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

Qualified Trust Service Provider

Manual Operativo

para los procedimientos de firma electrónica cualificada

remota

en ámbito bancario y financiero

Código del documento:
MO_REMBAN
OID: 1.3.76.21.1.50.110
Redacción: Antonio Raia
Aprobación: Franco Tafini
Fecha de emisión:
01/07/2019
Versión: 04

Firmado por: ANTONIO RAIA
Organización: IN.TE.S.A. S.p.A.

An IBM Company
intesa
DIGITAL
BUSINESS SOLUTIONS

VERSIONES

Versión nº: 04		***Fecha de la Revisión:***	***01/07/2019***
Descripción de las modificaciones:	Variación de los datos societarios y logotipo Actualización de las definiciones y referencias normativas Actualización del esquema gráfico Introducción del procedimiento de firma para el Cliente Prospect (I.2.3)		
Motivaciones:	Actualizaciones normativas: Reglamento (UE) 910/2014 (eIDAS), D.Lgs.179/2016 (GDPR) Variaciones organizativas del TSP Nuevo procedimiento para captación del cliente		
Versión nº: 03		***Fecha de la Revisión:***	***13/06/2012***
Descripción de las modificaciones:	Extensión del manual al ámbito financiero (Entidades de pago), además del bancario		
Motivaciones:	Actualización		
Versión nº: 02		***Fecha de la Revisión:***	***02/04/2012***
Descripción de las modificaciones:	B.4.2. - Se ha introducido el sistema de reconocimiento de la identidad del Titular (comprobación adecuada) sin la presencia física del mismo C.5. - Se han introducido modalidades del sistema de reconocimiento de la identidad del Titular (comprobación adecuada) F.1.3. - Introducido el límite de uso estándar G. – Introducida la forma de comunicación por correo electrónico de las confirmaciones operativas		
Motivaciones:	Actualización		
Versión nº: 01		***Fecha de la Revisión:***	***01/11/2011***
Descripción de las modificaciones:	Ninguna		
Motivaciones:	Primera emisión		

Índice

Referencias legislativas

Texto Único - DPR 445/00 y siguientes modificaciones e integraciones	Decreto del Presidente de la República nº 445 de 28 de diciembre de 2000 *"Texto único de las disposiciones legislativas y reglamentarias en materia de documentación administrativa*". A continuación indicado solamente como *TU*.
CAD - DLGS 82/05 y siguientes modificaciones e integraciones	Decreto Legislativo nº 82 de 7 de marzo de 2005. *"Código de la Administración Digital"*. A continuación indicado solamente como *CAD*.
DPCM 22/02/2013 *Nuevas Reglas Técnicas* y siguientes modificaciones e integraciones	Decreto del Presidente del Consejo de Ministros de 22 de febrero de 2013 *"Reglas técnicas en materia de generación, introducción y comprobación de las firmas electrónicas avanzadas, cualificadas y digitales, a tenor de los artículos 20 apartado 3, 24 apartado 4, 28 apartado 3, 32 apartado 3 letra b), 35 apartado 2, 36 apartado 2, y 71" (del CAD, ndr).* A continuación indicado solamente como *DPCM.*
Reglamento (UE) N. 910/2014 (eIDAS) y siguientes modificaciones e integraciones	Reglamento (UE) n. 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, en materia de identificación electrónica y servicios fiduciarios para las transacciones electrónicas en el mercado interno y que abroga la Directiva 1999/93/CE. A continuación indicado solamente como *Reg. eIDAS.*
GDPR General Data Protection Regulation y siguientes modificaciones e integraciones	REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en relación con el tratamiento de los datos personales, además de la libre circulación de estos datos y que abroga la Directiva 95/46/CE (reglamento general sobre protección de datos). A continuación indicado solamente como *GDPR.*
DETERMINACIÓN N. 147/2019 y siguientes modificaciones e integraciones	Líneas guía que contienen las "Reglas Técnicas y Recomendaciones relativas a la generación de certificados electrónicos cualificados, firmas y sellos electrónicos habilitados y validaciones temporales electrónicas habilitadas. A continuación indicado solamente como *DETERMINACIÓN.*

Definiciones y acrónimos

AgID	*Agenzia per l'Italia Digitale (Agencia para una Italia Digital, ndt) (antes* CNIPA y DigitPA) - . *www.agid.gov.it* Organismo de Vigilancia a tenor del Reg. UE 910/2014 (eIDAS). De ahora en adelante incluso solo *Agenzia*.
QTSP *Qualified Trust Service Provider.* *Certificador Acreditado*	*Prestador de Servicios Fiduciarios Cualificado.* Persona física o jurídica que presta uno o varios servicios fiduciarios cualificados. Anteriormente *Certificador Acreditado*, a tenor del CAD. En el presente documento es el QTSP In.Te.S.A. S.p.A.
Servicio Fiduciario Cualificado	Servicio electrónico proporcionado por un QTSP y que consiste en los elementos a los que se refiere el art. 3, puntos 16) y 17) del Reg. UE 910/2014 (eIDAS). En el presente documento es el QTSP In.Te.S.A. S.p.A. que presta los servicios cualificados de firma electrónica y de validación temporal electrónica y demás servicios conectados con estas últimas.
Certificado Cualificado de firma electrónica	Certificado electrónico que conecta los datos de convalidación de una firma electrónica con una persona física y confirma como mínimo el nombre o el seudónimo de esa persona. Es expedido por un prestador de servicios fiduciarios cualificado y cumple con los requisitos a los que se refiere el Anexo I del Reg. UE 910/2014 (eIDAS).
Clave Privada	El elemento del par de claves asimétricas, utilizado por el Titular, mediante el que se introduce la firma digital en el documento informático.
Clave Pública	El elemento del par de claves asimétricas destinado a hacerse público, con el que se comprueba la firma digital en el documento informático.
CRL	Lista de los Certificados Revocados, Certificate Revocation List, un listado de indica los certificados revocados o suspendidos, que ya no se consideran válidos por el Certificador que los ha expedido.

OCSP	Online Certificate Status Protocol: servicio de comprobación del estado de validez del Certificado, según el protocolo OCSP.
Documento informático	El documento electrónico que contiene la representación informática de documentos, hechos o datos jurídicamente relevantes.
FEQ - Firma Electrónica Cualificada *FD - Firma Digital*	Firma electrónica creada por un dispositivo para la creación de una firma electrónica cualificada y basada en un certificado cualificado para firmas electrónicas. Coincide, en Italia, con la *Firma Digital* definida en el CAD, art.1, apartado 1, punto s): Firma electrónica cualificada basada en un sistema de claves criptográficas, una pública y una privada, correlacionadas entre ellas, que permite al Titular, mediante la clave privada y al destinatario mediante la clave pública, respectivamente, hacer manifiesta y comprobar la procedencia y la integridad de un documento informático o de un conjunto de documentos informáticos.
Firma Remota	Procedimiento especial de firma electrónica cualificada o de firma digital, generada en HSM custodiado y gestionado, bajo la responsabilidad, por el certificador acreditado, que permite garantizar el control exclusivo de las claves privadas por parte de sus titulares.
HSM - Hardware Security Module	Dispositivos para la creación de la firma electrónica cualificada, si cumplen con los requisitos establecidos en el Anexo II del Reg. (UE) 910/2014. Llamados también *Dispositivos de Firma*.
Qualified Electronic Time Stamp (Marca Temporal)	*Validación Temporal Electrónica Cualificada* Datos en forma electrónica que conectan otros datos de forma electrónica a una hora y fecha concretas, de tal manera que se pruebe que estos últimos datos existían en ese momento. Responde a los requisitos del art. 42 del Reg. eIDAS.
CA - Certification Authority	Autoridad que emite los certificados para la firma electrónica.
RA- Registration Authority	*Autoridad de Registro*: ente que, por encargo del QTSP, tiene la responsabilidad de registrar y comprobar la información (de forma especial la identidad del Titular) necesaria para el QTSP para emitir el Certificado Cualificado.
Registro de los Certificados	La combinación de uno o varios archivos informáticos, que lleva el Certificador, que contiene todos los Certificados emitidos.
Solicitante	La Persona Física que solicita el Certificado.
Titular	La Persona Física a la que el certificado cualificado se expide y que está autorizada para utilizarlo con el fin de introducir su firma digital.
Cliente *Cliente Prospect*	Es el Cliente (o cliente potencial, denominado Prospect) del Banco/de la Entidad financiera.
Referencia Temporal	Información que contiene la fecha y la hora, que se asocia a uno o varios documentos informáticos.
TSA- Time Stamping Authority	Autoridad que emite las validaciones temporales electrónicas.

A. Introducción

El presente documento constituye el *Manual Operativo para los procedimientos de firma electrónica cualificada remota en ámbito bancario y financiero* (de ahora en adelante, *Manual Operativo* o incluso solamente *MO*) del QTSP In.Te.S.A. S.p.A.

El contenido de este Manual Operativo es conforme con lo establecido en las reglas técnicas contenidas en el *Decreto del Presidente del Consejo de Ministros del 22 de febrero de 2013* (de ahora en adelante *DPCM*) y en el *D. lgs. 7 de marzo de 2005, nº 82, que comprende el "Código de la Administración Digital"* tal y como queda modificado e integrado posteriormente (de ahora en adelante "*CAD*") y es conforme con el *Reglamento UE 910/2014* (de ahora en adelante, *Reg. eIDAS*).

