e posteriores alterações.
- Decreto do Presidente do Conselho de Ministros de 22 de fevereiro de 2013.
- Regulamento (UE) 2016/679 (RGPD)
- Regulamento (UE) 910/2014 (eIDAS)

Em particular, o QTSP:

- adota todas as medidas organizacionais e técnicas adequadas para evitar danos a terceiros;
- cumpre as regras técnicas especificadas no DPCM e nas modificações e adendas seguintes;
- garante que o seu sistema de qualidade esteja em conformidade com as normas ISO 9001;
- assegura que o dispositivo para a criação de assinatura (HSM) tenha os requisitos de segurança previstos pelo artigo 29.º do Reg. eIDAS;
- emite e torna público o certificado qualificado, salvo indicação em contrário do Titular, de acordo com o estabelecido no Art. 32.º do CAD;
- informa os requerentes, explícita e claramente, sobre o procedimento de certificação, sobre os requisitos técnicos
  necessários de acesso, sobre as características e limitações do uso das assinaturas emitidas com base no serviço de certificação;
- cumpre as medidas de segurança para o tratamento de dados pessoais (RGPD);
- não é depositário de dados para a criação da assinatura do Titular;
- procede à publicação da revogação e suspensão do certificado eletrónico em caso de solicitação por parte

do Titular ou do terceiro interessado;

- assegura a determinação precisa da data e hora da emissão, revogação e suspensão dos certificados eletrónicos;
- mantém um registo, também eletrónico, de todas as informações relativas ao certificado qualificado por 20 (vinte) anos, em particular a fim de comprovar a certificação em eventuais processos judiciais;
- assegura que o código de identificação (exclusivo do QTSP) atribuído a cada Titular seja único entre os seus utilizadores;
- fornece em meios de comunicação duradouros todas as informações úteis para os indivíduos que solicitem o serviço de certificação. Isto inclui: os termos e condições exatos relativos ao uso do certificado, incluindo qualquer limitação de uso, a existência de um sistema de acreditação facultativo e os procedimentos de reclamação e de resolução de disputas. Estas informações, que podem ser transmitidas eletronicamente, devem ser escritas em linguagem clara e fornecidas antes do acordo entre o solicitante do serviço e o QTSP;
- utiliza sistemas fiáveis para gerir o registo de certificados de forma a garantir que apenas as pessoas autorizadas possam efetuar entradas e alterações, que a autenticidade das informações seja verificável, que os certificados sejam acessíveis para consulta pública apenas nos casos permitidos pelo Titular do certificado e que o operador possa aperceber-se de qualquer evento que compromete os requisitos de segurança;
- regista a emissão de certificados qualificados no registo de controlo com a especificação da data e hora da criação.

De acordo com as disposições do Art. 14.º do DPCM, o Certificador fornece ou, pelo menos, indica um sistema que permite a verificação das assinaturas digitais.

Além disso, o QTSP:

- gera um certificado qualificado, para cada uma das chaves avançadas de assinatura eletrónica utilizadas pela Agência para a Itália Digital para a assinatura da lista pública de certificadores, e publica-a no registo próprio de certificados nos termos do Art. 42.º do DPCM;
- indica um sistema de verificação de assinatura eletrónica, conforme o Art. 10.º do DPCM;
- conserva uma cópia da lista, assinada pela Agência para a Itália Digital, dos certificados relativos às chaves de certificação de acordo com o Art. 43.º do DPCM, e disponibiliza-a por via telemática, conforme estabelecido no Art. 42.º, parágrafo 3, do DPCM.

C.2. Obrigações do Titular

O Titular que solicita um certificado qualificado para os serviços descritos no presente Manual de Operação é um cliente do Banco ou da Instituição de Pagamento, que atua como Registration Authority.

O Titular receberá um certificado qualificado para a Assinatura Eletrónica Qualificada Remota, com a qual será possível assinar contratos e documentos relativos a produtos e/ou serviços oferecidos pelo Banco/Instituição das formas descritas no par. .

O Titular deve conservar as informações necessárias para a utilização da sua chave de assinatura privada de forma adequada e deve adotar todas as medidas organizacionais e técnicas adequadas para evitar danos a terceiros (CAD, Art. 32.º, parágrafo 1).

O Titular da chave deve também:

- fornecer todas as informações exigidas pelo QTSP, garantindo a sua fiabilidade sob sua própria responsabilidade;
- enviar o pedido de certificação de acordo com os meios indicados neste Manual de Operação;
- comunicar ao QTSP, mesmo que através da LRA, quaisquer alterações nas informações fornecidas no momento do registo: dados pessoais, morada, números de telefone, endereço de e-mail, etc.;
- conservar as informações de habilitação ao uso da chave privada com o máximo cuidado e diligência;
- informar imediatamente as autoridades competentes e o Banco/Instituição em caso de perda ou roubo dos códigos e/ou dispositivos indicados para aceder às suas chaves de assinatura; o Banco/Instituição procederá à revogação imediata do certificado;

- encaminhar quaisquer pedidos de revogação e suspensão do certificado qualificado, conforme indicado neste Manual de Operação.

C.3. Obrigações dos utilizadores dos certificados

O Utilizador (*Relying Party*) é qualquer pessoa que receba um documento assinado digitalmente e, para verificar a sua validade, recorra ao Certificado Qualificado utilizado pelo Titular para assinar o próprio documento.

A verificação da assinatura digital e a subsequente extração dos objetos assinados podem ser realizadas com qualquer software que permita processar ficheiros assinados de acordo com o Reg. eIDAS.

Os utilizadores que recorram a um Certificado Qualificado para verificar a validade de um documento assinado digitalmente devem:

- verificar a validade do certificado que contém a chave pública do Titular da mensagem, conforme indicado pelas normas em vigor no momento da sua emissão;
- verificar o estado de validade do certificado usando o protocolo OCSP ou através do acesso às Listas de Revogação;
- verificar a validade do percurso de certificação, com base na lista pública dos QTSP;
- verificar a existência de quaisquer limitações no uso do certificado utilizado pelo Titular.

C.4. Obrigações do Terceiro em Causa

O Terceiro em Causa, nos serviços descritos neste Manual de Operação, é o Banco ou a Instituição de pagamento. Portanto, o Banco/Instituição, na qualidade de Terceiro em Causa:

- verifica se o Cliente possui todos os requisitos necessários e autoriza o Cliente a solicitar a emissão do Certificado Qualificado para a Assinatura Digital Remota.
- desenvolve uma atividade de suporte ao Titular
- indica ao QTSP eventuais limitações adicionais no uso do Certificado Qualificado para a Assinatura Digital, além das previstas no par. *F.1.1*.

Portanto, o Banco/Instituição, enquanto Terceiro em Causa, pode indicar ao QTSP quaisquer limitações de uso do certificado,
eventuais poderes de representação e deve comunicar quaisquer alterações a estes. A título de exemplo, indicam-se as seguintes circunstâncias:

- alteração ou cessação de poderes de representação;
- alteração de cargos e qualificações internas;
- cessação de contratos de trabalho.

