In.Te.S.A. S.p.A.
Qualified Trust Service Provider
ai sensi del Regolamento (UE) N. 910/2014 (eIDAS)

Manuale Operativo
per le procedure di firma elettronica qualificata remota nell'ambito dei servizi di FCA Bank

Codice documento: MO_FCAB

OID: 1.3.76.21.1.50.8

Redazione: Antonio Raia

Approvazione: Simone Baldini
(Resp. servizio di certificazione e validazione temporale)

Data emissione: 7/10/2022

Versione: 01

Revisioni

Versione n°: 01		***Data Revisione: 7/10/2022***
Descrizione modifiche:	nessuna	
Motivazioni:	primo rilascio	

Sommario

Riferimenti di legge

Testo Unico - DPR 445/00 e ss.mm.ii.	Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445. *"Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*". Nel seguito indicato anche solo come *TU*.
CAD - DLGS 82/05 e ss.mm.ii.	Decreto Legislativo 7 marzo 2005, n. 82 - "*Codice dell'amministrazione Digitale"*. Nel seguito indicato anche solo come *CAD*.
DPCM 22/02/2013 Nuove Regole Tecniche e ss.mm.ii.	Decreto Del Presidente Del Consiglio Dei Ministri 22 febbraio 2013. *"Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20 comma 3, 24 comma 4, 28 comma 3, 32 comma 3 lettera b), 35 comma 2, 36 comma 2, e 71" (del CAD, n.d.r.).* Nel seguito indicato anche solo come *DPCM.*
Regolamento (UE) N. 910/2014 (eIDAS) e ss.mm.ii.	Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2104, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. Nel seguito indicato anche solo come *Reg. eIDAS.*
Regolamento (UE) N. 2016/679 GDPR - General Data Protection Regulation e ss.mm.ii.	REGOLAMENTO (UE) 2016/679 del Parlamento Europeo e Del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) Nel seguito indicato anche solo come *GDPR.*
DETERMINAZIONE N. 147/2019 e ss.mm.ii.	Linee guida contenenti le "Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate". Nel seguito indicato anche solo come *DETERMINAZIONE*.
Comunicazione AgID 0016101 del 07-06-2016	"agid.AOO-AgID.REGISTRO UFFICIALE(U).0016101.07-06-2016", avente per oggetto "Richiesta di chiarimenti in merito all'utilizzo della firma digitale in particolari ambiti chiusi di utenti". Nel seguito indicato anche solo come *Com. AgID 7/6/2016.*
D.lgs. 231/07 e ss.mm.ii.	DECRETO LEGISLATIVO 21 novembre 2007, n. 231 Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione.

Definizioni e acronimi

AgID	*Agenzia per l'Italia Digitale* (già CNIPA e DigitPA) - *www.agid.gov.it*. Organismo di Sorveglianza ai sensi del Reg. UE 910/2014 (eIDAS). Nel seguito anche solo *Agenzia*.
QTSP *Qualified Trust Service Provider.* *Certificatore Accreditato*	*Prestatore di Servizi Fiduciari Qualificato*. Persona fisica o giuridica che presta uno o più servizi fiduciari qualificati. Già *Certificatore Accreditato*, ai sensi del CAD. Nel presente documento è il QTSP In.Te.S.A. S.p.A.
Servizio Fiduciario Qualificato	Servizio elettronico fornito da un QTSP e consistente negli elementi di cui all'Art.3, punto 16) e 17) del Reg. UE 910/2014 (eIDAS). Nel Presente documento è il QTSP In.Te.S.A. S.p.A. che presta i servizi qualificati di firma elettronica e di validazione temporale elettronica e altri servizi connessi con queste ultime.
Certificato Qualificato di firma elettronica	Attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona. È rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I del Reg. UE 910/2014 (eIDAS)
Chiave Privata	L'elemento della coppia di chiavi asimmetriche, utilizzato dal Titolare, mediante il quale si appone la firma digitale sul documento informatico.
Chiave Pubblica	L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale sul documento informatico.

CRL	Lista dei Certificati Revocati, Certificate Revocation List, un elenco che riporta i certificati revocati o sospesi, non più considerati validi dal Certificatore che li ha emessi.
OCSP	Online Certificate Status Protocol: servizio di verifica dello stato di validità del Certificato, secondo il protocollo OCSP.
Documento informatico	Il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
FEQ - Firma Elettronica Qualificata *FD - Firma Digitale*	Firma elettronica creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche. Coincide, in Italia, con la *Firma Digitale* definita nel CAD, Art.1, comma1, punto s): Firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al Titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità' di un documento informatico o di un insieme di documenti informatici.
Firma Remota	Particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM custodito e gestito, sotto la responsabilità, dal QTSP (certificatore accreditato), che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse.
HSM - Hardware Security Module	Dispositivi per la creazione della firma elettronica qualificata, se conformi ai requisiti di cui all'Allegato II del Reg. (UE) 910/2014. Anche detti *Dispositivi di Firma*.
Qualified Electronic Time Stamp *(Marca Temporale)*	*Validazione Temporale Elettronica Qualificata* Dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi dati esistevano in quel momento. Risponde ai requisiti dell'Art.42 del Reg. eIDAS
CA - Certification Authority	Autorità che emette i certificati per la firma elettronica.
LRA – Local Registration Authority	*Autorità di Registrazione Locale*: Entità che, su mandato del QTSP, ha la responsabilità di identificare, registrare e verificare le informazioni (in particolare modo l'identità del Titolare) necessarie al QTSP per emettere il Certificato Qualificato. Nell'ambito del presente Manuale Operativo sono da intendersi come LRA tutte le società e organizzazioni afferenti al Gruppo Bancario FCA Bank (https://www.fcabankgroup.com/it/il-gruppo/struttura-societaria)
Registro dei Certificati	La combinazione di uno o più archivi informatici, tenuto dal Certificatore, contenente tutti i Certificati emessi.
Richiedente *Richiesta di certificazione*	La Persona Fisica che richiede il Certificato, cioè che inoltra al QTSP una richiesta di certificazione.
Titolare	La Persona Fisica cui il certificato qualificato di firma è rilasciato e che è autorizzato ad usarlo al fine di apporre la propria firma digitale.
Cliente *Cliente Prospect*	È il Cliente (o potenziale cliente, detto Prospect) di FCA Bank.
Riferimento Temporale	Informazione contenente la data e l'ora, che viene associata ad uno o più documenti informatici.
TSA - Time Stamping Authority	Autorità che rilascia le validazioni temporali elettroniche.
Giornale di Controllo	Insieme delle registrazioni effettuate anche automaticamente dai dispositivi installati presso il QTSP, tenuto in modo da garantire l'autenticità delle annotazioni e consentire la ricostruzione, con la necessaria accuratezza, di tutti gli eventi rilevanti ai fini della sicurezza (DPCM 22/02/2013, Art. 36
CPS - CP	*CPS - Certification Practice Statement e CP - Certificate Policy per i Certificati Qualificati di Firma Elettronica e di Sigillo Elettronico* del QTSP INTESA: documento costituisce il Practice Statement del QTSP e descrive le regole e le procedure operative per l'emissione dei certificati qualificati di firma elettronica e di sigillo elettronico, come definiti nel Regolamento (UE) 910/2014 (eIDAS). E' pubblicato sul sito dell'Agenzia e dal QTSP all'URL: *https://www.intesa.it/e-trustcom/*
URL	*Uniform Resource Locator* E' una sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa su una rete di computer, come ad esempio un documento, un pagina web o un portale presente su un host server e resa accessibile ad un client.