En todo lo que no se haya previsto en este Manual Operativo se reenvía a las normas vigentes y futuras que regulan la circunstancia concreta.

Este documento describe las reglas y los procedimientos operativos del *QTSP In.Te.S.A. S.p.A.* (de ahora en adelante, *QTSP INTESA, Certificador* o bien incluso solamente *INTESA*) para la emisión de los certificados cualificados, la generación y comprobación de la firma electrónica cualificada y los procedimientos del servicio de validación temporal de conformidad con la normativa vigente cuando la misma se gestione dentro de proyectos bancarios o

financieros.

En esta tipología de proyectos, las entidades bancarias o financieras, que prestan servicios de home banking y aplicaciones de ventanilla, también harán las veces de Local Registration Authority (de ahora en adelante, LRA) por cuenta de QTSP INTESA. De ahora en adelante, nos referiremos a estas entidades bancarias o financieras con el término de *Banco* o *Entidad de Pago* (o incluso solamente *Banco / Entidad*).

En este contexto, los Titulares de un Certificado Cualificado son solamente las personas identificadas por el mismo Banco/la misma Entidad que, en virtud de un específico acuerdo con el QTSP INTESA, están autorizados a desempeñar la función de Registration Authority.

Por lo tanto, se subraya que todos los procesos de firma de documentos que constituyan el objeto de este Manual Operativo se implementarán exclusivamente dentro de aplicaciones bancarias o financieras.

Las actividades descritas en este Manual Operativo se llevan a cabo de conformidad con el Reg. UE 910/2014 (eIDAS).

A.1. Propriedad intelectual

Este Manual Operativo es de propiedad exclusiva de In.Te.S.A. S.p.A., que es Titular de todos los derechos de propiedad intelectual correspondientes.

Lo que se describe aquí para llevar a cabo las actividades de QTSP está cubierto por derechos sobre la propiedad intelectual.

A.2. Validez

Lo descrito en este documento se aplica al QTSP INTESA (o sea, a sus infraestructuras logísticas y técnicas, además de su personal), a los Titulares de los certificados emitidos por el mismo y a todas las personas que utilizan estos certificados para comprobar la autenticidad y la integridad de los documentos a los que se pone una firma electrónica cualificada, incluso haciendo uso de las marcas temporales cualificadas emitidas por el QTSP INTESA, y al Banco/Entidad de pago en calidad de Local Registration Authority.

El uso de las claves y los correspondientes certificados emitidos está regulado por lo establecido en el art. 5, apartado 4 del DPCM, en el que se establece que las claves de creación y comprobación de la firma y los servicios correspondientes se distinguen según las siguientes tipologías:

a) claves de suscripción, destinadas a la generación y comprobación de las firmas introducidas o asociadas a los documentos;
b) claves de certificación, destinadas a la generación y comprobación de las firmas introducidas en los certificados cualificados, la información sobre el estado de validez del certificado o bien la firma de los certificados relativos a claves de validación temporal electrónica;
c) claves de marcado temporal, destinadas a la generación y comprobación de las marcas temporales.

B. Generalidades

El objetivo del presente documento es la descripción, en términos generales, de los procedimientos y correspondientes reglas que regulan la emisión de certificados cualificados por parte del QTSP INTESA.

Las susodichas reglas y procedimientos surgen de observar las actuales normas de referencia, cuyo cumplimiento permite a INTESA ser introducida en el listado de certificadores acreditados.

Por lo tanto, con el fin de cumplir con la normativa mencionada, resultará necesaria la participación de varios entes que se identificarán con detalle más adelante en el documento.

B.1. Datos de identificación de la versión del Manual Operativo

Este documento constituye la versión nº *04* del *Manual Operativo para los procedimientos de firma electrónica cualificada remota en ámbito bancario y financiero,* emitido de conformidad con el art. 40 del DPCM.

El *object identifier* de este documento es **1.3.76.21.1.50.110**.

Este Manual Operativo está publicado y se puede consultar por vía telemática:

- en la dirección de Internet del QTSP, *https://www.intesa.it/e-trustcom/*
- en la dirección de internet de la Agenzia per l'Italia Digitale, *www.agid.gov.it*

- en el ámbito del sitio institucional del Banco/ de la Entidad.

Nota: la publicación de versiones actualizadas de este Manual Operativo podrá producirse solamente previa autorización de la Agenzia per l'Italia Digitale.

B.2. Datos de identificación del QTSP – Qualified Trust Service Provider

El QTSP (*Prestador de Servicios Fiduciarios Cualificado*) es la sociedad ***In.Te.S.A. S.p.A.***, cuyos datos de identificación se indican a continuación.

Denominación social	**In.Te.S.A. S.p.A.**
Dirección de la sede legal	**Strada Pianezza, 289** **10151 Turín**
Representante Legal	**Administrador Delegado**
Registro Mercantil de Turín	**Nº de inscripción 1692/87**
Nº de código I.V.A.	**05262890014**
Nº de teléfono (centralita)	**+39.011.19216.111**
Sitio web	**www.intesa.it**
Dirección de correo electrónico	**marketing@intesa.it**
Dirección (URL) registro de certificados	**ldap://x500.e-trustcom.intesa.it**
ISO Object Identifier (OID)	**1.3.76.21.1**

El personal responsable de las actividades de certificación, de conformidad con el art. 38 del DPCM, se articula en las siguientes figuras:

a) Responsable de Seguridad.
b) Responsable del servicio de certificación y validación temporal.
c) Responsable de la gestión técnica de los sistemas.
d) Responsable de los servicios técnicos y de logística.
e) Responsable de las comprobaciones e inspecciones (auditing).

Las figuras anteriormente enumeradas pertenecen todas a la organización del QTSP INTESA.

B.3. Responsabilidad del Manual Operativo

La responsabilidad del presente Manual Operativo, a tenor del art. 40 apartado 3 letra c) del DPCM, es de la Certification Authority INTESA, que se dedica a su redacción y publicación.

Con el fin de recoger las observaciones que hubiera y solicitudes de aclaraciones, INTESA ha preparado los instrumentos siguientes:

una dirección de correo electrónico: *marketing@intesa.it*

un contacto telefónico: +39 011.192.16.111

un servicio de HelpDesk para llamadas desde Italia 800.80.50.93
para llamadas desde el extranjero +39 02.871.193.396

B.4. Entidades interesadas en los procesos

Dentro de la estructura del QTSP se identifican entidades que forman parte de los procesos relativos a la emisión de los certificados.

Estos actores operan cumpliendo con las reglas y los procesos actuados por el QTSP llevando a cabo, por la parte de su competencia, las actividades atribuidas a los mismos.

B.4.1. Certification Authority (CA)

INTESA, operando en cumplimiento de lo establecido en el DPCM, CAD y el Reg. eIDAS, lleva a cabo las actividades de Qualified Trust Service Provider. Estas actividades incluyen los servicios fiduciarios cualificados de creación, comprobación y convalidación de firmas electrónicas, sellos electrónicos o validaciones temporales

electrónicas (marcas temporales).

Los datos de identificación del QTSP INTESA se indican en el anterior párrafo *B.2*.

B.4.2. Local Registration Authority (LRA)

Por la especial tipología de servicio ofrecido (firma electrónica cualificada remota en el ámbito de las aplicaciones bancarias y financieras) descrita en este Manual Operativo, el QTSP INTESA remite las funciones de Registration Authority al Banco/a la Entidad que haya adquirido el servicio.

La LRA se compromete a llevar a cabo las actividades siguientes:

- Identificación del Titular;
- Registro del Titular.

El Banco/la Entidad, en el ejercicio de sus funciones de Registration Authority, tendrá que vigilar para que la actividad de reconocimiento se lleve a cabo respetando la normativa vigente y lo establecido en este Manual Operativo.

En concreto, el Banco/la Entidad, respetando la normativa contra el blanqueo de capitales, podrá identificar al Titular (*comprobación adecuada*) incluso aunque no se presente físicamente en una agencia.

En este caso el Banco/la Entidad de todas formas tendrá que:

- comprobar la identidad mediante documentos, datos o información complementaria como documentos públicos, escrituras privadas autenticadas, certificados utilizados para generar una firma electrónica cualificada asociada a documentos informativos o bien a través de declaración de la Autoridad Consular Italiana;
- aplicar medidas complementarias para la comprobación de los documentos proporcionados como, por ejemplo, certificado de confirmación de una entidad de crédito o financiera sometida a la directiva;
- utilizar la documentación que da prueba de que la relación de provisión procede de una cuenta a nombre del cliente.