O pedido de revogação ou suspensão enviado pelo Terceiro em Causa à LRA deve ser imediatamente encaminhado para a CA caso deixem de existir os requisitos na base da emissão de um certificado qualificado para a assinatura eletrónica ao Titular.

C.5. Obrigações das Registration Authorities externas (LRA)

O QTSP INTESA, por exigências ligadas à prestação do serviço, recorre a outras entidades em todo o território nacional (de ora em diante denominadas RA externas ou LRA - Local Registration Authority) para realizar parte das atividades específicas do Gabinete de registo.

O QTSP In.Te.S.A. S.p.A. solicita o desempenho da função de Registration Authority ao Banco ou à Instituição de pagamento por meio de um *Contrato de Mandato* específico, assinado por ambas as partes.

Em particular, as RAs externas realizam as seguintes atividades:

- identificação com certeza do requerente da certificação (de ora em diante Titular do certificado);
- registo do requerente/Titular;
- entrega ao Titular dos dispositivos e/ou códigos que lhe permitirão aceder à sua chave de assinatura em conformidade com os Art. 8.º e 10.º, parágrafo 2, do DPCM;

- envio da documentação assinada ao Gabinete RA do QTSP INTESA, exceto acordo em contrário no contrato de mandato.

No Contrato de Mandato são especificadas as obrigações que o Banco/Instituição à qual o QTSP INTESA atribui a posição de LRA deve cumprir e que o QTSP é obrigado a monitorizar.

Em particular, solicita-se à LRA que:

- garanta que a atividade de identificação seja realizada em conformidade com as normas em vigor (CAD e modificações e adendas seguintes, DPCM, Reg. eIDAS e norma em matéria de combate ao branqueamento de capitais);
- utilize e trate os dados pessoais recolhidos durante o reconhecimento de acordo com o RGPD;
- disponibilize ao QTSP INTESA o material recolhido durante a fase de identificação e registo.

O serviço de identificação (*verificação adequada*) pode ser gerido de três formas diferentes, descritas em seguida:

- *Padrão*: o Requerente é identificado numa agência do Banco ou da Instituição de Pagamento;
- *On demand*: ao abrir uma nova conta corrente, o Requerente pode solicitar que seja contactado por um *Personal Financial Adviser* que, após a marcação de uma reunião, apoiará o Cliente em todos os procedimentos relativos à abertura de uma Conta Corrente. Nesta fase, o Cliente será orientado (após ter sido identificado e registado) também no pedido de um certificado de assinatura eletrónica qualificada;
- *Online*: se o Requerente escolher o modo de adesão direta e já for titular de uma conta corrente num Banco em território nacional, para ser reconhecido para fins legais, poderá:
  - utilizar um procedimento SEPA (ou SDD - SEPA Direct Debit);
  - realizar uma transferência a partir da conta corrente anteriormente aberta no Banco.

Através dos procedimentos acima mencionados, a LRA do Banco ou da Instituição de Pagamento passará a possuir todas as
informações exigidas por lei, em total segurança e em pleno respeito pela privacidade.

D. Responsabilidade e limitações das indemnizações

D.1. Responsabilidade do QTSP - Limitações das indemnizações

O INTESA QTSP é responsável perante os Titulares pelo cumprimento de todas as obrigações decorrentes do desempenho das atividades previstas pelo DPCM, pelo RGPD, pelo CAD e pelo Reg. eIDAS (e todas as suas modificações e adendas seguintes), conforme descrito no par. *C.1. Obrigações do Prestador de Serviços de Confiança Qualificado (QTSP)*.

A INTESA, sem prejuízo dos casos de fraude ou negligência (Reg. eIDAS, Art. 13.º), não assume qualquer responsabilidade pelas consequências decorrentes de um uso de certificados que não seja o disposto pelo Art. 5.º do DPCM e, em particular, do incumprimento da parte do Titular e do Terceiro em Causa das indicações do presente Manual de Operação e/ou do incumprimento por parte dos mesmos da norma em vigor.

Da mesma forma, a INTESA não poderá ser responsabilizada pelas consequências devido a causas que não lhe possam ser atribuídas como, por exemplo: desastres naturais, ineficiências e/ou disfunções técnicas e logísticas fora do seu controlo, intervenções da Autoridade, revoltas ou atos de guerra que afetem também ou apenas os sujeitos a cujas atividades a INTESA recorre para a prestação dos seus serviços de certificação.

O QTSP INTESA não se responsabiliza por danos resultantes do uso não conforme do Certificado Qualificado para a Assinatura Digital Remota em relação à limitação de uso, conforme especificado no par. *F.1.1*.

O Titular, após a leitura deste Manual de Operação, deve implementar todas as medidas de diligência especial destinadas a evitar danos a terceiros relacionados com o uso inadequado do que é fornecido pelo certificador acreditado. Em particular, lembramos que se devem conservar com os devidos cuidados os dispositivos OTP e os códigos secretos necessários para aceder às chaves de assinatura.

D.2. Seguro

O QTSP INTESA é beneficiário de contratos de seguro para cobertura dos riscos da atividade e dos danos causados a terceiros, cujo conteúdo está em linha com o necessário para a realização da atividade profissional em questão.

É enviada aos AgID uma declaração específica de estipulação deste contrato.

E. Tarifas

O Serviço é fornecido pelo Banco ou Instituição de pagamento aos seus Clientes: as Tarifas de emissão, renovação, revogação e suspensão do certificado qualificado serão indicadas nos contratos estipulados entre o Cliente e o Banco/Instituição.

F. Métodos de identificação e registo dos utilizadores

F.1. Identificação dos utilizadores

O QTSP deve verificar com certeza a identidade do requerente no momento do primeiro pedido de emissão de certificado
qualificado.

A referida operação é solicitada ao Banco/Instituição que, na qualidade de LRA e em conformidade com as disposições da norma em matéria de combate ao branqueamento de capitais, identificará e registará o Titular.

Para renovações subsequentes, se realizadas quando o certificado qualificado ainda se encontra dentro da validade, esta atividade não deve ser repetida: será da responsabilidade do Titular comunicar ao QTSP através do Banco/Instituição quaisquer alterações relativas aos seus dados de registo.

Entre os dados de registo necessários para a execução do serviço objeto do presente documento, relembramos:

- nome e apelido;
- data de nascimento;
- concelho ou país estrangeiro de nascimento;
- NIF;
- morada de residência;
- morada para envio de comunicações em papel;
- número de telemóvel;
- endereço de correio eletrónico;
- tipo e número do documento de identidade apresentado;
- autoridade que emitiu o documento e data e local da emissão e de validade.

No final desta fase de registo, poderá ser emprestado ao Titular um dispositivo One Time Password com ecrã e capaz de gerar códigos numéricos de utilização única (de ora em diante *códigos OTP* ou simplesmente *OTP*).