A. Introduzione

Il presente documento è il *Manuale Operativo per la procedura di firma digitale remota del Prestatore di Servizi Fiduciari Qualificati In.Te.S.A. S.p.A. nell'ambito dei servizi forniti da FCA Bank S.p.A*. Capogruppo del Gruppo Bancario FCA Bank - Sede Legale: Corso Orbassano n. 367 - 10137 Torino www.fcabankgroup.com Capitale Sociale al 24.11.2021: euro 700.000.000 i.v. - ABI 3445 – Codice Fiscale 08349560014, Iscritta all'Albo dei Gruppi Bancari, Iscritta al Registro Unico degli Intermediari Assicurativi (RUI) n. D000164561.

Il Manuale Operativo descrive le procedure e le relative regole attuate dal Prestatore di Servizi Fiduciari Qualificati In.Te.S.A. S.p.A. (di seguito anche solo *QTSP INTESA* o *Certificatore*) per l'emissione dei Certificati Qualificati, ai sensi del Reg. UE 910/2014, nella generazione e verifica della firma elettronica qualificata del Cliente di FCA Bank S.p.A. (di seguito anche solo *FCA Bank*) nell'ambito dei servizi dalla stessa offerti. Il contenuto di questo Manuale Operativo è conforme a quanto stabilito dalle regole tecniche contenute nel Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 (di seguito DPCM) e dal D. lgs 7 marzo 2005, n. 82, recante il "Codice dell'Amministrazione Digitale" come successivamente modificato e integrato (di seguito "CAD") e conforme al Reg. UE 910/2014 (nel seguito, Reg. eIDAS); in particolare:

- CAD - capo II, Sez. II, che disciplina le firme elettroniche e i certificatori;
- CAD - capo VII, che prevede le modalità con le quali vengono dettate le regole tecniche previste dal Codice.

Per quanto non espressamente previsto nel presente Manuale Operativo si fa riferimento alle norme vigenti e future che regolano la fattispecie concreta.

In questo contesto, i Titolari di un Certificato Qualificato sono solo i soggetti identificati dalla stessa FCA Bank che, in virtù di specifico accordo con il Certificatore, è autorizzato a svolgere la funzione di Registration Authority.

Il processo prevede che il Titolare possa avviare la procedura di Firma Digitale Remota di documenti, atti, contratti, ordini, relativi a prodotti e servizi prestati o distribuiti da FCA Bank.

Le attività descritte nel presente Manuale Operativo sono svolte in conformità con il Reg. UE 910/2014 (eIDAS).

A.1. Proprietà intellettuale

Il presente Manuale Operativo è di esclusiva proprietà di In.Te.S.A. S.p.A., che è Titolare di ogni relativo diritto intellettuale.

Quanto qui descritto per l'espletamento delle attività di QTSP è coperto da diritti sulla proprietà intellettuale.

A.2. Validità

Quanto descritto in questo documento si applica al QTSP INTESA (alle sue infrastrutture logistiche e tecniche, nonché al suo personale), ai Titolari dei certificati da esso emessi e a quanti utilizzino tali certificati per verificare l'autenticità e l'integrità dei documenti cui sia apposta una firma elettronica qualificata relativa ad essi, anche avvalendosi delle marche temporali qualificate emesse da INTESA, nonché a FCA Bank in qualità di Local Registration Authority.

L'uso delle chiavi e dei relativi certificati emessi è regolato da quanto disposto dall'Art.5 c.4 DPCM 22/02/2013, in cui si dispone che le chiavi di creazione e verifica della firma e i correlati servizi, si distinguono secondo le seguenti tipologie:

a) chiavi di sottoscrizione, destinate alla generazione e verifica delle firme apposte o associate ai documenti;
b) chiavi di certificazione, destinate alla generazione e verifica delle firme apposte ai certificati qualificati, alle informazioni sullo stato di validità del certificato ovvero alla sottoscrizione dei certificati relativi a chiavi di validazione temporale elettronica;
c) chiavi di marcatura temporale, destinate alla generazione e verifica delle marche temporali;
d) chiavi dedicate alla sottoscrizione delle informazioni sullo stato di validità dei certificati (OCSP);
e) chiavi destinate alla sottoscrizione del separato certificato di attributo.

B. Generalità

Il presente documento ha come obiettivo la descrizione, in termini generali, delle procedure e delle relative regole che disciplinano l'emissione di certificati qualificati da parte del QTSP INTESA.

Le suddette regole e procedure scaturiscono dall'ottemperanza alle attuali normative di riferimento la cui osservanza permette ad INTESA di essere inserita nell'elenco dei certificatori accreditati.

Pertanto, al fine di adempiere alle normative menzionate, risulterà necessario il coinvolgimento di più entità che saranno meglio identificate nel prosieguo del documento.

B.1. Dati identificativi della versione del Manuale Operativo

Il presente documento è la versione n. ***01*** del ***Manuale Operativo per le procedure di firma digitale qualificata remota nell'ambito dei servizi di FCA Bank***, emesso in conformità con l'Art.40 del DPCM.

L'object identifier di questo documento è ***1.3.76.21.1.50.8***.

Il presente Manuale Operativo è pubblicato e consultabile per via telematica:

- all'indirizzo Internet del QTSP, *https://www.intesa.it/e-trustcom/*
- all'indirizzo Internet dell'Agenzia per l'Italia Digitale, *www.agid.gov.it*

Nota: la pubblicazione di versioni aggiornate del presente Manuale Operativo potrà avvenire solo previa autorizzazione dell'Agenzia per l'Italia Digitale.

B.2. Dati identificativi del QTSP – Qualified Trust Service Provider

Il QTSP (*Prestatore di Servizi Fiduciari Qualificato*) è la società ***In.Te.S.A. S.p.A.***, di cui di seguito sono riportati i dati identificativi.

Denominazione sociale	*In.Te.S.A. S.p.A.*
Indirizzo della sede legale	*Strada Pianezza, 289* *10151 Torino*
Legale Rappresentante	*Amministratore Delegato*
Registro delle Imprese di Torino	*N. Iscrizione 1692/87*
N. di Partita I.V.A.	*05262890014*
N. di telefono (centralino)	*+39.011.19216.111*
Sito Internet	*www.intesa.it*
Indirizzo di posta elettronica	*marketing@intesa.it*
Indirizzo (URL) registro dei certificati	*ldap://x500.e-trustcom.intesa.it*
ISO Object Identifier (OID)	*1.3.76.21*

B.3. Responsabilità del Manuale Operativo

La responsabilità del presente Manuale Operativo, ai sensi dell'Art.40 comma 3 lett. c) del DPCM, è del QTSP INTESA, che ne cura la stesura e la pubblicazione.

Nel caso fosse necessario procedere con l'aggiornamento e ogni eventuale revisione del presente documento Intesa lo comunicherà senza ritardo a FCA Bank e in accordo con essa procederà alle modifiche.

Allo scopo di raccogliere eventuali osservazioni e richieste di chiarimenti, INTESA ha predisposto i seguenti strumenti:

- un recapito di posta elettronica: *marketing@intesa.it*
- un recapito telefonico: +39 011.192.16.111
- un servizio di Help Desk per le chiamate dall'Italia: 800.80.50.93
  per le chiamate dall'estero: +39 02.39.30.90.66

B.4. Entità coinvolte nei processi

All'interno della struttura del QTSP vengono identificate delle entità che prendono parte ai processi relativi all'emissione dei certificati.

Tali attori operano in ottemperanza alle regole e ai processi posti in opera dal QTSP espletando, per la parte di loro competenza, le attività a loro attribuite.

B.4.1. Certification Authority (CA)

INTESA, operando in ottemperanza a quanto previsto dal DPCM, CAD e dal Reg. eIDAS, espleta le attività di Qualified Trust Service Provider. Tali attività includono i servizi fiduciari qualificati di creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche (marche temporali).

I dati identificativi del QTSP INTESA sono riportati al precedente par. *B.2*.