C. Obligaciones

C.1. Obligaciones del Prestador de Servicios Fiduciarios Cualificado (QTSP)

En el desempeño de su actividad, el Prestador de Servicios Fiduciarios Cualificado (indicado también como *Certificador Acreditado*) opera de conformidad con lo dispuesto en el:

- Decreto Legislativo del 7 de marzo de 2005, nº 82 y siguientes modificaciones
- Decreto del Presidente del Consejo de Ministros de 22 de febrero de 2013
- Reglamento (UE) 2016/679 (GDPR)
- Reglamento (UE) 910/2014 (eIDAS)

En concreto, el QTSP:

- adopta todas las medidas de organización y técnicas adecuadas para evitar daño a los demás;
- se atiene a las reglas técnicas especificadas en el DPCM y siguientes modificaciones e integraciones;
- garantiza que su Sistema de calidad sea conforme con las normas ISO 9001;
- asegura que el dispositivo para la generación de las firmas (HSM) tenga los requisitos de seguridad establecidos en el art. 29 del Reg. eIDAS;
- emite y hace público el certificado cualificado, si el Titular no ha especificado otra cosa, según lo establecido en el Art. 32 del CAD;
- informa a los solicitantes, de forma explícita y clara, sobre el procedimiento de certificación, sobre los requisitos técnicos necesarios para acceder al mismo, sobre las características y limitaciones de uso de las firmas emitidas sobre la base del servicio de certificación;
- se atiene a las medidas de seguridad para el tratamiento de los datos de carácter personal (GDPR);
- no se hace depositario de datos para la creación de la firma del Titular;
- procede a la publicación de la revocación y de la suspensión del certificado electrónico en caso de solicitud por parte del Titular o del Tercero interesado;

- asegura la precisa determinación de la fecha y de la hora de emisión, de revocación y suspensión de los certificados electrónicos;
- mantiene el registro, incluso electrónico, de toda la información relativa al certificado cualificado durante 20 (veinte) años, en concreto con el fin de proporcionar prueba del certificado en posibles procesos judiciales;
- asegura que el código de identificación (de propiedad exclusiva del QTSP) asignado a cada Titular sea unívoco en el ámbito de sus usuarios;
- prepara en medios de comunicación duraderos toda la información útil para las personas que soliciten el servicio de certificación. Entre estos citamos: los términos y condiciones exactos relativos al uso del certificado, incluida cualquier limitación del uso, la existencia de un sistema de acreditación facultativa y los procedimientos de reclamación y resolución de controversias. Dicha información, que puede transmitirse de forma electrónica, tiene que escribirse en un lenguaje claro y proporcionarse antes del acuerdo entre el solicitante del servicio y el QTSP;
- utiliza sistemas fiables para la gestión del registro de certificados con modalidades tales que garanticen que solamente las personas autorizadas puedan efectuar introducciones y modificaciones, que la autenticidad de la información se pueda comprobar, que los certificados puedan ser consultados por el público solamente en los casos permitidos por el Titular del certificado y que el operador se pueda dar cuenta de cualquier evento que ponga en peligro los requisitos de seguridad;
- registra la emisión de los certificados cualificados en el diario de control con la especificación de la fecha y la hora de la generación.

Según lo establecido en el art. 14 del DPCM, el Certificador proporciona o indica al menos un sistema que permita efectuar la comprobación de las firmas digitales.

Además, el QTSP:

- genera un certificado cualificado, para cada una de las claves de firma electrónica avanzada utilizadas por la Agenzia per l'Italia Digitale, para la firma del listado público de los certificadores, y lo publica en su registro de certificados a tenor del art. 42 del DPCM;
- indica un sistema de comprobación de la firma electrónica, al que se refiere el art. 10 del DPCM;
- mantiene copia de la lista, firmada por la Agenzia per l'Italia Digitale, de los certificados relativos a las claves de certificación a las que se refiere el art. 43 del DPCM y la hace accesible por vía telemática como establece el art. 42, apartado 3 del DPCM.

C.2. Obligaciones del Titular

El Titular que solicita un certificado cualificado para los servicios descritos en este Manual Operativo es un cliente del Banco o de la Entidad de Pago, que operan como Registration Authority.

El Titular recibirá un certificado cualificado para la Firma Electrónica Cualificada Remota, con el que poder firmar contratos y documentos relativos a productos y/o servicios ofrecidos por el Banco/la Entidad en las formas descritas en el párrafo.

El Titular está obligado a conservar la información necesaria para la utilización de su clave privada de firma de forma adecuada y adoptar todas las medidas de organización y técnicas idóneas para evitar daños a otras personas (CAD, art. 32, apartado 1).

El Titular de la clave, además, tiene que:

- proporcionar toda la información requerida por el QTSP, garantizando su fiabilidad bajo su responsabilidad;
- enviar la solicitud de certificación según las modalidades indicadas en este Manual Operativo;
- comunicar al QTSP, incluso mediante la LRA, posibles variaciones a la información proporcionada en el momento del registro: datos personales, residencia, contacto telefónico, dirección de correo electrónico, etc.;
- conservar con el mayor cuidado y diligencia posibles la información de habilitación para el uso de la clave privada;
- denunciar inmediatamente a las Autoridades competentes y al Banco/a la Entidad, en caso de pérdida o robo de los códigos y/o de los dispositivos indicados para acceder a las propias claves de firma; el Banco/la Entidad procederán a la inmediata revocación del certificado;

- enviar solicitudes de revocación y de suspensión del certificado cualificado según lo indicado en este Manual Operativo.

C.3. Obligaciones de los usuarios de los certificados

Utilizador (*Relying Party*) es cualquier persona que recibe un documento firmado digitalmente y, con el fin de comprobar su validez, se vale del Certificado Cualificado utilizado por el Titular para firmar el documento mismo.

La comprobación de la firma digital y la posterior extracción de los objetos firmados puede efectuarse con cualquier software que pueda elaborar archivos firmados de conformidad con el Reg. eIDAS.

Quienes hagan uso de un Certificado Cualificado para comprobar la validez de un documento firmado de forma digital, están obligados a:

- comprobar la validez del certificado que contiene la clave pública del Titular que firma el mensaje, según lo indicado en los estándares vigentes en el momento de su emisión;
- comprobar el estado de validez del certificado mediante el protocolo OCSP o mediante el acceso a las Listas de Revocación;
- comprobar la validez del proceso de certificación, basado en el listado público de los QTSP;
- comprobar la existencia de posibles limitaciones al uso del certificado utilizado por el Titular.

C.4. Obligaciones del Tercero interesado

El Tercero interesado, en los servicios descritos en el presente Manual Operativo, es el Banco o la Entidad de pago. Por lo tanto, el Banco/la Entidad, en su función de Tercero interesado:

- comprueba que el Cliente posea todos los requisitos necesarios y autoriza al Cliente para solicitar la emisión del Certificado Cualificado para la Firma Digital Remota
- lleva a cabo una actividad de soporte al Titular
- indica al QTSP posibles limitaciones añadidas de utilización del Certificado Cualificado para la Firma Digital además de las establecidas en el párrafo *F.1.1*.

El Banco/la Entidad, como Tercero interesado, por lo tanto, podrá indicar al QTSP posibles limitaciones de uso del certificado, posibles poderes de representación y tendrá que comunicar cualquier variación de los mismos. Como ejemplo, se indican las siguientes circunstancias:

- variación o cese de los poderes de representación;
- variación de funciones y cualificaciones internas;
- cese de la relación de subordinación.

La solicitud de revocación o suspensión por parte del Tercero interesado que llega a la LRA tendrá que enviarse inmediatamente a la CA cuando desaparezcan los requisitos en función de los que el Titular había recibido un certificado cualificado para la firma electrónica.

C.5. Obligaciones de las Registration Authority externas (LRA)

El QTSP INTESA, por necesidades relacionadas con la prestación del servicio, se vale en todo el territorio nacional de otras personas (de ahora en adelante denominadas RA externas o LRA - Local Registration Authority) para llevar a cabo una parte de las actividades propias de la Oficina de registro.

El QTSP In.Te.S.A. S.p.A. remite el desarrollo de la función de Registration Authority al Banco o a la Entidad de pago mediante específico *Contrato de Mandato*, firmado por ambas partes.

En concreto, las RA externas llevan a cabo las actividades siguientes:

- identificación con certeza del solicitante de la certificación (de ahora en adelante Titular del certificado);
- registro del solicitante/Titular;

- entrega al Titular de los dispositivos y/o códigos que le permitirán acceder a su clave de firma respetando los artículos 8 y 10, apartado 2, del DPCM;
- envío de la documentación firmada a la Oficina RA del QTSP INTESA, sin perjuicio de acuerdos diferentes indicados en el contrato de mandato.

En el Contrato de Mandato se especifican las obligaciones a las que se tiene que atener el Banco/la Entidad a la que el QTSP INTESA asigna el encargo de LRA y sobre los que el QTSP tiene la obligación de vigilar.

En concreto, se le pide a la LRA que:

- vigile para que la actividad de identificación llevada a cabo se realice respetando la normativa vigente (CAD, y siguientes modificaciones e integraciones, DPCM, Reg. eIDAS y normativa contra el blanqueo de capitales);
- utilice y trate los datos personales adquiridos en fase de reconocimiento de acuerdo con el GDPR;
- haga disponible al QTSP INTESA el material recopilado en la fase de identificación y registro.