Em alternativa a um token OTP físico, o Banco ou a Instituição de pagamento poderão indicar aos Titulares como ativar um sistema de autenticação através de software para dispositivos móveis (caso o Titular disponha de um e prefira este método por ser mais prático do que o uso de um token físico). Este sistema de software permitirá gerar uma One Time Password no dispositivo móvel do Titular e poderá portanto ser utilizado como instrumento de autenticação para os sistemas de assinatura remota.

Além do OTP, serão fornecidas ao Titular todas as informações necessárias e um *Personal Identification Number* (*PIN*) que lhe podem garantir um acesso seguro ao serviço de assinatura remota disponibilizado pelo Banco/Instituição.

O mesmo PIN poderá ser utilizado como código de emergência (em caso, por exemplo, de desaparecimento e/ou perda do Token OTP ou dispositivo móvel) para suspender com urgência o seu certificado qualificado (par. *H.2.2*).

O PIN poderá posteriormente ser alterado ou atualizado pelo Titular usufruindo dos serviços que o Banco ou a Instituição de Pagamento terão colocado à disposição.

Nesta fase são também fornecidas ao Titular as informações necessárias para lhe permitir alterar a qualquer momento o número de telemóvel anteriormente fornecido.

Além disso, diretamente ao balcão do Banco/Instituição, ou posteriormente, ligando-se ao serviço de internet banking disponibilizado pelo mesmo Banco/Instituição, mas de qualquer forma antes do pedido de emissão de certificado qualificado, o Titular deverá:

- ler o Manual de Operação do QTSP INTESA;
- autorizar o Banco ou Instituição de pagamento ao tratamento dos seus dados pessoais para as finalidades ligadas à emissão de um certificado qualificado para assinatura eletrónica.

A documentação anterior, relativa ao registo dos Titulares, é guardada durante 20 (vinte) anos a partir da vencimento do certificado.

F.1.1. Limites de uso

No Certificado Qualificado para assinatura eletrónica, emitido no âmbito dos serviços descritos no presente manual e disponibilizados pelo Banco/Instituição, é sempre inserido um limite de uso.

A fórmula padrão é a seguinte:

O uso do certificado é limitado às relações com** Nome do Banco / Instituição**. This certificate may only be used in dealings with** Nome do Banco / Instituição**.

Podem ser concordados limites de uso específicos com o Banco ou Instituição de Pagamento.
A INTESA não se responsabiliza por danos derivantes do uso de um certificado qualificado que exceda os limites estabelecidos ou derivantes da ultrapassagem desse limite.

F.1.2. Títulos e habilitações profissionais

Caso seja exigida a indicação, no certificado qualificado, das habilitações profissionais (por exemplo, a associação a uma ordem profissional), o requerente deve apresentar documentação adequada que demonstre a existência efetiva dessas habilitações profissionais ou documentação equivalente.

Uma cópia desta documentação é guardada por 20 (vinte) anos a partir do vencimento do certificado.

A documentação de apoio do pedido de inserção de títulos ou habilitações profissionais no certificado qualificado não pode ser anterior a 10 (dez) dias à data de apresentação do pedido de emissão do referido certificado.

A INTESA não se responsabiliza por danos derivantes do uso inadequado de um certificado qualificado com informações relativas a habilitações profissionais.

Em caso de autocertificação, a INTESA não assume qualquer responsabilidade, exceto nos casos de fraude ou negligência (Reg. eIDAS, Art. 13.º), pela possível inclusão no certificado de informações autocertificadas pelo Titular.

F.1.3. Poderes de representação

Caso seja exigida a indicação no certificado qualificado de poderes de representação (por exemplo, a associação a uma organização e o cargo ocupado, a autorização para operar em nome e por conta de um Cliente, etc.), o requerente deve apresentar documentação adequada que demonstre a existência efetiva de tais poderes de representação.

Para a representação de pessoas singulares, o requerente deve apresentar uma cópia autenticada da procuração assinada pela pessoa representada, juntamente com o certificado de autorização desta última para a inclusão da função no certificado.

Caso seja exigida a indicação no certificado de uma função relativa à representação de organizações ou entidades de direito privado, o Titular deverá apresentar documentação para comprovar a função para a qual é pedida a inclusão no certificado e uma declaração da organização ou da entidade à qual pertence, mediante a qual a instituição ou organização autoriza o QTSP a inserir a função específica no certificado. Este último documento não pode ser anterior a 20 (vinte) dias à data de pedido de emissão do certificado qualificado.

A introdução no certificado qualificado de informações relativas ao exercício de funções públicas ou poderes de representação de entidades e organizações de direito público estará sujeita a acordos específicos com as próprias entidades. Com bases nesses acordos, será possível especificar o papel desempenhado pelo Titular na entidade ou organização pública.

A documentação apresentada será guardada por um período de 20 (vinte) anos.

A INTESA não se responsabiliza por danos derivantes do uso inadequado de um certificado qualificado com informações relativas a poderes de representação.

F.1.4. Uso de pseudónimos

O Titular pode solicitar, em casos particulares, que o certificado apresente um Pseudónimo em alternativa aos seus dados reais.

As informações relativas à identidade real do utilizador serão guardadas por 20 (vinte) anos.

F.2. Registo dos utilizadores que requerem a certificação

Após a fase de identificação, é executado o registo dos dados dos Titulares nos arquivos da Certification Authority.

Esta operação poderá ser executada através de uma aplicação de software que pode ser realizada diretamente a partir
das aplicações do Banco ou Instituição de Pagamento.

G. Criação de chaves de Certificação, Selo Temporal e assinatura

G.1. Criação de chaves de certificação

A criação de chaves dentro dos dispositivos de assinatura é feita na presença do Responsável de Certificação, tal como previsto pelo DPCM, Art. 7.º.

A referida operação é precedida pela inicialização dos dispositivos de assinatura para o sistema de criação de certificados com os quais se assinam os certificados dos Titulares e os do sistema de selo temporal.

Tudo isto é feito em modo dual control para evitar operações ilícitas.

As operações sucessivas após a criação dos pares de chaves do Certificador só são possíveis através de dispositivos particulares de autorização (token usb): o acesso privilegiado aos HSM só pode ser feito através das chaves contidas nesses dispositivos de autorização acima referidos.

Para maior segurança, estas chaves são divididas em vários dispositivos, segundo uma lógica do tipo "*n de m*", de forma que apenas a presença concomitante de pelo menos *n* de *m* partes da chave permita operar com os privilégios adequados. Assim, estas são guardadas em cofres distintos.

A extensão das chaves de certificação é de pelo menos 2048 bits.

G.2. Criação de chaves do sistema de selo temporal

A criação de chaves de selo temporal é realizada em conformidade com o estabelecido pelo Art. 49.º do DPCM. A extensão das chaves do sistema de selo temporal é de pelo menos 2048 bits.

G.3. Criação de chaves de assinatura

Terminada a fase de registo, durante a qual os dados dos Titulares são memorizados nos arquivos do Certificador, é possível proceder à criação das chaves de assinatura.