Il personale responsabile delle attività di certificazione, in conformità con l'Art.38 del DPCM, è articolato nelle figure seguenti:

a) Responsabile della sicurezza.
b) Responsabile del servizio di certificazione e validazione temporale.
c) Responsabile della conduzione tecnica dei sistemi.
d) Responsabile dei servizi tecnici e logistici.
e) Responsabile delle verifiche e delle ispezioni (auditing).

Le figure sopra elencate sono tutte appartenenti all'organizzazione del QTSP INTESA.

B.4.2. Local Registration Authority (LRA)

Per la particolare tipologia di servizio offerto (firma elettronica qualificata remota nell'ambito delle applicazioni bancarie e finanziarie) descritta nel presente Manuale Operativo, il QTSP INTESA può demandare lo svolgimento delle funzioni di Registration Authority a FCA Bank tramite apposito atto di mandato.

FCA Bank, in qualità di LRA, si impegna a svolgere le seguenti attività:

- Identificazione del Titolare;
- Registrazione del Titolare.

FCA Bank, nell'esercizio della funzione di Registration Authority, dovrà vigilare affinché l'attività di riconoscimento si svolga nel rispetto della normativa vigente e di quanto previsto nel presente Manuale Operativo.

In particolare, FCA Bank, nel rispetto della normativa antiriciclaggio, così come previsto dal D.lgs. 231/07 e ss.mm.ii., nonché dalle Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo, potrà identificare il Titolare e verificarne con certezza l'identità (vedi contenuti degli obblighi di *adeguata verifica*) anche se questi non si presenterà fisicamente presso il Dealer (convenzionato con la LRA e abilitato all'identificazione della clientela secondo quanto definito nell'accordo di convenzionamento) ovvero l'ufficio di FCA Bank preposto.

In particolare, sia nei casi di operatività a distanza che in presenza, FCA Bank applicherà e verificherà il corretto espletamento delle seguenti misure, applicabili a seconda del prodotto e dell'operatività scelta dal cliente:

- acquisizione dei dati identificativi ed effettuazione di riscontro su un documento di identità in corso di validità di cui è acquisita copia;
- acquisizione copia della Tessera sanitaria in casi di valutazione elevata del rischio;
- acquisizione di un ulteriore documento identificativo in corso di validità di cui è acquisita copia in casi di valutazione elevata del rischio;
- acquisizione copia documento di reddito (ove richiesto in caso di finanziamento);
- ricezione di un bonifico "di riconoscimento" ordinato dal cliente e dall'eventuale cointestatario (in caso di conto co-intestato);
- verifica dell'account di posta elettronica tramite One Time Password (OTP) inviato via e-mail o altro codice one time di verifica (ad es. magic link);
- allineamento SDD (SEDA) sul conto corrente del Cliente (nei casi di identificazione per la clientela carte di credito e prestiti personali);
- welcome call al cliente (nei casi di identificazione per la clientela polizze e di apertura di credito);
- controlli Scipafi (o altre fonti terze autoritative) sui dati e documenti acquisiti;

infine, per i clienti per i quali uno dei controlli precedenti fallisca o presenti anomalie, sarà richiesta documentazione supplementare quale ad esempio una copia dell'estratto conto della banca d'appoggio con l'indicazione della filiale di riferimento ovvero un secondo documento di identificazione.

In ogni caso la LRA si impegna a garantire l'identificazione certa dell'utente prima del rilascio del certificato qualificato.

C. Obblighi

C.1. Obblighi del Prestatore di Servizi Fiduciari Qualificato (QTSP)

Nello svolgimento della sua attività, il Prestatore di Servizi Fiduciari Qualificato (indicato anche come *Certificatore Accreditato*) opera in conformità con quanto disposto dal:

- Decreto Legislativo del 7 marzo 2005, n.82 e successive modifiche.
- Decreto Presidente del Consiglio dei Ministri 22 febbraio 2013.
- Regolamento (UE) 2016/679 (GDPR)
- Regolamento (UE) 910/2014 (eIDAS)

In particolare, il QTSP:

- adotta tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
- si attiene alle regole tecniche specificate nel DPCM e ss.mm.ii.;
- garantisce che il proprio Sistema qualità sia conforme alle norme ISO 9001;
- assicura che il dispositivo per la generazione delle firme (HSM) abbia i requisiti di sicurezza previsti dall'Art.29 del Reg. eIDAS;
- rilascia e rende pubblico il certificato qualificato, se non diversamente specificato dal Titolare, secondo quanto stabilito all'Art.32 del CAD;
- informa i richiedenti, in modo esplicito e chiaro, sulla procedura di certificazione, sui necessari requisiti tecnici per accedervi, sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
- si attiene alle misure di sicurezza per il trattamento dei dati personali (GDPR);
- non si rende integralmente depositario dei dati per la creazione della firma del Titolare;
- procede alla pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del Titolare o del terzo interessato;
- assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
- tiene registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato per 20 (venti) anni in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
- assicura che il codice identificativo (di esclusiva pertinenza del QTSP) assegnato a ciascun Titolare sia univoco nell'ambito dei propri utenti;
- predispone su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione. Tra questi citiamo: gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie. Dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio e il QTSP;
- utilizza sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal Titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza;
- registra l'emissione dei certificati qualificati nel giornale di controllo con la specificazione della data e dell'ora della generazione.

Secondo quanto stabilito dall'Art.14 del DPCM, il Certificatore fornisce ovvero indica almeno un sistema che consenta di effettuare la verifica delle firme digitali.

Inoltre, il QTSP:

- genera un certificato qualificato, per ciascuna delle chiavi di firma elettronica avanzata utilizzate dall'Agenzia per l'Italia Digitale per la sottoscrizione dell'elenco pubblico dei certificatori, e lo pubblica nel proprio registro dei certificati ai sensi dell'Art.42 del DPCM;
- indica un sistema di verifica della firma elettronica, di cui all'Art.10 del DPCM;
- mantiene copia della lista, sottoscritta dall'Agenzia per l'Italia Digitale, dei certificati relativi alle chiavi di certificazione di cui all'Art.43 del DPCM, e la rende accessibile per via telematica come stabilito dall'Art.42, comma 3 del DPCM.

C.2. Obblighi del Titolare

Il richiedente un certificato qualificato (Titolare) per i servizi descritti nel presente Manuale Operativo è un cliente di FCA Bank, ovvero un soggetto afferente all'organizzazione di quest'ultima, che opera da Registration Authority.

Il Titolare riceverà un certificato qualificato per la Firma Elettronica Qualificata Remota, con cui poter sottoscrivere contratti e documenti relativi a prodotti e/o servizi offerti da FCA Bank, nelle modalità descritte al par. *I. Modalità operative per la sottoscrizione di documenti*.

Il Titolare è tenuto a conservare le informazioni necessarie all'utilizzo della propria chiave privata di firma (si pensi ad esempio agli eventuali codici monouso ricevuti sul proprio cellulare) in modo adeguato e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri (CAD, art. 32, comma 1).

Il Titolare della chiave deve inoltre:

- fornire tutte le informazioni richieste dal QTSP, garantendone l'attendibilità sotto la propria responsabilità;
- inoltrare la richiesta di certificazione secondo le modalità indicate in questo Manuale Operativo;
- comunicare al QTSP, anche per tramite di FCA Bank, eventuali variazioni alle informazioni fornite all'atto della registrazione: dati anagrafici, residenza, recapiti telefonici, indirizzo di posta elettronica, ecc.;
- conservare con la massima cura e diligenza le informazioni di abilitazione all'uso della chiave privata;
- dare immediata comunicazione al QTSP, per il tramite di FCA Bank, in caso di perdita o furto dei codici e/o dei dispositivi indicati per accedere alle proprie chiavi di firma (es cellulare) affinché FCA Bank e il QTSP possano provvedere l'immediato blocco del certificato e dei canali di accesso agli stessi;
- inoltrare eventuali richieste di revoca e di sospensione del certificato qualificato secondo quanto indicato nel presente Manuale Operativo.