El servicio de identificación (*comprobación adecuada*) podrá gestionarse de tres maneras diferentes, descritas a continuación:

- *Tradicional*: el Solicitante se identifica en una filial del Banco o del Ente de Pago;
- *Por solicitud*: cuando se abre una nueva cuenta corriente, el Solicitante podrá pedir que le contacte un *Personal Financial Adviser* que, una vez que le da una cita, dará soporte al Cliente en todos los procedimientos relativos a la apertura de una Cuenta Corriente. En esta fase, al Cliente se le guiará (después de que se haya identificado y registrado) también en la solicitud de un certificado de firma electrónica cualificada;
- *On line*: en cambio, si el Solicitante elige el modo de aceptación directa y ya es titular de una cuenta corriente en un Banco en el territorio nacional, para ser reconocido a fines legales podrá:
  - utilizar un procedimiento SEPA (o SDD - SEPA Direct Debit);
  - ordenar una transferencia desde la cuenta corriente ya abierta en el Banco anterior.

A través de los procesos anteriores, la LRA del Banco o de la Entidad de Pago tomará posesión de toda la información establecida en la Ley, con total seguridad y respetando plenamente la política de protección de datos personales.

D. Responsabilidades y limitaciones a las indemnizaciones

D.1. Responsabilidades del QTSP – Limitación a las indemnizaciones

El QTSP INTESA es responsable frente a los Titulares para el cumplimiento de todas las obligaciones derivadas de la realización de las actividades establecidas en el DPCM, por el GDPR, por el CAD y por el Reg. eIDAS (y siguientes modificaciones e integraciones), como se describe en el párrafo *C.1.Obligaciones del Prestador de Servicios Fiduciarios Cualificado (QTSP)*.

INTESA, sin perjuicio de los casos de dolo o culpa (Reg. eIDAS, Art.13), no asume ninguna responsabilidad por las consecuencias derivadas de un uso de los certificados diferente de lo dispuesto en el art. 5 del DPCM, y en concreto por la falta de respeto por parte del Titular y del Tercero interesado de lo indicado en el presente Manual Operativo y/o por la falta de cumplimiento por parte de los mismos de la normativa vigente.

De la misma manera, INTESA no podrá considerarse responsable de las consecuencias debidas a causas que no puedan imputársele, como ejemplo, sin ánimo de exhaustividad: calamidades naturales, deservicios y/o disfunciones técnicas y logísticas fuera de su control, intervenciones de la Autoridad, revueltas o actos de guerra que incidan también o solo en personas de cuya actividad INTESA se valga para la prestación de sus servicios de certificación.

El QTSP INTESA no será responsable por los daños que se deriven de una utilización no conforme del Certificado Cualificado para la Firma Digital Remota en relación con la limitación de uso tal y como se especifica en el párrafo *F.1.1*.

El Titular, después de haber leído este Manual Operativo, tiene que llevar a cabo todas las medidas de diligencia especial adecuadas para evitar daños a terceros relacionados con el uso impropio de lo que le ha proporcionado el certificador acreditado. En especial, se recuerda que hay que conservar con la debida diligencia los dispositivos OTP y los códigos secretos imprescindibles para acceder a las claves de firma.

D.2. Seguro

El QTSP INTESA es beneficiario de contratos de seguro para cubrir los riesgos de la actividad y daños causados a terceros, cuyo contenido está en línea con lo necesario para llevar a cabo la actividad profesional de que se trata.

De este contrato se le ha enviado a AgID la correspondiente declaración de estipulación.

E. Tarifa

El Banco o la Entidad de pago proporciona el servicio a sus clientes: las Tarifas para la emisión, revocación y suspensión del certificado cualificado se indicarán en los contratos estipulados entre el cliente y el Banco/la Entidad.

F. Modalidad de identificación y registro de los usuarios

F.1. Identificación de los usuarios

El QTSP tiene que comprobar con certeza la identidad del solicitante a la primera solicitud de emisión del certificado cualificado.

La susodicha operación se le pide al Banco/ a la Entidad que, en calidad de LRA y en cumplimiento con lo establecido en la normativa vigente contra el blanqueo de capitales, identificará y registrará al Titular.

Para las renovaciones siguientes, si se efectúan cuando el certificado cualificado aún es válido, esta actividad no deberá repetirse: el Titular se encargará de comunicar al QTSP a través del Banco/de la Entidad los cambios que hubiera habido en relación con sus datos de registro.

Entre los datos de registro necesarios para llevar a cabo el servicio que constituye el objeto de este documento, recordamos:

- Nombre y Apellidos;
- Fecha de nacimiento;
- Municipio o Estado extranjero de nacimiento;
- Número de Identificación Fiscal;
- Dirección de residencia;
- Domicilio al que se enviarán las comunicaciones en formato papel;
- Número de teléfono móvil;
- Dirección de correo electrónico;
- Tipo y número de documento de identidad mostrado;
- Autoridad que ha emitido el documento y fecha y lugar de emisión y vencimiento.

Al final de esta fase de registro, al Titular se le podrá entregar en comodato de uso un dispositivo One Time Password con display y que puede generar códigos numéricos monouso (denominados de ahora en adelante *códigos OTP* o más sencillamente *OTP*).

En alternativa a un token OTP fijo, el Banco o la Entidad de Pago podrán indicar a los Titulares cómo activar un sistema de autenticación software para dispositivos móviles (en caso de que el Titular dispusiera de uno ya y eligiera esta modalidad como preferible por comodidad de uso respecto al empleo de un Token físico). Este sistema de software permitirá la generación de una One Time Password en el dispositivo móvil del Titular y podrá ser utilizado, por lo tanto, como instrumento de autenticación a los sistemas de firma remota.

Además del OTP, se le proporcionarán al Titular toda la información necesaria y un *Personal Identification Number (PIN*) que puedan garantizarle un acceso seguro al servicio de firma remota que el Banco/la Entidad le ha puesto a disposición.

El mismo PIN podrá utilizarse como código de emergencia (en caso, por ejemplo, de robo y/o pérdida del Token OTP o del móvil) para suspender con urgencia el certificado cualificado del que es titular (párrafo *H.2.2*).

El Titular podrá modificar o actualizar posteriormente el PIN haciendo uso de los servicios que el Banco o la Entidad de Pago le hayan puesto a su disposición.

En esta fase también se le proporciona al Titular la información necesaria para permitirle cambiar en cualquier momento el número de móvil que hubiera facilitado anteriormente.

Además, directamente en la ventanilla del Banco/de la Entidad, o bien en un momento posterior, conectándose al servicio de internet banking expuesto por el mismo Banco/la misma Entidad, pero en cualquier caso de forma previa a la solicitud de emisión de un certificado cualificado, el Titular tendrá que:

- visionar el Manual Operativo del QTSP INTESA:
- autorizar al Banco o a la Entidad de Pago al tratamiento de sus datos personales con los fines relacionados con la emisión de un certificado cualificado para la firma electrónica.

La documentación anterior, relativa al registro de los Titulares, se conserva durante 20 (veinte) días desde el vencimiento del certificado.

F.1.1. Límites de uso

En el Certificado Cualificado para la firma electrónica, emitido en el ámbito de los servicios descritos en este Manual y ofrecidos por el Banco/la Entidad, se introduce siempre un límite de uso.

La fórmula estándar es la siguiente:

La utilización del certificado se limita a las relaciones con Nombre del Banco/de la Entidad.

This certificate may only be used in dealings with Nombre del Banco de la /Entidad.

Podrán acordarse específicos límites de utilización con el Banco o con la Entidad de Pago.
INTESA no es responsable por los daños derivados del uso de un certificado cualificado que exceda los límites que se le ponen al mismo o que se deriven del hecho de superar ese límite.

F.1.2. Títulos y habilitaciones profesionales

En el caso de que se solicite que se indiquen, en el certificado cualificado, habilitaciones profesionales (ej. la pertenencia a un colegio profesional), el solicitante tiene que presentar documentación adecuada para demostrar la efectiva existencia de estas habilitaciones profesionales o documentación equivalente.

Una copia de esta documentación se guarda durante 20 (veinte) años desde que el certificado vence.

La documentación adecuada para completar la solicitud para añadir títulos o habilitaciones profesionales dentro del certificado cualificado no podrá ser anterior a 10 (diez) días desde la fecha de presentación de la solicitud de emisión del susodicho certificado.

INTESA no se responsabiliza por los daños que se deriven del uso impropio de un certificado cualificado con información relativa a habilitaciones profesionales.

INTESA, en caso de autocertificación, no asume ninguna responsabilidad, sin perjuicio de los casos de dolo o culpa (Reg. eIDAS, art.13), por la introducción en el certificado de información autocertificada por el Titular.

F.1.3. Poderes de representación

En caso de que se solicite la indicación en el certificado cualificado de poderes de representación (ej. la pertenencia a una organización y el cargo desempeñado en la misma, la habilitación para operar en nombre y por cuenta de un Cliente, etc.), el solicitante tiene que presentar la documentación adecuada para demostrar la existencia efectiva de estos poderes de representación.

Para la representación de personas físicas, el solicitante deberá presentar una copia auténtica de la autorización o poder notarial firmado por la persona representada, junto con la prueba de la autorización de esta última para la introducción de la función en el certificado.

En caso de que se solicite la indicación en el certificado de una función relativa a la representación de organizaciones o entidades de derecho privado, el Titular tendrá que presentar documentación adecuada para comprobar la función cuya introducción se requiere en el certificado y una declaración de la organización o de la entidad de pertenencia, mediante la que el ente o la organización autoriza al QTSP a la introducción de la función específica en el certificado. Este último documento no tendrá que tener una antigüedad superior a 20 (veinte) días respecto a la fecha de solicitud de emisión del certificado cualificado.