O Titular poderá iniciar o procedimento de criação das chaves e pedido do Certificado de assinatura associado à mesma numa das modalidades descritas no par. *I. Modalidades operativas para a assinatura de documentos*.

Os pares de chaves de assinatura são criados em dispositivos de assinatura seguros (HSM – Hardware Security Module),
em conformidade com as especificações do *Anexo II* do Reg. eIDAS.

A extensão das chaves de assinatura é de pelo menos 2048 bits.

H. Modalidade de emissão dos certificados

H.1. Procedimento de emissão dos Certificados de certificação

Após a criação das chaves de certificação, descrita no par. *G.1*, são criados os certificados das chaves públicas, em conformidade com o disposto pelo DPCM, assinados com as respetivas chaves privadas e registados no registo dos certificados conforme as modalidades previstas.

Os certificados das chaves de certificação são enviados para a Agência para a Itália Digital através do sistema de comunicação referido no Art. 12.º, parágrafo 1, do DPCM.

O Certificador gera um certificado qualificado para cada uma das chaves de assinatura eletrónica qualificada utilizadas pela Agência para a assinatura da lista pública dos certificadores e publica-o no seu registo de certificados. O Certificador deve depois guardar uma cópia da lista, assinada pelo departamento, dos certificados relativos às chaves de certificação, e torná-la disponível por via telemática (DPCM, Art. 42.º, parágrafos 1 e 3).

H.2. Procedimento de emissão dos Certificados de assinatura

A INTESA emite certificados com um sistema em conformidade com o Art. 33.º do DPCM.

Após a criação do par de chaves de assinatura, descrita no par. *G.3*, é gerado um pedido de novo certificado no formato *PKCS#10*, que fornece automaticamente a prova de posse da chave e a verificação do funcionamento correto do par de chaves.

Depois de geradas as chaves, o pedido de certificado será imediatamente enviado pela aplicação do Banco / Instituto Financeiro à Certification Authority do QTSP.

A criação dos certificados é registada no registo de controlo (DPCM, Art. 18.º, parágrafo 4).

H.2.1. Informações contidas nos certificados de assinatura

Os certificados INTESA, emitidos no âmbito do presente manual, são certificados qualificados nos termos do Regulamento (UE) 910/2014 (eIDAS) e, portanto, é garantida a sua interoperabilidade e reconhecimento a nível comunitário.

O Certificado Qualificado define com certeza o Certificador que o emitiu e contém os dados necessários para a verificação da Assinatura Digital.

Cada Certificado Qualificado para a assinatura eletrónica está em conformidade com o Regulamento eIDAS e com a DETERMINAÇÃO AgID N. 147/2019 (*Linhas de orientação com as Regras Técnicas e Recomendações relativas à criação de certificados*).

Todos os Certificados Qualificados emitidos no âmbito dos serviços descrito no presente Manual contêm um limite de uso (par. *F.1.1*).

H.2.2. Código de Emergência

O Certificador garante, em conformidade com o disposto no Art. 21.º do DPCM, um *código de emergência* a utilizar para pedir a ***suspensão urgente*** do Certificado.

Nas aplicações descritas no presente Manual de Operações, será considerado como código de emergência o PIN entregue ao Titular no momento do seu registo.

I. Modalidades operativas para a assinatura de documentos

O QTSP INTESA, através dos serviços do Banco ou da Instituição de pagamento, disponibiliza ao Titular tudo o que é necessário para criar assinaturas eletrónicas qualificadas conforme previsto pela norma vigor.

Este tipo de serviço específico não exige o fornecimento de uma aplicação de assinatura para instalar no seu computador pessoal, mas sim funções de assinatura que podem ser recuperadas ou acedendo ao serviço de home banking do Banco ou da Instituição de Pagamento ou diretamente ao balcão de uma agência do Banco ou do Instituto de Pagamento.

As assinaturas eletrónicas qualificadas obtidas através destes procedimentos estarão necessariamente em conformidade com o
previsto pelo DPCM no Art. 4.º, parágrafo 2, relativo aos algoritmos utilizados.

Além disso, estes documentos, conforme exigido pelo Art. 4.º, parágrafo 3, do mesmo DPCM, não conterão macro instruções ou códigos executáveis, para ativar funcionalidades que podem, sem o conhecimento do assinante, modificar atos, factos e dados nos próprios documentos.

Em seguida são descritas duas modalidades diferentes de autenticação que, em conformidade com a norma em vigor, permitem a um Titular, depois de registado, prosseguir primeiro com a geração das chaves de assinatura e pedido de um certificado qualificado e, em seguida, utilizá-los para executar assinaturas eletrónicas qualificadas.

A confirmação da execução das operações de assinatura será feita através de SMS. Se o Titular tiver um smartphone habilitado para a leitura da correspondência, a pedido do Titular, em alternativa, poderão ser enviados e-mails.

I.1. Autenticação de tipo “Call Drop”

Esta modalidade de autenticação exige que o utilizador, previamente identificado, efetue uma chamada com o seu número de telemóvel (do mesmo número fornecido na fase de identificação) para um número de telefone específico, fornecido no âmbito do serviço, para confirmar a sua intenção de assinar um documento.

Ao receber a referida chamada telefónica, é verificada a proveniência através do número de telefone (*Call Identifier*) anteriormente associado ao utilizador na fase de registo e, em caso de verificação positiva, é autorizada a operação de assinatura eletrónica qualificada.

Portanto, quando o Titular quiser assinar um documento acedendo ao portal do Banco/Instituição, utilizará uma autenticação de dois fatores digitando um PIN (informação que apenas o utilizador conhece) e um número de telefone (fornecido pelo cartão SIM, que apenas o utilizador possui).

Este tipo de autenticação também é chamado "*Call Drop*", pois quando o Titular liga para ser autenticado não é ativada nenhuma conversação e, após alguns segundos, a chamada é encerrada.

O utilizador Titular nunca recebe uma resposta à sua chamada e, portanto, não incorre em nenhum custo telefónico.

Entre as vantagens desta técnica estão o baixo custo e a praticidade, pois não é necessário o uso de nenhum dispositivo físico de autenticação e é muito fácil de usar.

Veremos mais adiante como esta autenticação descrita acima é muito apreciada quando o Titular opera em terminais sem pessoal (normalmente ligando-se aos serviços do Banco ou da Instituição de Pagamento com o seu próprio PC através dos serviços de home banking disponibilizados pelo Banco ou pela Instituição de Pagamento) mas, pelo contrário, não é praticável quando o Titular se encontra perante um operador externo, por exemplo, num terminal dotado de pessoal, por um caixa do Banco ou da Instituição de Pagamento.

Para gerir estas últimas situações, foi estudada uma solução baseada numa gestão dinâmica dos números de telefone para os quais ligar para finalizar o processo de autenticação precisamente naquilo a que chamaremos terminais dotados de pessoal.

I.1.1. Processo de assinatura em terminais sem pessoal (Home banking)

Quando estiver na posse dos códigos necessários durante a fase de identificação, o Titular poderá, posteriormente, solicitar o seu Certificado digital e proceder à assinatura de um documento nas modalidades descritas abaixo.