C.3. Obblighi degli utilizzatori dei certificati

Utilizzatore (*Relying Party*) è chiunque riceva un documento firmato digitalmente e, al fine di verificarne la validità, si avvalga del Certificato Qualificato utilizzato dal Titolare per firmare il documento stesso.

La verifica della firma digitale e la successiva estrazione degli oggetti firmati può essere effettuata con qualsiasi software in grado di elaborare file firmati in conformità al Reg. eIDAS.

Coloro che si avvalgono di un Certificato Qualificato per verificare la validità di un documento firmato digitalmente, sono tenuti a:

- verificare la validità del certificato contenente la chiave pubblica del Titolare firmatario del messaggio, secondo quanto indicato dagli standard vigenti al momento della sua emissione;
- verificare lo stato di validità del certificato mediante il protocollo OCSP o tramite l'accesso alle Liste di Revoca (CRL);
- verificare la validità del percorso di certificazione, basato sull'elenco pubblico dei QTSP;
- verificare l'esistenza di eventuali limitazioni all'uso del certificato utilizzato dal Titolare.

C.4. Obblighi del Terzo Interessato

Il Terzo Interessato, nei servizi descritti dal presente Manuale Operativo, è rappresentato dalle società del gruppo FCA Bank laddove quest'ultime abbiano la necessità di rilasciare al richiedente un certificato qualificato contenente anche i dati della specifica LRA.

In tali circostanze, la consociata FCA Bank, nella veste di Terzo Interessato:

- verifica che il Cliente sia in possesso di tutti i requisiti necessari e autorizza il Cliente stesso a richiedere il rilascio del Certificato Qualificato per la Firma Digitale Remota;
- svolge un'attività di supporto al Titolare;
- indica al QTSP eventuali ulteriori limitazioni d'utilizzo del Certificato Qualificato per la Firma Digitale oltre a quelle previste al par. *F.1.1*.

FCA Bank o sue consociate, in qualità di Terzo Interessato potranno quindi indicare al QTSP eventuali limitazioni d'uso del certificato, eventuali poteri di rappresentanza e dovrà comunicare qualsiasi variazione delle stesse.

A titolo esemplificativo si riportano le seguenti circostanze:

- variazione o cessazione dei poteri di rappresentanza;
- variazione di ruoli e qualifiche interne;
- cessazione del rapporto di dipendenza.

La richiesta di revoca o sospensione da parte del Terzo Interessato dovrà essere immediatamente inoltrata alla CA quando vengano meno i requisiti in base ai quali al Titolare era stato rilasciato un certificato qualificato per la firma elettronica.

C.5. Obblighi delle Registration Authority esterne (LRA)

Il QTSP INTESA, per esigenze connesse alla fornitura del servizio, si avvale su tutto il territorio comunitario di ulteriori soggetti (nel seguito denominati RA esterne o LRA – Local Registration Authority) per svolgere una parte delle attività proprie dell'Ufficio di registrazione.

Il QTSP In.Te.S.A. S.p.A. può demandare lo svolgimento della funzione di Registration Authority alle consociate FCA Bank del gruppo bancario mediante specifico documento di Mandato.

In particolare, le RA esterne espletano le seguenti attività:

- identificazione certa del richiedente il certificato qualificato (in seguito Titolare del certificato);
- registrazione del Titolare;
- consegna al Titolare dei dispositivi e/o codici che gli permetteranno di accedere alla propria chiave di firma nel rispetto degli Art.8 e 10 comma 2 del DPCM;
- invio della documentazione sottoscritta all'Ufficio RA del QTSP INTESA, salvo differenti accordi riportati sul Mandato.

Nel Mandato sono esplicitati gli obblighi cui si deve attenere FCA Bank alla quale il QTSP INTESA assegna l'incarico di LRA e sui quali il QTSP ha l'obbligo di vigilare.

In particolare, si richiede alla LRA di:

- vigilare affinché l'attività di identificazione posta in essere si svolga nel rispetto della normativa vigente (normativa in materia Antiriciclaggio, CAD, DPCM, Reg. eIDAS);
- rendere possibile il tracciamento dell'operatore di LRA che ha effettuato l'identificazione del Titolare;
- utilizzare e trattare i dati personali acquisiti in fase di riconoscimento in accordo con il GDPR;
- rendere disponibile ad INTESA il materiale raccolto nella fase di identificazione e registrazione;
- conservare in modo sicuro la documentazione raccolta nella fase di identificazione e registrazione, quindi inviarla all'Ufficio RA del QTSP INTESA su richiesta della QTSP stessa;
- consentire l'accesso presso i propri locali di personale del QTSP, ovvero di terzi dallo stesso incaricati, per adempiere agli obblighi di ispezione (audit); tale accesso deve essere consentito anche agli auditor incaricati dall'Organismo di Vigilanza (AgID);
- segnalare senza indugio al QTSP INTESA, per tramite dell'Ufficio RA (*uff_ra@intesa.it*) ovvero dei propri riferimenti INTESA, ogni evento o incidente inerente i punti indicati precedentemente, nonché tutte le violazioni della sicurezza o le perdite di integrità che abbiano un impatto significativo sui servizi oggetto del presente Manuale Operativo o sui dati personali dei titolari.

C.5.1. Identificazione del Titolare

Il processo di identificazione, eseguito in piena aderenza alla normativa antiriciclaggio, avviene secondo una delle modalità di seguito descritte:

- ***Canonica***: il Richiedente viene identificato ai sensi della normativa antiriciclaggio in modalità de visu presso un Dealer FCA Bank (convenzionato con la LRA e abilitato all'identificazione della clientela secondo quanto definito nell'accordo di convenzionamento).
- ***On line***: se il Richiedente sceglie la modalità di adesione diretta ed è già titolare di un conto corrente presso una Banca, per essere riconosciuto ai fini della normativa antiriciclaggio, potrà:
  - utilizzare una procedura SEPA (o SDD - SEPA Direct Debit);
  - disporre un bonifico dal conto corrente già aperto presso la Banca di cui sopra.
- **Video identificazione da remoto**: nella modalità "con operatore" ovvero, in alternativa, "self + welcome call" oppure "self + attività di adeguata verifica", più ampiamente descritte al par. *F.1.2*.

Attraverso le procedure di cui sopra, il QTSP INTESA, per il tramite delle prassi antiriciclaggio messe in atto dalla consociata FCA Bank (LRA), entrerà in possesso di tutte le informazioni previste dalla legge, in totale sicurezza e nel pieno rispetto della privacy.

D. Responsabilità e limitazioni agli indennizzi

D.1. Responsabilità del QTSP – Limitazione agli indennizzi

Il QTSP INTESA è responsabile verso i Titolari per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività previste dal DPCM, dal GDPR, dal CAD e dal Reg. eIDAS (e ogni loro ss.mm.ii.), come descritto al par. *C.1. Obblighi del Prestatore di Servizi Fiduciari Qualificato (QTSP)*.

INTESA, fatti salvi i *casi di dolo o colpa* (Reg. eIDAS, Art.13), non assume alcuna responsabilità per le conseguenze derivanti da un uso dei certificati diverso da quanto disposto dall'Art.5 del DPCM, e in particolare dal mancato rispetto da parte del Titolare e dal Terzo Interessato di quanto indicato nel presente Manuale Operativo e/o dalla mancata osservanza da parte degli stessi della normativa vigente.

Parimenti, INTESA non potrà essere ritenuta responsabile delle conseguenze dovute a cause ad essa non imputabili, quali, a solo titolo esemplificativo: calamità naturali, disservizi e/o disfunzioni tecniche e logistiche al di fuori del proprio controllo, interventi dell'Autorità, rivolte o atti di guerra che colpiscano anche o solo i soggetti delle cui attività INTESA si avvale per la prestazione dei propri servizi di certificazione.