La introducción en el certificado cualificado de información relativa al ejercicio de funciones públicas o poderes de representación en entidades u organizaciones de derecho público quedará supeditado a específicos acuerdos con las entidades mismas. Sobre la base de estos acuerdos, se podrá especificar la función desempeñada por el Titular dentro de la entidad u organización pública.

La documentación presentada se guardará durante un período de 20 (veinte) años.

INTESA no se responsabiliza por los daños que se deriven del uso impropio de un certificado cualificado con información relativa a poderes de representación.

F.1.4. Uso de seudónimos

El Titular puede solicitar, en casos especiales, que en el certificado se indique un seudónimo en alternativa a los datos reales.

La información relativa a la identidad real del usuario se guardará durante 20 (veinte) años.

F.2. Registro de los usuarios que solicitan el certificado

Con posterioridad a la fase de identificación, se realiza el registro de los datos de los Titulares en los archivos de la Certification Authority.

Esta operación se podrá llevar a cabo mediante una aplicación software a la que puede accederse directamente desde las aplicaciones del Banco o de la Entidad de Pago.

G. Generación de las claves de Certificación, Validación Temporal y firma

G.1. Generación de las claves de certificación

La generación de las claves dentro de los dispositivos de firma tiene lugar ante el Responsable de Certificación, como se establece en el art. 7 del DPCM.

La susodicha operación viene una vez inicializados los dispositivos de firma para el sistema de generación de los certificados con los que se firman los certificados de los Titulares y los del sistema de validación temporal.

Todo ello tiene lugar en modo dual control para evitar operaciones ilícitas.

Las operaciones siguientes a la generación de las parejas de las claves del Certificador son posibles solo mediante especiales dispositivos de autorización (token usb): el acceso privilegiado a los HSM se puede llevar a cabo solamente mediante las claves contenidas en estos dispositivos de autorización a los que hemos hecho referencia anteriormente.

Para más seguridad, estas claves están divididas en varios dispositivos, según una lógica de tipo *«n de m»*, de manera que solo ante la presencia simultánea de, como mínimo, *n* de *m* partes de la clave se permita operar con los privilegios adecuados. Por lo tanto, se custodian en las correspondientes cajas fuertes.

La longitud de las claves de certificación es, como mínimo, de 2048 bit.

G.2. Generación de las claves del sistema de validación temporal

La generación de las claves de validación temporal se produce de conformidad con lo establecido en el art. 49 del DPCM. La longitud de las claves de validación temporal es, como mínimo, de 2048 bit.

G.3. Generación de las claves de firma

Una vez completada la fase de registro, durante la que los datos de los Titulares se memorizan en los archivos del Certificador, se puede proceder a la generación de las claves de firma.

El Titular podrá poner en marcha el proceso de generación de las claves y solicitud del Certificado de firma asociado a las mismas con una de las modalidades descritas en el párrafo *I. Modos operativos para la firma de documentos*.

Las parejas de llaves de firma se crean en dispositivos de firma seguros (HSM - Hardware Security Module), de conformidad con las especificaciones a las que hace referencia el *Anexo II* del Reg. eIDAS.

La longitud de las claves de firma es de 2048 bit como mínimo.

H. Modos de emisión de los certificados

H.1. Procedimiento de emisión de los Certificados de certificación

Una vez generadas las claves de certificación, descrita en el párrafo *G.1*, se generan los certificados de las claves públicas, de conformidad con lo dispuesto por el DPCM, firmados con las respectivas claves privadas y registradas en el registro de certificados según las formas establecidas.

Los certificados de las claves de certificación se envían a la Agenzia per l'Italia Digitale a través del sistema de comunicación al que se refiere el art. 12, apartado 1, del DPCM.

El Certificador genera un certificado cualificado, para cada una de las claves de firma electrónica avanzada utilizadas por la Agenzia para la firma del listado público de los certificadores, y lo publica en su registro de certificados. El Certificador, después, tiene que mantener copia de la lista, firmada por el departamento, de los certificados correspondientes a las claves de certificación, y la pone a disposición por vía telemática (DPCM, art. 42, apartados 1 y 3).

H.2. Procedimiento de emisión de los certificados de firma

INTESA emite certificados con un sistema conforme con el art. 33 del DPCM.

Después de la generación del par de claves de firma, descrita en el párrafo *G.3*, se genera una solicitud de certificado nuevo en formato *PKCS#10*, que proporciona automáticamente la prueba de la posesión de la clave privada y la comprobación del correcto funcionamiento del par de claves.

Una vez generadas las claves, la aplicación del Banco/de la Entidad enviará inmediatamente la solicitud de certificado a la Certification Authority del QTSP.

La generación de los certificados se registra en el diario de control (DPCM, art. 18, apartado 4).

H.2.1. Información contenida en los certificados de firma

Los certificados INTESA, emitidos en el ámbito de este manual, son certificados cualificados a tenor del Reglamento (UE) 910/2014 (eIDAS), y, por lo tanto, se garantiza su interoperatividad y reconocimiento a nivel comunitario.

El Certificado Cualificado define con certeza al Certificador que lo ha emitido y contiene los datos necesarios para comprobar la Firma Digital.

Cada Certificado Cualificado para la firma electrónica es conforme con el Reglamento eIDAS y la DETERMINACIÓN AgID Nº 147/2019 (*Líneas guía que contienen las Reglas Técnicas y Recomendaciones relativas a la generación de los certificados).*

Todos los Certificados Cualificados emitidos en el ámbito de los servicios descritos en este Manual contienen una limitación de uso (párrafo *F.1.1*).

H.2.2. Código de Emergencia

El Certificador garantiza, de conformidad con lo establecido en el art. 21 del DPCM, un *código de emergencia* que deberá utilizarse para solicitar la ***suspensión urgente*** del Certificado.

En las aplicaciones descritas en este Manual Operativo, se considerará como código de emergencia el PIN entregado al Titular en el momento de su registro.

I. Modos operativos para la firma de documentos

El QTSP INTESA, a través de los servicios del Banco o de la Entidad de Pago, pone a disposición de los Titulares todo lo necesario para generar firmas electrónicas cualificadas de conformidad con lo establecido en la normativa vigente.

Su tipología especial no requiere el suministro de una aplicación de firma a instalar en el propio ordenador, sino funcionalidades de firma a las que se puede acceder o entrando en el servicio de home banking del Banco o de la Entidad de Pago o bien directamente en la ventanilla de una filial del Banco o de la Entidad de pago.

Las firmas electrónicas cualificadas obtenidas a través de estos procedimientos serán absolutamente conformes con lo establecido en el DPCM en el art. 4, apartado 2, en relación con los algoritmos utilizados.

Estos documentos, además, tal y como requiere el art. 4, apartado 3, del mismo DPCM, no contendrán macro instrucciones o códigos ejecutables, tales que puedan activar funcionalidades que puedan, sin que lo sepa el firmante, modificar actos, hechos y datos en los mismos documentos representados.

A continuación se describen dos formas de autenticación diferentes que, respetando la normativa vigente, permiten a un Titular, una vez registrado, proceder en primer lugar a la generación de las claves de firma y solicitud de un certificado cualificado y después utilizar las mismas para efectuar firmas electrónicas cualificadas.

Para confirmar la efectuación de las operaciones de firma, se enviarán SMS. En caso de que el Titular disponga de un smartphone habilitado para la lectura de la correspondencia, a petición del Titular mismo, en alternativa, se podrán enviar mediante correo electrónico.

I.1. Autenticación de tipo “Call Drop”

Esta modalidad de autenticación requiere al usuario, que ha sido identificado anteriormente, efectuar, con su teléfono móvil (desde el mismo número proporcionado en fase de identificación), una llamada a un número de teléfono específico, proporcionado en el ámbito del servicio, con el fin de confirmar su voluntad de firmar un documento.

Cuando se recibe esta llamada, se comprueba su procedencia desde el número de teléfono (*Call identifier*) previamente asociado al usuario en fase de registro y, en caso de resultado positivo, se autoriza la operación de firma electrónica cualificada.

Por lo tanto, cuando el Titular desee firmar un documento accediendo al portal del Banco/de la Entidad, utilizará una autenticación de dos factores mediante la introducción de un PIN (información que solamente conoce el usuario) y un número de teléfono (dado por la SIM, que solo el usuario posee).

Este tipo de autenticación también se denomina «*Call Drop*», ya que cuando el Titular llama para ser autenticado no se activa ninguna conversación y la llamada telefónica, después de unos segundos, se cierra.

El usuario Titular nunca recibe una respuesta a su llamada, y, por lo tanto, no incurre en ningún coste telefónico.

Además de tener otras ventajas, esta técnica es extremadamente económica y práctica, ya que no requiere el uso de ningún dispositivo físico de autenticación, y es muy fácil de usar.

A continuación veremos cómo esta autenticación que se acaba de describir es muy apreciada cuando el Titular se encuentra operando en ausencia de empleado (normalmente conectándose a los servicios del Banco o de la Entidad de Pago con su ordenador, a través de los servicios de home banking expuestos por el Banco o la Entidad de Pago mismos), pero, en cambio, sea poco practicable cuando el Titular se encuentre operando frente a un operador externo, por ejemplo, en presencia de un cajero del Banco o de la Entidad de Pago.