1. O Titular liga-se à aplicação bancária ou financeira através dos seus códigos pessoais para acesso à aplicação;
2. Seleciona e verifica o documento a assinar;
3. Introduz o seu código PIN;

4. Depois de validado o PIN, o Titular, num tempo configurado (não superior ao primeiro minuto) e utilizando o telemóvel anteriormente registado, deve confirmar a sua intenção de assinar o documento, e ligar imediatamente para um número telefónico que surgirá entretanto no ecrã;
5. O sistema, verificando que o número que está a ligar é o previamente registado e associado ao Titular, prossegue com a operação de assinatura e envia uma confirmação de que a operação foi concluída com sucesso;
6. Se, por outro lado, tiver decorrido o tempo definido sem que o sistema tenha recebido uma chamada para o número indicado no ponto 4, a operação será considerada nula e concluída sem a assinatura do documento.

Se os documentos a assinar forem mais do que um, o Titular deverá repetir os passos 2 a 5 para cada documento.

I.1.2. Processo de assinatura em terminais dotados de pessoal (balcão de agência bancária ou financeira)

Uma vez obtido o certificado qualificado, o Titular pode proceder à assinatura de um documento.

Como mencionado acima, ao balcão de uma agência bancária ou financeira e perante um operador, pode ser difícil para o Titular inserir códigos pessoais e confidenciais, como por exemplo um PIN.

Assim, pensou-se numa solução alternativa, que garanta ainda assim a máxima segurança:

1. o utilizador dirige-se ao balcão de uma agência do Banco/Instituição (terminal dotado de pessoal) e é reconhecido pelo pessoal (o caixa, por exemplo) da forma habitual;
2. Depois de visionado o documento a assinar, o Titular poderá iniciar o processo de assinatura;
3. Nesta altura, é disponibilizado num ecrã, visível para o Titular, um número de telefone (escolhido aleatoriamente dentro de um conjunto amplo de números disponíveis) a ao mesmo tempo é iniciada a contagem num temporizador;
4. O Titular, dentro de um tempo configurado não superior a um minuto, deve ligar para o número que apareceu no ecrã (utilizando o seu telemóvel, previamente registado) para confirmar a sua intenção de assinar o documento;
5. Neste momento, se o sistema detetar que o número que está a ligar está correto, executa a assinatura do documento e envia via SMS uma confirmação da operação;
6. Se, pelo contrário, se esgotar o tempo estabelecido sem que o sistema tenha recebido uma chamada para o número
indicado no ponto 3, a operação é anulada.

Se os documentos a assinar forem mais do que um, o Titular deverá repetir os passos 2 a 5 para cada documento.

I.2. Autenticação de tipo OTP Mobile

Em alternativa ao instrumento de autenticação Call Drop, está disponível uma segunda modalidade de autenticação, denominada "*OTP Mobile*".

Para ativar esta modalidade, o Titular deverá dispor de um smartphone entre os especificados pelo Banco/Instituição como adequados para esse serviço.

Depois de executada esta verificação, em fase de identificação ao balcão do Banco/Instituição onde foi feito o registo, será comunicado ao Titular um endereço de internet específico no site do Banco ou da Instituição de Pagamento de onde poderá descarregar no seu smartphone uma aplicação definida de "*OTP Mobile*" e ser-lhe-á entregue um PIN.

Também para esta segunda modalidade de autenticação descrevemos o processo de assinatura, dependendo se a mesma se realizar em terminais com ou sem pessoal.

I.2.1. Processo de assinatura em terminais sem pessoal (Home banking)

Quando está na posse do seu certificado qualificado, o Titular pode assinar um documento através dos seguintes passos:

1. O Titular liga-se à aplicação bancária ou financeira através dos seus códigos pessoais para acesso à aplicação;
2. Seleciona e verifica o documento a assinar;
3. Introduz o seu PIN;
4. Liga a aplicação anteriormente descarregada no seu smartphone recebendo uma OTP Mobile que deve inserir após o PIN;
5. O sistema, ao detetar que o PIN e a OTP Mobile acabados de inserir estão corretos, procede à operação de assinatura e envia uma confirmação do sucesso da operação.

Se os documentos a assinar forem mais do que um, o Titular deverá repetir os passos 2 a 5 para cada documento.

I.2.2. Processo de assinatura em terminais dotados de pessoal (balcão de agência bancária ou financeira)

Também neste caso foi estudada uma solução que não exige que o Titular insira códigos confidenciais à frente do pessoal do Banco ou da Instituição de Pagamento, que poderão ser reutilizados de forma fraudulenta em seu prejuízo.

Quando está na posse do seu certificado qualificado, o Titular pode assinar um documento da seguinte forma:

1. O utilizador dirige-se ao balcão de uma agência do Banco ou Instituição de pagamento (terminal dotado de pessoal) e é reconhecido pelo pessoal (o caixa, por exemplo) da forma habitual;
2. No momento da assinatura, é ativado à frente do utilizador um monitor específico equipado com uma webcam;
3. O Titular, depois de verificar neste monitor o documento a assinar e decidir prosseguir com a operação de assinatura, lança a partir do seu smartphone a criação de um OTP que é exibido também em formato de código de barras;
4. O Titular pode então, colocando o smartphone virado para a webcam, permitir a leitura do OTP gerado no passo 3 e iniciar o procedimento de assinatura real;
5. Depois de o documento ter sido assinado, o Titular será notificado imediatamente através do envio de um SMS.

Para assinar mais documentos, devem ser repetidos os passos 2 a 5.

I.2.3. Processo de assinatura para clientes Prospect

O processo de emissão do Certificado qualificado de assinatura remota também pode ser gerido por um Cliente Prospect durante as atividades de Onboarding (aquisição do Cliente).

O processo é compatível com os principais browsers (Chrome, Firefox, Edge, Safari) e com os dispositivos móveis mais recentes da família Android e Apple.