Il QTSP INTESA non sarà responsabile per i danni derivanti da un utilizzo non conforme del Certificato Qualificato per la Firma digitale Remota in relazione alla limitazione d'uso come specificata al par. *F.1.1* ovvero *F.3.1*.

Il Titolare, a seguito della presa visione del presente Manuale Operativo, deve porre in opera tutte quelle misure di speciale diligenza atte ad evitare danni a terzi legati all'uso improprio di quanto fornito dal certificatore accreditato. Si ricorda, in particolare, di conservare con la dovuta diligenza i dispositivi OTP e/o i codici segreti indispensabili per accedere alle chiavi di firma.

D.2. Assicurazione

Il QTSP INTESA è beneficiario di contratti assicurativi per la copertura dei rischi dell'attività e dei danni causati a terzi, il cui contenuto è in linea con quanto necessario per svolgere l'attività professionale di cui trattasi.

Di tale contratto è resa disponibile ad AgID apposita dichiarazione di stipula.

E. Tariffe

Il Servizio viene fornito da FCA Bank ai propri Clienti. Nei casi in cui siano previste tariffe a carico dell'utente finale per l'emissione, rinnovo, revoca e sospensione del certificato qualificato saranno indicate nei contratti stipulati tra Cliente e FCA Bank.

F. Modalità di identificazione e registrazione degli utenti

F.1. Identificazione degli utenti

Il QTSP deve verificare con certezza l'identità del richiedente alla prima richiesta di emissione di certificato qualificato.

La suddetta operazione può essere demandata a FCA Bank che, in qualità di LRA e in ottemperanza con quanto previsto dalla vigente normativa in materia di Antiriciclaggio, identificherà e registrerà il Titolare.

Nei casi di certificati a lungo termine, per i successivi rinnovi, se effettuati quando il certificato qualificato è ancora in corso di validità, tale attività non dovrà essere ripetuta: sarà cura del Titolare comunicare al QTSP, attraverso FCA Bank, gli eventuali cambiamenti relativi ai propri dati di registrazione.

Nei casi di certificati one-shot trovano invece applicazione le indicazioni di cui al successivo par. *F.5*.

Fra i dati di registrazione necessari per l'esecuzione del servizio oggetto del presente documento ricordiamo:

- Nome e Cognome;
- Data di nascita;
- Comune o stato estero di nascita;
- Codice fiscale;
- Indirizzo di residenza;
- Numero di telefono cellulare personale;
- Indirizzo di posta elettronica;
- Tipo e numero del documento d'identità esibito;
- Autorità che ha rilasciato il documento e data e luogo del rilascio e di scadenza.

Il numero di cellulare personale del richiedente verrà utilizzato dal QTSP per l'invio di codici numerici monouso (chiamati nel seguito codici OTP o semplicemente OTP) in grado di garantire un accesso sicuro al servizio di firma remota resogli disponibile da FCA Bank.

Oltre all'OTP, nel caso in cui il Titolare faccia uso di certificati qualificati a lungo termine, saranno forniti tutte le informazioni necessarie e un Personal Identification Number (PIN) da utilizzare in abbinamento all'OTP quale secondo fattore di autenticazione.

Lo stesso PIN potrà essere utilizzato come *codice di emergenza* (in caso, ad esempio, di smarrimento e/o indisponibilità dell'OTP) per *sospendere con urgenza* il certificato qualificato in corso di validità a lui intestato (par. *H.4*).

Per il caso d'uso di certificati a lungo termine, vengono anche fornite al Titolare le necessarie informazioni per permettergli di cambiare in un qualsiasi momento il numero di cellulare precedentemente fornito.

Preventivamente al rilascio di un certificato qualificato, il Titolare dovrà inoltre:

- prendere visione del Manuale Operativo del QTSP INTESA;
- autorizzare il trattamento dei propri dati personali per le finalità legate all'emissione di un certificato qualificato per la firma elettronica.

La documentazione relativa alla registrazione dei Titolari è conservata per 20 (venti) anni.

F.1.1. Limiti d'uso

Nel Certificato Qualificato per la firma elettronica, emesso nell'ambito dei servizi descritti nel presente Manuale e offerti da FCA Bank, è inserito sempre un limite d'uso, che deve essere riportato sia in lingua italiana, sia in lingua inglese.

Le formule standard sono le seguenti:

#1

"Il presente certificato e' valido solo per firme apposte con procedura automatica per la sottoscrizione di documenti e/o contratti relativi a prodotti e/o servizi offerti o distribuiti da Nome Banca / Istituto gruppo FCAB."

"This certificate may only be used for unattended/automatic digital signature for the signature of documents concerning products and/or services offered or distributed by Name of Bank or Company belonging FCAB Group."

#2

"Il presente certificato e' valido solo per firme elettroniche apposte con procedura automatica. Il presente certificato e' valido solo per la sottoscrizione di documenti e contratti relativi ai servizi di conto deposito e carte di credito erogati da Nome Banca / Istituto gruppo FCAB ai propri Clienti."

"This certificate may only be used for unattended/automatic electronic signature. This certificate may be used only to sign documents and contracts relating to deposit account and credit card services provided by Name of Bank or Company belonging FCAB Group its Customers."

#3

"Il presente Certificato Qualificato e' valido solo per la sottoscrizione di documenti e contratti relativi ai servizi di conto deposito e carte di credito erogati da Nome Banca / Istituto gruppo FCAB ai propri Clienti."

"This Qualified Certificate may only be used for signing documents and contracts relating to deposit accounts and credit cards' services provided by Name of Bank or Company belonging FCAB Group."

Eventuali ulteriori specifici limiti d'uso potranno essere concordati con FCA Bank.

INTESA non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti allo stesso o derivanti dal superamento di tale limite.

F.1.2. Identificazione degli utenti da remoto (video identificazione)

Nel rispetto delle normative vigenti, il riconoscimento del Titolare può essere eseguito attraverso una procedura di identificazione remota tramite webcam, in modalità assistita con operatore ovvero, in alternativa, in modalità video self.

Il servizio consente al cliente di collegarsi nel momento a lui più comodo senza necessariamente doversi spostare dal luogo in cui si trova per eseguire tale procedura.

F.1.2.1. Video identificazione con operatore

Questa modalità prevede un'interazione tra richiedente e operatore completamente «online» e assistita, favorendo l'esperienza d'uso ed agevolando tutti coloro meno consoni all'uso delle tecnologie.

A fronte della conferma da parte dell'operatore di avvenuta identificazione, il video viene cifrato e inviato in Conservazione a Norma.

Il servizio di identificazione si sviluppa come segue:

- Il Richiedente, in possesso di un device (PC, tablet, smartphone) abilitato ad una connessione Internet e dotato sia di una webcam che di un sistema audio funzionante, riceve un'e-mail di invitation contenente un link per l'accesso alla piattaforma di riconoscimento.
- Il Richiedente si connette alla piattaforma di riconoscimento. All'interno di questa piattaforma, il Richiedente trova un form che lo guida nell'inserimento dei dati utili al set-up del processo di video riconoscimento (dati anagrafici, dati del documento di identità, dati di residenza, dati di contatto tra cui e-mail e cellulare, etc.) e nel caricamento delle scansioni del documento di riconoscimento.
- Nel caso in cui la richiesta sia per un certificato a lungo termine, in questa fase la piattaforma di video riconoscimento permette la scelta, da parte del Richiedente, del PIN e del codice di emergenza che potrà utilizzare con il certificato che verrà rilasciato al termine del riconoscimento.
- Vengono quindi mostrati al richiedente l'informativa privacy, l'informativa di processo, il Manuale Operativo, le eventuali Policy legate all'utilizzo del certificato e raccolti obbligatoriamente i relativi consensi.
  Le informative di cui sopra fanno riferimento a documenti che l'utente potrà scaricare agevolmente dalla piattaforma.
- In questa fase vengono anche mostrate le istruzioni per un corretto svolgimento degli step successivi.