Para gestionar estas últimas situaciones, se ha estudiado una solución basada en una gestión dinámica de los números de teléfono a los cuales llamar, para concluir el proceso de autenticación propio en las que denominaremos situaciones en presencia de empleado.

I.1.1. Proceso de Firma en ausencia de empleado (Home banking)

Una vez que entra en posesión de los códigos necesarios durante la fase de identificación, el Titular podrá, posteriormente, solicitar su Certificado digital y proceder después a la firma de un documento según las formas descritas a continuación.

1. El Titular se conecta a la aplicación bancaria o financiera a través de sus códigos personales para el acceso a la aplicación;
2. selecciona y comprueba el documento a firmar;
3. introduce su código PIN;

4. una vez validado el PIN, el Titular, en un tiempo configurado (que no supera el primer minuto) y utilizando el móvil anteriormente registrado, para confirmar su intención de firmar el documento, tiene que llamar inmediatamente a un número telefónico que mientras tanto le saldrá en la pantalla;
5. el sistema, detectando que el número que llama es precisamente el número registrado anteriormente y asociado al Titular, procede a la operación de firma y envía una confirmación del éxito de la operación;
6. en cambio, si hubiera transcurrido el tiempo preestablecido sin que el sistema haya recibido una llamada telefónica al número indicado en el punto 4, la operación se considera nula y concluida sin la firma del documento.

En caso de que los documentos a firmar fueran más de uno, el Titular, por cada documento, tiene que repetir los pasos del 2 al 5.

I.1.2. Proceso de Firma en presencia de empleado (Ventanilla bancaria o financiera)

Una vez obtenido el certificado cualificado, el Titular podrá proceder a firmar un documento.

Como se ha dicho anteriormente, en una ventanilla bancaria o financiera y frente a un operador, al Titular le podría resultar difícil introducir los códigos personales y reservados, como por ejemplo, un PIN.

Por eso se ha pensado también en una solución alternativa, que garantice de todas formas el nivel máximo de seguridad.

1. El usuario se presenta en la ventanilla de una filial del Banco/de la Entidad (en presencia de empleado) y es identificado por el personal encargado (el cajero, por ejemplo) de forma tradicional;
2. una vez visto el documento a firmar, el Titular puede poner en marcha el proceso de firma;
3. en un vídeo, que puede ver el Titular, se pone a disposición un número de teléfono (elegido de forma casual dentro de un numeroso listado de números disponibles) y al mismo tiempo se activa un temporizador;
4. el Titular, en un tiempo configurado que no supere el primer minuto, tiene que llamar al número que le aparece en la pantalla (utilizando su móvil, registrado con anterioridad) para confirmar su intención de firmar el documento;
5. el sistema, entonces, si detecta que la persona que llama es correcta, procede a firmar el documento y a enviar por SMS una confirmación de la operación;
6. en cambio, si ha transcurrido el tiempo preestablecido sin que el sistema haya recibido una llamada de teléfono al número indicado en el punto 3, la operación se anula.

En caso de que los documentos a firmar fueran más de uno, el Titular, por cada documento, tiene que repetir los pasos del 2 al 5.

I.2. Autenticación de tipo OTP Móvil

En alternativa al instrumento de autenticación Call Drop, se ha puesto a disposición una segunda modalidad de autenticación denominada "*OTP Mobile*".

Para activarla, el Titular deberá disponer de un smartphone de entre los especificados por el Banco/la Entidad como adecuados para este servicio.

Una vez realizada esta comprobación, en fase de identificación en la ventanilla del Banco/de la Entidad en la que haya tenido lugar el registro, al Titular se le comunicará una dirección de internet específica en el sitio del Banco o de la Entidad de pago desde la que descargar en el smartphone una aplicación definida de *«OTP Mobile»* y se le entregará un PIN.

También para esta segunda modalidad de autenticación describimos el proceso de firma según si se lleva a cabo en ausencia o en presencia de empleado.

I.2.1. Proceso de Firma en ausencia de empleado (Home banking)

Una vez que entra en posesión del propio certificado cualificado, el Titular podrá firmar un documento en los siguientes pasos:

1. el Titular se conecta a la aplicación bancaria o financiera a través de sus códigos personales para el acceso a la aplicación;
2. selecciona y comprueba el documento a firmar;
3. después introduce su PIN;
4. después lanzará la aplicación anteriormente descargada en su smartphone, recibiendo un OTP móvil que tendrá que introducir después del PIN;
5. una vez que el sistema detecta que el PIN y el OTP recién introducidos son correctos, procede con la operación de firma y envía la confirmación de que la operación se ha llevado a cabo con éxito.

En caso de que los documentos a firmar fueran más de uno, el Titular, por cada documento, tiene que repetir los pasos del 2 al 5.

I.2.2. Proceso de Firma en presencia de empleado (Ventanilla bancaria o financiera)

También en este caso se ha estudiado una solución que no le requiera al Titular introducir ante el personal del Banco o del Ente de Pago códigos reservados que puedan reutilizarse después de forma fraudulenta en su perjuicio.

Una vez que entra en posesión del propio certificado cualificado, el Titular podrá firmar un documento de la manera siguiente:

1. el usuario se presenta en la ventanilla de una filial del Banco/de la Entidad (en presencia de empleado) y es identificado por el personal encargado (el cajero, por ejemplo) de forma tradicional;
2. en el momento de firmar, se activa frente al usuario una pantalla específica con cámara web;
3. el Titular, una vez que en esa pantalla se comprueba el documento a firmar y se decide proceder a la operación de firma, lanza desde su smartphone la generación de un OTP que se visualiza también en formato de código de barras;
4. el Titular, entonces, orientando su smartphone hacia la cámara web, puede permitir la lectura del OTP generada en el paso 3 y poner en marcha el procedimiento de firma propiamente dicho;
5. una vez firmado el documento, el sistema procede a notificarlo inmediatamente a través del envío de un SMS al mismo Titular.

Para firmar varios documentos, se repetirán los pasos del 2 al 5.

I.2.3. Proceso de Firma para los clientes Prospect

El proceso para la emisión del Certificado cualificado de firma remota puede gestionarse incluso por un Cliente Prospect durante las actividades de Onboarding (adquisición del Cliente).

El proceso es compatible con los principales navegadores de internet (Chrome, Firefox, Edge, Safari) y con los dispositivos móviles más recientes de la familia Android y Apple.

Se articula de la manera siguiente:

1. cuando se pone en marcha el proceso, se le solicita al Client Prospect la introducción de sus datos personales con el fin de permitir una posterior identificación clara, previa firma de la información acerca de la privacidad del QTSP INTESA;
2. el Banco Entidad procede a enviar un SMS cuyo texto contiene un OTP (One Time Password) con validez temporal: se le solicita al cliente Prospect que dé input a ese código para comprobar la disponibilidad real del dispositivo móvil indicado en la fase de introducción de datos;
3. una vez completada la comprobación del punto anterior, el Cliente Prospect procede a transmitir los documentos de identidad al Banco Entidad: los datos de registro serán introducidos por el Prospect o serán recibidos a partir de los documentos mediante un sistema de OCR;
4. una vez completada la fase de registro, el Banco enviará al cliente Prospect la documentación contractual que el Cliente Prospect podrá firmar con un certificado cualificado de firma digital remota (FDR) emitido por el QTSP INTESA;

5. al Cliente Prospect, de la misma manera que sucede con el proceso descrito para el internet banking, se le presentará la documentación de solicitud del certificado del QTSP INTESA;
6. la visualización de la misma deberá firmarse obligatoriamente marcando los check boxes del documento e incluyendo una firma electrónica mediante la introducción de un OTP recibido mediante sms de QTSP INTESA;
7. si el OTP proporcionado por el QTSP INTESA se comprueba con resultado positivo, se podrá proceder a emitir un certificado cualificado; de lo contrario, tendrá que solicitarse un OTP nuevo;
8. en el momento de la generación del certificado, es imprescindible, de todas formas, que se introduzca un PIN, que después se pedirá con cada utilización del certificado de firma;
9. el certificado recién emitido podrá, de todas maneras, ser utilizado solamente para firmar la propuesta contractual y ningún otro documento, mientras que el Banco complete las comprobaciones necesarias propedéuticas a la apertura de una cuenta corriente;
10. si las comprobaciones del Banco resultan positivas y la cuenta corriente se activa, el Cliente Prospect podrá utilizar el certificado emitido, respetando sus límites de uso, en las relaciones con el Banco;
    en cambio, si el Banco decidiera no admitir la solicitud de apertura de una cuenta corriente, el mismo certificado se revocaría, inhibiendo su utilización posterior;
11. en ambos casos del punto anterior, el Cliente Prospect de todas maneras será informado acerca del resultado de las comprobaciones y la revocación del certificado, si fuera el caso.

I.3. Autenticación con Token OTP

Por último, puede utilizarse una autenticación relacionada con la utilización de Token OTP físicos (muy extendidos en el mundo bancario y financiero).