Articula-se como se segue:

1. Ao iniciar o processo, pede-se ao Cliente Prospect a introdução do seus dados pessoais para permitir uma posterior identificação certa, mediante prévia assinatura da política de privacidade do QTSP INTESA;
2. O Banco/Instituição procede ao envio de um SMS cujo texto contém uma OTP (One Time Password) com validade temporária: solicita-se ao Cliente Prospect que introduza esse código, para verificar a efetiva disponibilidade do dispositivo móvel indicado na fase de introdução dos dados;
3. Completada a verificação referida no ponto anterior, o Cliente Prospect transmite então os documentos de identidade ao Banco/Instituição: os dados pessoais serão inseridos pelo Prospect ou adquiridos a partir dos documentos através de um sistema de OCR;
4. Concluída a fase de registo, o Banco enviará ao Cliente Prospect a documentação contratual que o Cliente Prospect poderá assinar com um certificado qualificado de assinatura digital remota (FDR) emitido pelo QTSP INTESA;

5. Ao Cliente Prospect, juntamente com o procedimento descrito para o internet banking, será apresentada a
documentação de pedido do certificado do QTSP INTESA;
6. A visualização da mesma deverá ser obrigatoriamente comprovada marcando as caixas de verificação do documento e inserindo uma assinatura eletrónica através da introdução de uma OTP recebida através de SMS do QTSP INTESA;
7. Se a OTP fornecida pelo QTSP INTESA estiver correta, poderá proceder-se à emissão de um certificado qualificado, caso contrário, deverá ser solicitada uma nova OTP;
8. No momento da criação do certificado, é indispensável que seja inserido um PIN, que será depois necessário a cada utilização do certificado de assinatura;
9. O certificado acabado de emitir poderá ser utilizado apenas para assinar a proposta contratual e nenhum outro documento até que o Banco tenha completado as verificações propedêuticas necessárias para a abertura de uma conta corrente;
10. Se as verificações do Banco forem bem sucedidas e se a conta corrente for ativada, o Cliente Prospect poderá
utilizar o certificado emitido, respeitando os seus limites de uso, nas relações com o Banco;
Se, pelo contrário, o Banco decidir não dar seguimento ao pedido de abertura de uma conta corrente, o mesmo certificado será revogado inibindo a sua utilização;
11. Em ambos os casos referidos no ponto anterior, o Cliente Prospect será informado sobre o resultado das verificações e sobre a eventual revogação do certificado.

I.3. Autenticação com Token OTP

Por fim, pode ser utilizada uma autenticação ligada ao uso de Tokens OTP físicos (muito comuns no mundo bancário e financeiro).

O uso deste Token OTP físico está atualmente previsto apenas para acessos em terminais sem pessoal (normalmente um
posto remoto de home banking).

O Titular liga-se à aplicação bancária ou financeira através dos seus códigos pessoais para acesso à aplicação e, para iniciar o procedimento de assinatura, deverá inserir o PIN e o código OTP que terá entretanto gerado e visualizado no ecrã do Token.

J. Modalidades operativas para a verificação da assinatura

Os documentos assinados com as modalidades descritas anteriormente serão exclusivamente em formato PDF: este
formato de assinatura é considerado de fácil utilização no âmbito das aplicações bancárias ou financeiras.

A verificação dos documentos assinados poderá ser facilmente efetuada utilizando o software *Acrobat Reader DC*, aplicação capaz de verificar todos os tipos de assinatura eletrónica qualificada em formato PDF produzidas na União Europeia em conformidade com o Regulamento eIDAS.

Acrobat Reader DC pode ser descarregado gratuitamente a partir do site da Adobe, *https://www.adobe.com/it/*

K. Modalidade de revogação e suspensão dos certificados

Em conformidade com o Reg. eIDAS, as informações sobre o estado do certificado estão disponíveis através de protocolo OCSP, no URL
indicado no próprio certificado.

A revogação e a suspensão dos certificados podem ser confirmadas também pela sua introdução na lista CRL (Art. 22.º do DPCM). O perfil das CRL está em conformidade com a norma standard RFC 3280. Esta lista, assinada pela Certification Authority que emite o certificado, é atualizada com periodicidade predefinida e em conformidade com a norma em vigor.

A lista CRL está disponível também no registo dos certificados.

Nos casos em que a revogação ou a suspensão ocorram por iniciativa do Certificador ou do Terceiro em Causa, (artigos 23.º, 25.º, 27.º e 29.º do DPCM), o Certificado notifica ao Titular o pedido e o momento em que entrará em vigor o evento em questão.

Em fase de pedido, serão especificadas a data e a hora a partir das quais o certificado será revogado (Art. 24.º, parágrafo 2, DPCM).

K.1. Revogação dos certificados

Um certificado pode ser revogado a pedido do Titular, do Terceiro em Causa ou da Certification Authority (ou seja, do QTSP).

Um certificado revogado não poderá de nenhuma forma ser reativado.

K.1.1. Revogação a pedido do Titular

O Titular pode solicitar a revogação acedendo a uma secção específica disponibilizada no âmbito dos serviços do Banco ou da Instituição de Pagamento ou entrando em contacto direto com o Apoio ao Cliente do Banco ou da Instituição de Pagamento.

O QTSP, avisado pelo Banco/Instituição, que entretanto terá também bloqueado os códigos de acesso do Titular, procederá à revogação imediata do certificado.

K.1.2. Revogação a pedido do Terceiro em Causa

O Banco ou a Instituição de Pagamento, na qualidade de Terceiro em Causa, podem solicitar a revogação do certificado.

O QTSP, verificada a correção do pedido, notificará os Titulares em causa sobre a revogação utilizando os canais de comunicação definidos com o Titular no momento do registo ou posteriormente atualizados e comunicados pelo Titular ao QTSP, incluindo através das LRA (par. *C.2. Obrigações do Titular*).

K.1.3. Revogação por iniciativa do Certificador

O Certificador que pretenda revogar o Certificado Qualificado, exceto em casos de urgência motivada, envia uma comunicação prévia por e-mail ou correio eletrónico certificado ao Banco/Instituição (Terceiro em causa) e, ao mesmo tempo, será comunicado ao Titular através do endereço de e-mail fornecido em fase de pedido do certificado ou para a morada de residência, especificando os motivos da revogação, bem como a data e a hora a partir das quais a revogação terá efeito.

K.1.4. Revogação dos certificados relativos a chaves de certificação

Nos casos de:

- comprometimento da chave de certificação,
- cessação de atividade,

o Certificador procede à revogação dos certificados de certificação correspondentes e dos certificados de assinatura assinados com a mesma chave de certificação.

No prazo de 24 horas, o Certificador irá notificar a Agência para a Itália Digital e os Titulares sobre a revogação.

K.2. Suspensão dos certificados

Sobre as modalidades de suspensão e notificação da mesma, é válido o que foi dito para a modalidade de revogação no par. *K.1*.

A suspensão de um certificado é prevista caso se tenha de realizar uma avaliação adicional para verificar se este tem de ser efetivamente revogado (por exemplo, nos casos em que se suspeite de desaparecimento/furto do Token OTP, ou se for necessário verificar a efetiva cessação do Titular do cargo para o qual lhe tinha sido emitido o certificado, etc.).

O pedido de suspensão pode ser feito por todas as entidades previstas pelo DPCM nos Art. 27.º, 28.º e 29.º (Certificador, Titular, Terceiro em Causa).

Na ausência de comunicações por parte do Titular, o certificado será automaticamente revogado após um período de suspensão de 90 (noventa) dias ou até à data de validade do mesmo.

A data de produção de efeitos da revogação coincidirá, em qualquer caso, com a data de produção de efeitos da suspensão.

K.2.1. Suspensão a pedido do Titular

O Titular pode solicitar a suspensão do certificado acedendo a uma secção específica disponibilizada no âmbito dos serviços do Banco ou da Instituição de Pagamento ou entrando em contacto direto com o Apoio ao Cliente do Banco ou da Instituição de Pagamento.