- Precisiamo, a tal proposito, che la buona qualità del collegamento audio-video è fondamentale affinché la procedura di identificazione possa essere effettuata con successo; infatti, in caso di disturbi sulla linea e/o problemi che non rendessero possibile la verifica certa dell'identità del Richiedente, l'operatore di RA interromperà la sessione, invitando il Richiedente a prendere un nuovo appuntamento quando saranno stati risolti i problemi riscontrati.
- Completata la fase di inserimento dati e invio (upload) dei documenti necessari per l'identificazione, il Richiedente potrà continuare la sessione attivando appena possibile il collegamento via webcam.
- All'inizio della sessione di video riconoscimento l'operatore si qualificherà e chiederà il consenso alla videro registrazione al richiedente.
- Durante la sessione on-line (via webcam), l'operatore di RA domanda al soggetto richiedente di presentarsi con i documenti di riconoscimento precedentemente inviati e controlla che i documenti siano gli stessi, verificando che nella foto del documento sia riconoscibile il Richiedente. Inoltre, l'operatore chiede al soggetto di effettuare azioni estemporanee al fine di accertare la reale presenza nella postazione remota del richiedente.
- Nel corso della sessione l'operatore verificherà il possesso dell'e-mail e del numero di cellulare inviando al richiedente un OTP/SMS ed un magic link che dovranno essere verificati prima di poter procedere
- L'intera sessione viene registrata in modalità audio e video e la sequenza viene poi cifrata con una chiave pubblica messa a disposizione dalla Certification Authority. La stessa CA conserva la chiave privata e la rende disponibile solo in caso di contenzioso ad un perito di parte e/o agli enti di vigilanza che richiedessero un controllo sulle attività svolte.
- La registrazione audio/video della sessione deve essere di buona qualità (immagine a colori, definizione delle riprese chiare e a fuoco, adeguata luminosità e contrasto, ripresa distinguibile del documento di riconoscimento inquadrato). L'intera sessione audio/video deve essere fluente e continua, senza alcuna interruzione.
  L'operatore che effettua l'identificazione può escludere l'ammissibilità della sessione audio/video per qualunque ragione, inclusa l'eventuale inadeguatezza del documento presentato dal richiedente (ad esempio perché logoro o carente delle caratteristiche elencate).
- Completati i controlli relativi ai documenti di riconoscimento presentati, al Richiedente vengono date le informazioni necessarie per permettergli, successivamente, di utilizzare il certificato qualificato che verrà emesso.
- In particolare, viene illustrato come poter utilizzare, ai fini della firma, l'OTP/SMS ricevuto sul numero di cellullare censito e verificato nel corso della sessione di video riconoscimento.
- Al termine del processo, il certificato di firma viene emesso dalla Certification Authority e al Richiedente, ora Titolare di certificato, viene anche associato un identificativo univoco presso il QTSP.

Il numero di cellulare personale del richiedente verrà utilizzato dal QTSP per l'invio di codici numerici monouso (chiamati nel seguito codici OTP o semplicemente OTP) in grado di garantire un accesso sicuro al servizio di firma remota resogli disponibile da FCA Bank.

Oltre all'OTP, nel caso in cui il Titolare faccia uso di certificati qualificati a lungo termine, saranno forniti tutte le informazioni necessarie e un Personal Identification Number (PIN) da utilizzare in abbinamento all'OTP quale secondo fattore di autenticazione.

Per il caso d'uso di certificati a lungo termine, vengono anche fornite al Titolare le necessarie informazioni per permettergli di cambiare in un qualsiasi momento il numero di cellulare precedentemente fornito.

Le tracce audio/video sopracitate relative all'identificazione e registrazione dei titolari, vengono conservate dal QTSP INTESA per 20 (venti) anni.

F.1.2.2. Video identificazione in modalità self & welcome call

In alternativa al video riconoscimento descritto al paragrafo precedente, una possibile modalità di video identificazione è rappresentata dalla modalità "*self + welcome call*".

Il processo prevede che l'utente, in fase di identificazione, venga guidato dal sistema ad eseguire una serie di passi all'interno di una sessione video registrata.

Al richiedente sarà richiesto di:

- caricare o fotografare il proprio documento d'identità per acquisizione (dati anagrafici e foto);

- inserire il proprio codice fiscale o, eventualmente, caricare/fotografare il proprio tesserino sanitario o tesserino del codice fiscale attualmente rilasciato;
- verificare l'indirizzo di posta elettronica e il numero di cellulare tramite OTP e/o Link di verifica;
- riprendere il proprio volto tramite un *video selfie* (per confronto biometrico), eseguendo contestualmente alcune azioni casuali guidate del volto guidate verifica del *liveness*. Lo stream sarà successivamente analizzato utilizzando algoritmi di riconoscimento facciale per rilevare i movimenti del viso.

Il processo di verifica potrà avvenire in automatico, attraverso un algoritmo di *Face Recognition*, per match biometrico tra foto del documento di identità e ripresa del volto (tramite alcuni fotogrammi).

In modalità *unattended* per il richiedente, vengono quindi eseguite una serie di verifiche tra cui:

- controllo sui dati anagrafici;
- verifica di leggibilità delle foto dei documenti d'identità e confronto tra fotogrammi del Video Self e la foto sul documento di identità;
- confronto tra i dati inseriti nel portale e quelli riportati nei documenti d'identità caricati;
- verifica della liveness;
- verifica con fonte autoritativa (Scipafi).

In caso di esito positivo, il video sarà accettato dal sistema, altrimenti si inviterà l'utente ad effettuare la video identificazione con operatore ovvero a recarsi presso gli uffici dell'intermediario per effettuare l'adeguata verifica e il video sarà cancellato.

In caso di positivo riscontro dei controlli suindicati, un operatore autorizzato verificherà i dati del richiedente relativi ai video accettati dal sistema e confermerà il riconoscimento solo dopo aver effettuato una procedura di *welcome call*, nella quale chiederà al titolare di confermare i suoi dati e la volontà di richiedere un certificato qualificato.

Il video sarà cifrato e memorizzato su sistemi del QTPS INTESA insieme alla registrazione della welcome call.

La procedura di welcome call, necessaria ai fini dell'identificazione certa del Titolare, si compone dei seguenti step:

- Le informazioni raccolte dal Portale e dall'applicazione sono passate al backoffice e al Service Telefonico, per il completamento del riconoscimento.
- Il Cliente è quindi chiamato dal Service Telefonico (*Welcome Call*) per una verifica incrociata dell'identità: saranno poste in questa fase al cliente una serie di domande per verificare la corrispondenza tra risposte fornite e i dati/documenti acquisiti con il Self ID.

Allo scopo di assicurare la conformità del procedimento a quanto disposto dalle normative vigenti che regolano la materia, la chiamata sarà registrata e conservata per il periodo previsto di 20 (venti) anni. La registrazione della welcome call potrà essere utilizzata quale ulteriore evidenza atta a confermare l'identità della persona e la sua volontà a procedere con la richiesta di un certificato qualificato.

F.1.2.3. Video identificazione in modalità self & adeguata verifica

In alternativa al video riconoscimento descritto al paragrafo precedente, una possibile modalità di video identificazione è rappresentata dalla modalità "*self + adeguata verifica"* in ambito antiriciclaggio.

Per *adeguata verifica* si intende la possibilità, da parte di FCA Bank, di poter adottare le prassi previste dalla normativa afferente la verifica dell'identità di cui al D.lgs. 231/2007, ove applicabile, ovvero in applicazione della normativa afferente la verifica dell'identità ai sensi della Direttiva (UE) 2018/843 e relative implementazioni a livello dei singoli Stati Membri.