La utilización de este Token OTP físico hoy está previsto solo para accesos en ausencia de empleado (típicamente un puesto remoto de home banking).

El Titular se conecta a la aplicación bancaria o financiera a través de sus códigos personales para el acceso a la aplicación y para poner en marcha el procedimiento de firma introducirá el PIN y el código OTP, que mientras tanto habrá generado y visualizado en la pantalla del Token.

J. Modos operativos para la comprobación de la firma

Los documentos firmados de las maneras descritas anteriormente serán exclusivamente en formato PDF: este formato de firma, en efecto, es fácil de utilizar en el ámbito de las aplicaciones bancarias o financieras.

La comprobación de los documentos firmados podrá llevarse a cabo de forma sencilla utilizando el software *Acrobat Reader DC*, aplicación que puede comprobar todas las tipologías de firma electrónica cualificada en formato PDF presentadas en la Unión Europea de conformidad con el Reglamento eIDAS.

Acrobat Reader DC se puede descargar gratuitamente del sitio de Adobe, *https://www.adobe.com/it/*

K. Modos de revocación y suspensión de los certificados

De conformidad con el Reg. eIDAS, la información sobre el estado del certificado está disponible mediante protocolo OCSP, en la URL indicada en el mismo certificado.

La revocación y la suspensión de los certificados pueden certificarse incluso a través de su introducción en la lista CRL (art. 22 del DPCM). El perfil de las CRL es conforme con el estándar RFC 3280. Esta lista, firmada por la Certification Authority que emite el certificado, se actualiza con periodicidad preestablecida y conforme con la normativa vigente.

La lista CRL está disponible también en el registro de certificados.

En los casos en los que la revocación o la suspensión tengan lugar a iniciativa del Certificador o del Tercero interesado (arts. 23, 25, 27 y 29 del DPCM), el Certificador le notifica al Titular la solicitud y el momento en el que entrará en vigor el evento solicitado.

En fase de solicitud, se especificarán la fecha y la hora a partir de la que el certificado resultará revocado (art. 24, apartado 1, del DPCM).

K.1. Revocación de los certificados

Un certificado puede revocarse a petición del Titular, del Tercero interesado o de la Certification Authority (o sea, el QTSP).

El certificado revocado no puede reactivarse de ninguna manera.

K.1.1. Revocación a petición del Titular

El Titular puede solicitar la revocación accediendo a una específica sección que se pone a disposición en el ámbito de los servicios del Banco o de la Entidad de Pago o bien poniéndose en contacto directo con el Servicio al Cliente del Banco o de la Entidad de Pago.

El QTSP, advertido por el Banco/la Entidad, que mientras tanto también habrá bloqueado los códigos de acceso del Titular, procederá a la inmediata revocación del certificado.

K.1.2. Revocación a petición del Tercero interesado

El Banco o la Entidad de pago, en calidad de Tercero interesado, pueden solicitar la revocación del certificado.

El QTSP, una vez comprobado que la solicitud sea correcta, se lo notificará a los Titulares interesados, utilizando los canales de comunicación definidos con el Titular en el momento del registro o con posterioridad actualizados y comunicados por el Titular al QTSP, incluso mediante las LRA (párrafo *C.2. Obligaciones del Titular*).

K.1.3. Revocación a iniciativa del Certificador

El Certificador que desee revocar el Certificado Cualificado, salvo casos de urgencia motivada, avisa con comunicación previa mediante correo electrónico o correo electrónico certificado al Banco/a la Entidad (Tercero interesado) y al mismo tiempo se le comunicará al Titular utilizando la dirección de correo electrónico proporcionada en la fase de solicitud del certificado o bien a la dirección de residencia, especificando los motivos de la revocación, además de la fecha y la hora a partir de la que la revocación es eficaz.

K.1.4. Revocación de los certificados relativos a claves de certificación

En los casos de:

- daño de la clave de certificación,
- cese de la actividad,

el Certificador procede a revocar los certificados de certificación correspondientes y los certificados de firma firmados con la misma clave de certificación.

En un plazo de 24 horas, el Certificador notificará la revocación a la Agenzia per l'Italia Digitale y a los Titulares.

K.2. Suspensión de los certificados

En cuanto a las formas de suspensión y de notificación de la misma, vale lo indicado para las formas de revocación en el párrafo *K.1*.

La suspensión de un certificado se prevé en caso de que se tenga que hacer un suplemento de estudio para comprobar si efectivamente tiene que revocarse (por ejemplo, en los casos en los que se tema la pérdida/el robo del Token OTP o se tengan que hacer comprobaciones para tener la certeza del cese efectivo del Titular en la función para la que se le había emitido el certificado, etc.).

La solicitud de suspensión puede presentarse por todas las entidades establecidas en el DPCM en los arts. 27, 28 y 29 (Certificador, Titular, Tercero interesado).

A falta de comunicaciones por parte del Titular, el certificado se revocará automáticamente tras un período de suspensión de 90 (noventa) días o de todas formas no más tarde de la fecha de vencimiento del mismo certificado. La fecha a partir de la que la revocación entra en vigor, en cualquier caso, coincidirá con la fecha en la que entra en vigor la suspensión.

K.2.1. Suspensión a petición del Titular

El Titular puede solicitar la suspensión del certificado accediendo a una específica sección que se pone a disposición en el ámbito de los servicios del Banco o de la Entidad de Pago o bien poniéndose en contacto directo con el Servicio al Cliente del Banco o de la Entidad de Pago.

El Certificador procede a la suspensión, que se comunicará al Titular, utilizando funciones específicas que se ponen
a disposición dentro de los servicios del Banco o de la Entidad de Pago.

Posteriormente, el Titular podrá solicitar que se restablezca el certificado según las formas que se hayan puesto a disposición, también por parte del Banco o de la Entidad de Pago.

A falta de más comunicaciones, el certificado suspendido será revocado automáticamente al final del período de suspensión y la fecha de revocación coincidirá con la fecha a partir de la que entra en vigor la suspensión.

K.2.2. Suspensión a petición del Tercero interesado

El Banco o la Entidad de pago, en calidad de Tercero interesado, podrán solicitar la suspensión del certificado.

El Certificador, una vez comprobado que la solicitud sea correcta, suspenderá inmediatamente el certificado e informará de ello a los Titulares interesados a través de correo electrónico o con comunicación a través de los servicios expuestos por el Banco o por la Entidad de Pago.

K.2.3. Suspensión a iniciativa del Certificador

El Certificador, salvo los casos de urgencia motivada, podrá suspender el certificado, dando comunicación previa al Titular a la dirección de correo electrónico facilitada en la fase de solicitud del certificado comunicado en fase de registro, o bien a la dirección de residencia, especificando los motivos de la suspensión y la fecha y la hora a partir de las cuales la suspensión adquirirá eficacia.

El Certificador enviará una comunicación similar también al Tercero interesado.

L. Modos de cambio de las claves

L.1. Sustitución de los certificados cualificados y de las claves del Titular

Los certificados cualificados de firma electrónica emitidos por el Certificador en el ámbito del contexto descrito en este Manual Operativo tienen una validez de 36 (treinta y seis) meses desde la fecha de emisión.

Una vez terminado este plazo, será necesario generar un nuevo par de claves de firma y al mismo tiempo la emisión de un nuevo certificado.

En este caso, el procedimiento seguido para emitir el nuevo certificado será similar al indicado en fase de primera emisión, restando la fase de identificación del Titular, que no tendrá que repetirse.

L.2. Sustitución de las claves del Certificador

L.2.1. Sustitución de emergencia de las claves de certificación

El proceso utilizado en caso de avería del dispositivo de firma (HSM) que contiene las claves de certificación (CA y TSCA) o de desastre en la sede central, se trata en la sección *P Procedimiento de gestión de eventos catastróficos.*

L.2.2. Sustitución planificada de las claves de certificación

Con un período de tiempo coherente con la normativa en vigor, antes de que caduque el certificado relativo a los pares de Claves de certificación (CA y TSCA), utilizados por el sistema de emisión de los certificados de firma y de los certificados de TSA, el Certificador procederá en función de lo establecido en el art. 30 del DPCM.

L.3. Claves del sistema de validación temporal (TSA)

De conformidad con lo indicado en el art. 49, apartado 2, del DPCM, con el fin de limitar el número de marcas temporales generadas con el mismo par de claves de validación temporal, las mismas se sustituyen en un plazo de 90 (noventa) días a partir de la fecha de su emisión. Al mismo tiempo, un certificado se emite en relación con el nuevo par de claves (sin revocar el anterior, relativo al par de claves sustituido).

M. Registro de los certificados

M.1. Modo de gestión del Registro de certificados

En el registro de los certificados, INTESA publica:

1. los certificados de las claves de firma y del sistema de validación temporal
2. los certificados de las claves de certificación (CA y TSCA
3. los certificados emitidos después del cambio de las claves de certificación
4. Los certificados para las claves de firma de la Agenzia per l'Italia Digitale (DPCM art. 24, apartado 1)
5. las listas de revocación y suspensión (CRL).

Las operaciones que afectan al registro de los certificados son llevadas a cabo solamente por las personas autorizadas para ello, presentes en cantidad adecuada para impedir acciones ilícitas por parte de un limitado número de empleados.