O Certificador procede à suspensão que será comunicada ao Titular utilizando funções específicas disponibilizadas no âmbito dos serviços do Banco ou da Instituição de Pagamento.

Posteriormente, o Titular poderá solicitar o restabelecimento do certificado de acordo com as modalidades disponibilizadas
pelo Banco ou Instituição de Pagamento.

Na ausência de comunicações adicionais, o certificado suspenso será automaticamente revogado no final do período de suspensão e a data de revogação coincidirá com a data de decorrência da suspensão.

K.2.2. Suspensão a pedido do Terceiro em Causa

O Banco ou a Instituição de Pagamento, na qualidade de Terceiro em Causa, podem solicitar a suspensão do certificado.

O Certificador, verificada a correção do pedido, irá suspender imediatamente o certificado e irá comunicar a suspensão aos Titulares em causa através de correio eletrónico ou por comunicação através dos serviços disponibilizados pelo Banco ou Instituição de Pagamento.

K.2.3. Suspensão por iniciativa do Certificador

O Certificador, exceto em casos de urgência motivada, poderá suspender o certificado notificando previamente o Titular para o endereço de correio eletrónico fornecido em fase de pedido do certificado comunicado em fase de registo ou para a morada de residência, especificando os motivos da suspensão e a data e hora a partir das quais a suspensão terá efeito.

O Certificador enviará também uma comunicação análoga ao Terceiro em Causa.

L. Modalidade de substituição das chaves

L.1. Substituição dos certificados qualificados e das chaves do Titular

Os certificados qualificados de assinatura eletrónica emitidos pelo Certificador no âmbito do contexto descrito no presente
Manual de Operação têm uma validade de 36 (trinta e seis) meses a partir da data de emissão.

Terminado o prazo acima referido, será necessária a criação de um novo par de chaves de assinatura e a emissão de um novo certificado.

Neste caso, o procedimento seguido para a emissão de um novo certificado será igual ao indicado em fase de primeira emissão, exceto a fase de identificação do Titular, que não terá de ser repetida.

L.2. Substituição das chaves do Certificador

L.2.1. Substituição em emergência das chaves de certificação

O procedimento utilizado em caso de avaria do dispositivo de assinatura (HSM) com as chaves de certificação (CA e TSCA) ou de desastre na sede central é tratado na secção *P Procedimento de gestão de eventos catastróficos*.

L.2.2. Substituição programada das chaves de certificação

Com um período de tempo de acordo com a norma em vigor, antes do vencimento do certificado referente aos pares de chaves de certificação (CA e TSCA), utilizados pelos sistemas de emissão de certificados de assinatura e dos certificados de TSA, o Certificador procederá com base no estabelecido pelo Art. 30.º do DPCM.

L.3. Chaves do sistema de selo temporal (TSA)

Em conformidade com o disposto no Art. 49.º, parágrafo 2, do DPCM, para limitar o número de selos temporais gerados com o mesmo par de chaves, estas são substituídas no prazo de 90 (noventa) dias a contar da data da sua emissão. Ao mesmo tempo, é emitido um certificado para o novo par de chaves (sem revogar o anterior, relativo ao par de chaves substituído).

M. Registo dos certificados

M.1. Modalidade de gestão do registo dos certificados

No registo dos certificados, a INTESA publica:

1. Os certificados das chaves de assinatura e do sistema de selo temporal.
2. Os certificados das chaves de certificado (CA e TSCA).
3. Os certificados emitidos após substituição das chaves de certificação.
4. Certificados para as chaves de assinatura da Agência para a Itália Digital (DPCM Art. 42.º, parágrafo 1).
5. As listas de revogação e suspensão (CRL).

As operações que envolvem o registo de certificados são realizadas apenas pelas pessoas autorizadas, presentes em quantidade adequada para impedir ações ilícitas por parte de um número limitado de colaboradores.

O Certificador guarda uma cópia de referência do registo de certificados inacessível pelo exterior; esta atualiza em tempo real a cópia operativa, acessível por parte dos utilizadores com protocolo LDAP.

A verificação da conformidade entre a cópia de referência e a cópia operativa é feita sistematicamente.

M.2. Acesso lógico ao registo dos certificados

A cópia de referência está localizada numa rede dedicada protegida por dispositivos adequados; como tal, não pode ser acedida por outros além do servidor de emissão de certificados, que regista os certificados emitidos e as CRL.

O acesso às cópias operativas é feito através do endereço ***ldap://x500.e-trustcom.intesa.it*** com protocolo LDAP.

O Certificador também permite o acesso às CRL através do protocolo http, no URL indicado no campo CDP (CRL Distribution Point) do certificado.

M.3. Acesso físico às instalações dos sistemas para registo dos certificados

Os colaboradores autorizados a gerir diretamente o registo de certificados podem aceder às instalações onde o sistema está instalado e operar apenas se estiverem na modalidade dual control para evitar ações ilegais.

Os funcionários encarregues de gerir os sistemas, a gestão da rede, manutenção, etc., podem aceder às instalações onde o sistema está instalado e, no caso de colaboradores específicos, operar apenas na presença de colaboradores autorizados a gerir o registo de certificados da forma anteriormente explicada para operadores autorizados.

N. Modalidade de proteção dos dados pessoais

As medidas de segurança para a proteção de dados pessoais estão em conformidade com as medidas previstas no Regulamento Europeu 679/2016 (RGPD) e posteriores modificações e adendas.

O. Procedimento de gestão de cópias de segurança

Os arquivos informáticos que são objeto de cópias de segurança são os seguintes:

- REGISTO DE CERTIFICADOS, arquivo digital que contém o que é especificado no par. M.

- INFORMAÇÕES OPERATIVAS, arquivo digital no qual são armazenadas todas as informações recebidas pelo Titular no momento do registo e do pedido de certificado, bem como os pedidos de revogação e suspensão, acompanhados da documentação relevante.
- REGISTO DE CONTROLO, arquivo constituído pelo conjunto dos registos realizados automaticamente pelos sistemas instalados no serviço de certificação do QTSP (Art. 36.º do DPCM).
- ARQUIVO DIGITAL DE SELOS TEMPORAIS, contém os selos temporais gerados pelo sistema de validação temporal (Art. 53.º, parágrafo 1, do DPCM).
- REGISTO OPERATIVO DE EVENTOS DE SELO TEMPORAL, registo no qual são guardados automaticamente os eventos relativos às atividades de selo temporal para os quais é previsto o registo de qualquer anomalia ou tentativa de adulteração que possa prejudicar o funcionamento do sistema de selos temporais (Art. 52.º do DPCM).

A conservação, para todas as cópias de segurança descritas, está em conformidade com as disposições das normas em vigor na matéria.