In taluni contesti di mercato bancario e finance, si evidenzia una spiccata ricerca di meccanismi di onboarding innovativi, rapidi e veloci tali per cui, sebbene la procedura video self appaia inizialmente come una soluzione particolarmente adatta al contesto, si rivela poi essere scarsamente adottata per la presenza della richiesta di welcome call, in quanto, proprio in questo specifico contesto regolamentato in ambito antiriciclaggio, risulta essere una misura ridondante rispetto alle operazioni di verifica normalmente attuate dal soggetto obbligato ai fini dell'espletamento degli obblighi previsti dalla normativa di riferimento.

In tal senso, questa specifica casistica di identificazione prevede l'integrazione del video self (par. *F.1.2.2*) all'interno del processo di adeguata verifica bancaria in modo tale che, in aggiunta all'esecuzione del video self, in luogo della welcome call sia ipotizzabile un'azione rafforzativa in ambito bancario/finanziario sul richiedente che ha aperto il conto e firmato un contratto con un certificato qualificato.

Tale azione, poiché effettuata all'interno di un contesto regolamentato e securizzato, quale appunto quello dei processi di adeguata verifica in ambito antiriciclaggio, è funzionale per la conferma dell'identità del richiedente e della volontà all'ottenimento del certificato.

Nel seguito sono riportate le azioni rafforzative previste da FCA Bank e sue consociate:

- acquisizione dei dati identificativi ed effettuazione di riscontro su un documento di identità in corso di validità di cui è acquisita copia;
- acquisizione copia della Tessera sanitaria in casi di valutazione elevata del rischio;
- acquisizione di un ulteriore documento identificativo in corso di validità di cui è acquisita copia in casi di valutazione elevata del rischio;
- acquisizione copia documento di reddito (ove richiesto in caso di finanziamento);
- ricezione di un bonifico "di riconoscimento" ordinato dal cliente e dall'eventuale cointestatario (in caso di conto co-intestato);
- verifica dell'account di posta elettronica tramite One Time Password (OTP) inviate via e-mail o altro codice one time di verifica (ad es. magic link)
- allineamento SDD (SEDA) sul conto corrente del Cliente (nei casi di identificazione per la clientela carte di credito e prestiti personali);
- welcome call al cliente (nei casi di identificazione per la clientela polizze e di apertura di credito);
- controlli Scipafi (o altre fonti terze autoritative) sui dati e documenti acquisiti;

Attraverso questo modello di identificazione, il cliente prospect della società del gruppo bancario FCA Bank è in grado di accedere ai servizi di una banca e firmare un contratto di apertura conto o di acquisto di un prodotto con un certificato qualificato emesso dopo una procedura video self, che viene quindi perfezionato al termine delle operazioni che rientrano nelle normali attività per il corretto espletamento dell'adeguata verifica.

In aggiunta a quanto sopraindicato, il processo di identificazione e rilascio deve prevedere che:

1. tale certificato contenga stringenti limiti d'uso;
2. che il contratto firmato con tale certificato resti a disposizione della sola banca fino a quando non siano stati ultimati ulteriori controlli finalizzati alla identificazione certa del richiedente, nell'ambito delle procedure di adeguata verifica adottate da FCA Bank e descritte nelle policy antiriciclaggio;
3. che i controlli finalizzati alla identificazione certa del richiedente di cui al punto 2 non prevedano l'impiego del certificato precedente emesso;
4. che tale certificato possa essere utilizzato solo per la firma dell'apertura di un conto ma non richiedere al contempo l'attivazione di un'utenza SPID;
5. che l'uso del certificato stesso venga comunque inibito sino a quando i controlli al punto 2 non vengano completati;
6. Qualora non venga completato il processo di onboarding il contratto deve essere distrutto.

A queste condizioni la welcome call può essere evitata.

F.1.3. Identificazione eseguita da FCA Bank in modalità de visu

In aggiunta alle identificazioni precedentemente descritte, Intesa può delegare l'attività di identificazione certa a FCA Bank in modalità *de visu*.

L'identificazione dovrà avvenire in conformità a quanto indicato al par. *B.4.2*, ovverosia in linea con la rilevante normativa antiriciclaggio (decreto legislativo 21 novembre 2007, n. 231, come modificato dal D. Lgs. 25 maggio 2017, n. 90, dalla direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, come modificata dalla direttiva (UE) 2018/843, ovvero in applicazione della normativa afferente la verifica dell'identità ai sensi della Direttiva (UE) 2018/843, e ss.mm.ii., in aderenza alle relative implementazioni a livello di singolo Stati Membro, nonché gli Orientamenti congiunti delle Autorità di Vigilanza Europee, emanati ai sensi dell'art. 17 e dell'art. 18, par. 4, della direttiva (UE) 2015/849 sulle misure semplificate e rafforzate di adeguata verifica della clientela) e dovrà essere completata e perfezionata prima del rilascio del certificato qualificato.

F.2. Registrazione degli utenti richiedenti la certificazione

Successivamente alla fase di identificazione certa, viene eseguita la registrazione dei dati dei Titolari sugli archivi della Certification Authority.

Questa operazione potrà essere eseguita mediante un'applicazione software direttamente richiamabile dagli applicativi FCA Bank.

Ferma restando l'identificazione certa del Titolare, laddove in fase di registrazione vi siano errori materiali nei dati acquisiti per la registrazione del Titolare, propedeutica all'emissione del certificato, quest'ultimo sarà revocato e ne verrà riemesso uno dopo la correzione sui dati di registrazione.

Nei casi in cui il certificato sia di tipo *one shot*, la revoca non sarà effettuata per vincoli tecnologici derivanti dagli standard internazionali che sottendono la gestione dei certificati X.509.

F.3. Certificati di firma digitale in particolari ambiti chiusi di utenti

È possibile l'emissione di un certificato qualificato di firma elettronica prima che sia conclusa l'identificazione del Titolare solamente nel caso sussistano particolari circostanze riconducibili a limitati utilizzi della firma digitale in contesti chiusi di utenti che non consentono alle firme digitali generate di produrre alcun effetto giuridico qualora la verifica dell'identità del titolare del certificato non termini con esito positivo.

Questa possibilità è stata confermata dall'Agenzia con la comunicazione alle CA del 7 giugno 2016, "*agid.AOO-AgID.REGISTRO UFFICIALE(U).0016101.07-06-2016*", avente per oggetto "*Richiesta di chiarimenti in merito all'utilizzo della firma digitale in particolari ambiti chiusi di utenti*".

Nello specifico, questo tipo di casi d'uso indirizza il rilascio del Certificato Qualificato in quelle circostanze riconducibili a limitati utilizzi della firma elettronica qualificata in contesti chiusi di utenti, che non consentono alle firme elettroniche qualificate generate di produrre alcun effetto giuridico qualora la verifica dell'identità del titolare del certificato non termini con esito positivo.

Tipico è il caso in cui l'oggetto della sottoscrizione è un atto per cui sia prescritta la sottoscrizione di due o più parti, senza le quali è *giuridicamente imperfetto*, privo quindi di qualunque effetto giuridico.