El Certificador mantiene una copia de referencia del registro de los certificados a la que no puede accederse desde fuera; esta actualiza en tiempo real la copia operativa, a la que todos los usuarios con protocolo LDAP pueden acceder.

La comprobación de correspondencia entre copia de referencia y copia operativa se hace sistemáticamente.

M.2. Acceso lógico al Registro de certificados

La copia de referencia se coloca dentro de una red específica protegida por dispositivos adecuados, por lo que no es accesible a otros que no sea el servidor de emisión de los certificados, que registra los certificados emitidos y las CRL.

El acceso a las copias operativas es posible en la dirección ***ldap://x500.e-trustcom.intesa.it*** con protocolo LDAP.

El Certificador también permite el acceso a las CRL mediante el protocolo http, en la URL indicada en el campo CDP (CRL Distribution Point) del certificado.

M.3. Acceso físico a los locales de los sistemas dedicados al registro de los certificados

Los encargados de la gestión directa del registro de certificados pueden acceder al local en el que el sistema está instalado y operar en él solamente si lo hacen en modalidad dual control, para evitar acciones ilícitas.

Los encargados de la gestión de sistemas, la gestión de red, el mantenimiento, etc., pueden acceder al local en el que el sistema va instalado, y, para los empleados específicos, operar en él solo en presencia de encargados habilitados para la gestión del registro de los certificados según las formas anteriormente explicitadas para los operadores habilitados.

N. Modos de protección de los datos personales

Las medidas de seguridad para la protección de los datos personales son conformes con las medidas establecidas por el Reglamento Europeo 679/2016 (GDPR) y siguientes modificaciones e integraciones.

O. Procedimiento de gestión de las copias de seguridad

Los archivos informáticos que constituyen objeto de copias de seguridad son los siguientes:

- REGISTRO DE CERTIFICADOS, archivo digital que contiene lo especificado en el párrafo M.

- INFORMACIÓN OPERATIVA, archivo digital en el que se memoriza toda la información recibida por el Titular en el momento del registro y de la solicitud de un certificado además de las solicitudes de revocación y suspensión, acompañadas de la correspondiente documentación.
- DIARIO DE CONTORL, archivo constituido por el conjunto de registros efectuados automáticamente por los sistemas instalados en el servicio de certificación del QTSP (art. 46 del DPCM).
- ARCHIVO DIGITAL DE LAS MARCAS TEMPORALES, que contiene las marcas temporales generadas por el sistema de validación temporal (art. 53, apartado 1, del DPCM).
- REGISTRO OPERATIVO DE LOS EVENTOS DE VALIDACIÓN TEMPORAL, registro en el que se memorizan automáticamente los eventos relativos a las actividades de validación temporal para las que se establece el registro de cualquier anomalía o intento de violación que pueda perjudicar el funcionamiento del sistema de validación temporal (art. 52 del DPCM).

La conservación, para todas las copias de seguridad descritas, es conforme con lo establecido en la normativa vigente en la materia.

P. Procedimiento de gestión de los eventos catastróficos

El QTSP INTESA cuenta con un plan de emergencia para la gestión de los eventos catastróficos que prevé las fases siguientes:

- gestión de la emergencia: en esta fase se garantiza la continuidad de acceso a las CRL: su emisión puede sufrir retrasos derivados de la necesidad de activar el servidor de backup de la CA, situado en el sitio de back up;
- gestión del transitorio: en este período se asegura la emisión de los certificados y el restablecimiento de posibles soluciones de disaster recovery;
- vuelta del ejercicio en régimen: en el mismo sitio original o en otro alternativo, pero definitivo.

Debe tenerse en cuenta que la existencia de repeticiones de la copia operativa del registro de certificados distribuidas en varios puntos de todas formas permite, en caso de interrupción de funcionamiento de una de las sedes, acceder al contenido del registro de certificados actualizado hasta el momento de la interrupción.

Para poder afrontar la gestión de la emergencia, existe la replicación en el sitio de backup del registro de los certificados, de los datos del sistema de emisión de los certificados y la intervención en un plazo de 24 horas de personal adecuado para activar la función de emisión de las CRL. De este personal se lleva a cabo su adiestramiento, además de la gestión del SW y HW, incluso de la situación de emergencia.

En todas las sedes afectadas por la gestión de eventos catastróficos se deposita copia en formato papel del plan de emergencia.

Q. Modos para la introducción y la definición de la referencia temporal

Todas las máquinas del sistema de PKI del Certificador están sincronizadas con el *I.N.RI.M. - Instituto Nacional de Investigación Metrológica de* Turín (anteriormente *Instituto Electrotécnico Nacional Galileo Ferraris*). Esta función es llevada a cabo por un software específico instalado en cada servidor que, mediante el protocolo NTP (Network Time Protocol), se conecta con el servidor remoto configurado.

El Network Time Protocol (NTP) es uno de los métodos más precisos y flexibles para pasar la información de tiempo y fecha en la red Internet. El mismo permite mantener sincronizados entre ellos ordenadores conectados mediante redes locales, metropolitanas o incluso mundiales (internet) utilizando una estructura de tipo jerárquico en pirámide.

El I.N.RI.M presta un servicio de sincronización para sistemas informáticos conectados con la red de internet, basado en dos servidores NTP primarios instalados en el Laboratorio de Tiempo y Frecuencia Muestra. Están sincronizados, a través de un generador de códigos de fecha, por las muestras atómicas de faz de cesio utilizadas para generar la escala de tiempo nacional italiana UTC(IT). El desvío de tiempo entre los servidores NTP del I.N.RI.M y la escala de tiempo nacional italiana se tiene bajo control y normalmente es de menos de unos milisegundos. La precisión de sincronización que puede obtenerse depende del tipo de red y de la distancia que exista entre el servidor NTP y el calculador que se desee

sincronizar; los valores de desvío típicos son de menos de un milisegundo para sistemas pertenecientes a la misma red y pueden llegar a unos centenares de milisegundos para redes remotas.

El software instalado en el Certificador se conecta al servidor remoto a intervalos regulares de tiempo y, después de haber obtenido la hora corriente, procede a corregir el reloj de la máquina local mediante sofisticados algoritmos.

Las referencias temporales aportadas por las aplicaciones son cadenas en formato fecha (DD/MM/AAAA hh:mm:ss), con la precisión del segundo, que representan la hora local, en función de la configuración de la máquina. Estas referencias son conformes con el art. 51 del DPCM.

Cada registro efectuado en el diario de control contiene una referencia temporal que, estando generada de las maneras aquí descritas, puede oponerse a terceros (art. 41 del DPCM).

Q.1. Modo de solicitud y comprobación de las marcas temporales

El Certificador pone una marca temporal (*validación temporal electrónica cualificada,* a tenor del Reg. eIDAS) en todos los documentos firmados por el Titular en el ámbito de los servicios descritos en este Manual Operativo.

La introducción de dicha marca es un proceso integrado con la operación de firma y no requiere ninguna actividad específica por parte del Titular.

R. Lead Time y Tabla Raci para la emisión de los certificados

A continuación se indica la Tabla relativa al "Lead Time di Processo" para la gestión de las solicitudes de Emisión, Revocación, Suspensión y Reactivación de los Certificados.

Persona	Solicitud	Ente interesado	Acción Ente interesado	Ente interesado	Acción Ente interesado
Usuario, Solicitante, Titular Certificado	*Solicitud de Emisión del Certifcado vs. LRA*	*Banco / Entidad (acting as) Local RA*	*Emite orden de publicación del Certificado vs CA previa comprobación de la identidad*	*Certification Authority*	*Gestión de la Solicitud de Certificación*
Usuario, Solicitante, Titular Certificado	*Solicitud de Revocación del Certificado vs. RA o LRA*	*Intesa (acting as) Registration Authority (RA) o Banco / Entidad (acting as LRA)*	*Emite orden de revocación del Certificado vs. CA previa comprobación de identidad*	*Certification Authority*	*Gestión de la Solicitud de Revocación*
Usuario, Solicitante, Titular Certificado	*Solicitud de Suspensión del Certificado vs. RA o LRA*	*Intesa (acting as) Registration Authority (RA) o Banco / Entidad (acting as LRA)*	*Emite orden de suspensión del Certificado vs CA previa comprobación de la identidad*	*Certification Authority*	*Gestión de la Solicitud de Suspensión*
Usuario, Solicitante, Titular Certificado	*Solicitud de Suspensión del Certificado vs. RA o LRA*	*Intesa (acting as) Registration Authority (RA) o Banco / Entidad (acting as LRA)*	*Emite orden de reactivación del Certificado vs CA previa comprobación de la identidad*	*Certification Authority*	*Gestión de la Solicitud de Reactivación*

A continuación se indica la Tabla RACI relativa a la identificación de las responsabilidades de los entes interesados en las solicitudes de Emisión, Revocación, Suspensión y Reactivación de los Certificados.

Persona interesada	Responsable	Accountable	Consultado	Informado
Registration Authority	***X***			
Local Registration Authority	***X***			
Certification Authority		***X***		
Usuario, Solicitante, Titular del Certificado			***X***	***X***

S. Referencias 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 (Protocollo NTP)
ETSI-319.421 for	ETSI EN 319 421 v1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements 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)

------- FIN DEL DOCUMENTO -------