P. Procedimento de gestão de eventos catastróficos

O QTSP INTESA dispõe de um plano de emergência para a gestão de eventos catastróficos que inclui as seguintes fases:

- gestão de emergências: nesta fase, é garantida a continuidade de acesso às CRL; a sua emissão pode sofrer atrasos devido à necessidade de ativar o servidor de backup da CA, localizado no site de backup;
- gestão transitória: neste período, é garantida a emissão de certificados e o restabelecimento de outras soluções de disaster recovery;
- regresso ao estado normal: no mesmo site original ou noutro alternativo, mas definitivo.

Deve-se ter em conta que a presença de réplicas da cópia operativa do registo de certificados distribuídas por vários locais ainda permite, em caso de interrupção de funcionamento de uma das sedes, aceder ao conteúdo do registo de certificados atualizado até ao momento da interrupção.

Para a gestão de emergência, está prevista uma réplica no site de backup do registo de certificados dos dados do sistema de emissão de certificados e a intervenção no prazo de 24 horas do pessoal para ativar a funcionalidade de emissão das CRL. O referido pessoal tem formação em situações de emergência, além da gestão do SW e HW.

Em todas as sedes afetadas pela gestão de eventos catastróficos está depositada uma cópia em papel do plano de emergência.

Q. Modalidade para a aposição e definição da referência temporal

Todas as máquinas do sistema de PKI do Certificador são sincronizadas com o *I.N.RI.M. - Istituto Nazionale di Ricerca Metrologica (Instituto Nacional de Investigação Meteorológica)* de Turim (antigo *Istituto Elettrotecnico Nazionale Galileo Ferraris - Instituto Eletrotécnico Nacional Galileo Ferraris*). Esta funcionalidade é realizada por um software específico instalado em todos os servidores que, através do protocolo NTP (Network Time Protocol), se liga ao servidor remoto configurado.

O Network Time Protocol (NTP) é um dos métodos mais precisos e flexíveis para passar a informação de data e hora na rede de internet. Permite manter sincronizados entre si computadores ligados através de redes locais, metropolitanas ou mesmo mundiais (Internet) utilizando uma estrutura de tipo hierárquico em pirâmide.

O I.N.RI.M fornece um serviço de sincronização para sistemas informáticos ligados à rede de internet, baseado em dois servidores NTP primários instalados no Laboratório de Tempo e Frequência de Amostra. Estes são sincronizados, através de um gerador de códigos de data, pelos padrões atómicos de feixe de césio utilizados para gerar a escala de tempo nacional italiana UTC(IT). O desfasamento temporal entre os servidores NTP do I.N.RI.M e a escala de tempo nacional italiana é mantido sob controlo e é normalmente inferior a alguns milissegundos. A precisão de sincronização obtida depende do tipo de rede e da distância entre o servidor NTP e o calculador que se pretende

sincronizar; os valores de desfasamento são normalmente inferiores a um milissegundo para sistemas pertencentes à mesma rede e podem chegar a algumas centenas de milissegundos para redes remotas.

O software instalado no Certificador liga-se ao servidor remoto em intervalos regulares de tempo e, depois de obter a hora atual, procede à correção do relógio da máquina local através de algoritmos sofisticados.

As referências temporais apostas pelas aplicações são cadeias em formato de data (DD/MM/YYYY hh:mm:ss), com precisão ao segundo, que representam a hora local, com base na configuração da máquina. Estas referências estão em conformidade com o DPCM Art. 51.º.

Cada registo efetuado no registo de controlo contém uma referência temporal que, sendo gerada com a modalidade aqui descrita, é oponível a terceiros (Art. 41.º do DPCM).

Q.1. Modalidade de pedido e verificação de selos temporais

O Certificador apõe um selo temporal (*selo temporal qualificado*, nos termos do Reg. eIDAS) em todos os documentos assinados pelo Titular no âmbito dos serviços descritos neste Manual de Operações.

A aposição da referida marca é um processo integrado com a operação de assinatura e não requer qualquer atividade específica por parte do Titular.

R. Lead Time e Matriz RACI para emissão dos certificados

Em seguida é apresentada a matriz relativa ao "Lead Time de Processo" para a gestão dos pedidos de Emissão, Revogação, Suspensão e Reativação dos Certificados.

Sujeito	Pedido	Entidade Envolvida	Ação Entidade Envolvida	Entidade Envolvida	Ação Entidade Envolvida
Utilizador, Requerente, Titular do Certificado	*Pedido de Emissão do Certificado vs. LRA*	*Banco / Instituição (acting as) Local RA*	*Emite ordem de publicação do Certificado vs CA mediante prévia verificação da identidade*	*Certification Authority*	*Despacho do Pedido de Certificação*
Utilizador, Requerente, Titular do Certificado	*Pedido de Revogação do Certificado vs. RA ou LRA*	*Intesa (acting as) Registration Authority (RA) ou Banco / Instituição (acting as LRA)*	*Emite ordem de revogação do Certificado vs CA mediante prévia verificação da identidade*	*Certification Authority*	*Despacho do Pedido de Revogação*
Utilizador, Requerente, Titular do Certificado	*Pedido de Suspensão do Certificado vs. RA ou LRA*	*Intesa (acting as) Registration Authority (RA) ou Banco / Instituição (acting as LRA)*	*Emite ordem de suspensão do Certificado vs CA mediante prévia verificação da identidade*	*Certification Authority*	*Despacho do Pedido de Suspensão*
Utilizador, Requerente, Titular do Certificado	*Pedido de Reativação do Certificado vs. RA ou LRA*	*Intesa (acting as) Registration Authority (RA) ou Banco / Instituição (acting as LRA)*	*Emite ordem de reativação do Certificado vs CA mediante prévia verificação da identidade*	*Certification Authority*	*Despacho do Pedido de Reativação*

Em seguida é apresentada a matriz RACI relativa à identificação de responsabilidades das entidades envolvidas nos pedidos de Emissão, Revogação, Suspensão e Reativação dos Certificados.

Sujeito Envolvido	Responsible	Accountable	Consulted	Informed
Registration Authority	***X***			
Local Registration Authority	***X***			
Certification Authority		***X***		

Utilizador, Requerente, Titular do Certificado			***X***	***X***

S. Referências Técnicas

ETSI-319.401	ETSI EN 319 401 v2.1.1 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI-319.411-1	ETSI EN 319 411-1 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI-319.411-2	ETSI EN 319 411-2 V2.1.0 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
ETSI-319.411-3	ETSI EN 319 411-3 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates
ETSI-319.412-1	ETSI EN 319 412-1 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
ETSI-319.412-2	ETSI EN 319 412-2 V2.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
ETSI-319.412-5	ETSI EN 319 412-5 V2.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
Rec ITU-R	Recommandation ITU-R TF.460-6, Annex 1 – Time Scales.
RFC5905	Network Time Protocol (Protocolo NTP)
ETSI-319.421	ETSI EN 319 421 v1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
ETSI-319.422	ETSI EN 319 422 v1.1.1 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time- stamp token profiles
Rec ITU-R	Recommandation ITU-R TF.460-6, Annex 1 – Time Scales.
RFC5905	Network Time Protocol (Protocollo NTP)

------- FIM DO DOCUMENTO -------