Questo tipo di certificati, in piena aderenza alle previsioni contenute nella comunicazione AgID 0016101.07-06-2016, in presenza di determinati vincoli di dominio e di ambiti di utilizzo, consente l'uso della firma digitale prima di aver ultimato il dovuto processo di verifica dell'identità del titolare, alle seguenti condizioni:

Restrizione	Responsabilità
1. Il processo è riconducibile esclusivamente a sistemi di firma remota;	Certificatore
2. L'uso della firma digitale deve avvenire in ambiti chiusi di utenti;	Certificatore
3. Nel certificato qualificato del titolare devono essere presenti stringenti limiti d'uso afferenti il rapporto specifico fra Titolare e cointeressato e cofirmatario (par. *F.1.1*);	Certificatore
4. Il certificato deve essere chiaramente distinguibile da quelli emessi con procedure più tradizionali. Il certificato qualificato del titolare deve contenere uno specifico OID, riscontrabile nel manuale operativo, in cui è descritto questo particolare processo e il suo ristretto ambito (par. *F.3.2Errore. L'origine riferimento non è stata trovata.*);	Certificatore
5. Devono sussistere stringenti limiti applicativi. L'applicazione che richiede la firma remota deve limitare i possibili oggetti di sottoscrizione ai soli documenti proposti dal cointeressato e cofirmatario. I documenti oggetto della sottoscrizione devono essere giuridicamente imperfetti, cioè privi di effetto fino all'apposizione della firma del cointeressato e cofirmatario. (A titolo di esempio, si citano i contratti per l'adesione ad un servizio).	Cointeressato e Cofirmatario

6. Nel caso in cui la verifica dell'identità del titolare avvenga per mezzo di un incontro fisico fra titolare e addetto alla verifica dell'identità, quest'ultimo deve essere personale del certificatore o soggetto da esso delegato, ma non del cointeressato e cofirmatario se diverso dal certificatore;	Certificatore
7. Il cointeressato e cofirmatario può espletare la verifica dell'identità in vece del certificatore, attraverso sessioni audio-video, attraverso le procedure indicate dal certificatore e approvate dall'AgID, ovvero in applicazione della normativa afferente la verifica dell'identità di cui al D.lgs. 231/2007 e s.m.i., ove applicabile. Qualora, nell'ambito della verifica ai sensi di tale D.lgs. sia utilizzato il bonifico bancario, deve essere verificato che tale bonifico provenga da un conto bancario intestato esclusivamente al titolare del certificato;	Cointeressato e Cofirmatario
8. All'apposizione della firma del titolare il Certificatore si impegna a non apporre la marca temporale.	Certificatore
9. All'apposizione della firma del titolare il Cointeressato e Cofirmatario si impegna a non apporre la marca temporale.	Cointeressato e Cofirmatario
10. La marca temporale deve essere apposta obbligatoriamente dopo la firma del cointeressato e cofirmatario che rende l'atto giuridicamente perfetto;	Cointeressato e Cofirmatario
11. Fino all'apposizione della firma e della marca di cui al precedente punto 10, l'oggetto sottoscritto dal solo titolare non deve essere fornito ad alcuno e, qualora la verifica dell'identità del titolare non avesse buon fine, deve essere distrutto conservando traccia degli eventi in appositi log. In quest'ultimo caso, quale misura a maggior tutela del Cliente Prospect, il certificato viene revocato.	Cointeressato e Cofirmatario

F.3.1. Limite d'uso specifico

Per ottemperare al punto 3) del par. *F.3*, potranno essere utilizzati gli stessi limiti d'uso descritti al par. *F.1.1* tenendo presenti le medesime considerazioni ivi definite.

F.3.2. OID specifico

Per ottemperare al punto 4), il certificato emesso sotto queste condizioni è distinguibile dagli altri certificati in quanto contiene, nel campo uno dei seguenti OID (ognuno definito in riferimento alla *CA di root* che ha emesso il certificato):

- ***1.3.76.21.1.3.1*.1.1**
- ***1.3.76.21.1.5.1*.1.1**
- ***1.3.76.21.10.2.1*.2.1**

Per ulteriori approfondimenti sugli OID utilizzati dal QTSP, è disponibile il documento *CPS - Certification Practice Statement e CP - Certificate Policy per i Certificati Qualificati di Firma Elettronica e di Sigillo Elettronico*, pubblicato all'URL *https://www.intesa.it/e-trustcom/*.

F.4. Identità Elettroniche

F.4.1. SPID

Ai sensi dell'art. 24, comma 1, lett. b) del Reg. eIDAS, Il QTSP INTESA può ottemperare alla verifica dell'identità del richiedente un certificato qualificato attraverso un processo di autenticazione SPID con credenziali di livello 2 o 3.

In tale processo di autenticazione, sono richiesti almeno i seguenti dati minimi:

- Nome
- Cognome
- Sesso
- Luogo di nascita
- Data di nascita

- Codice fiscale.

Il certificato qualificato rilasciato tramite identità digitale SPID conterrà l'***OID 1.3.76.16.5***, registrato a cura dell'Agenzia con la seguente descrizione: "*Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity*";

Eventuali certificati qualificati emessi a seguito di una richiesta sottoscritta con firma elettronica qualificata basata su tali certificati qualificati devono, a loro volta, contenente il suddetto OID.

F.4.2. Identificazione tramite CIE (Carta di Identità Elettronica)

Ai sensi dell'art. 24, comma 1, lett. b) del Reg. eIDAS, Il QTSP INTESA può ottemperare alla verifica dell'identità del richiedente un certificato qualificato attraverso un processo di autenticazione CIE.

In questo caso il Richiedente, previo inserimento del PIN, effettua l'autenticazione sul portale del Certificatore o del CIE ID Server. Il sistema, dopo aver completato l'autenticazione, verifica le informazioni anagrafiche inserite nel certificato digitale e le associa a quelle relative al certificato di sottoscrizione oggetto di richiesta.

F.5. Identificazione tramite credenziali utilizzate per l'emissione di un precedente certificato one-shot

In questa modalità, il Certificatore si basa sull'identificazione già effettuata durante l'emissione di un precedente certificato one-shot.

Possono essere individuati due tipi di casistiche:

a) Il certificato one-shot, rilasciato mediante le credenziali di un precedente certificato one-shot, viene emesso nell'ambito della stessa sessione o processo di firma in cui è stato rilasciato il precedente certificato one-shot.

b) Il certificato one shot, rilasciato mediante le credenziali di un precedente certificato one-shot, viene emesso in una differente sessione o processo di firma.

Nel caso a): il Richiedente, in possesso dell'e-mail e del numero di cellulare certificati dal Certificatore nel corso del rilascio del precedente certificato one shot, può richiedere il rilascio del nuovo certificato one-shot solo dopo aver ricevuto, sull'e-mail e sul cellulare certificati, i nuovi codici One-Time, che dovranno essere verificati dal Richiedente per l'emissione e per l'utilizzo del nuovo certificato, purché ciò avvenga all'interno della stessa sessione o processo di firma.

Nel caso b): il Richiedente, già in possesso di credenziali fornite dal Certificatore o dalla LRA, si autentica al portale del Certificatore o della LRA e chiede l'emissione di un nuovo certificato one-shot, previa la conferma o l'aggiornamento dei dati di registrazione. E-mail e cellulare precedentemente certificati non potranno essere variati. In questo caso, per il rilascio e l'utilizzo del certificato è necessario che il Titolare inserisca la One-Time-Password inviata al suo dispositivo OTP, ovvero OTP/SMS su cellulare, e che sia data l'autorizzazione a procedere dalla LRA o dal Terzo Interessato.

In entrambi i casi, la gestione del sistema di autenticazione OTP è sotto il controllo della CA.

Qualora il Certificatore, durante il processo di emissione del precedente certificato one-shot, abbia certificato il possesso di strumenti di *Strong Customer Authentication* (*SCA*) riconducibili allo specifico Richiedente, tali credenziali SCA potranno essere utilizzate in luogo dei codici One-Time inviati su e-mail e cellulare nel *caso a)*, ovvero dell'accesso all'area riservata e invio di OTP/SMS nel *caso b)*.

G. Generazione delle chiavi di Certificazione, di Validazione Temporale e di sottoscrizione

G.1. Generazione delle chiavi di certificazione

La generazione delle chiavi all'interno dei dispositivi di firma avviene in presenza del Responsabile di Certificazione, come previsto dal DPCM all'Art.7

La suddetta operazione è preceduta dall'inizializzazione dei dispositivi di firma per il sistema di generazione dei certificati con i quali si firmano i certificati dei Titolari e quelli del sistema di validazione temporale.

Il tutto avviene in modalità dual control ad evitare operazioni illecite.

Le operazioni successive alla generazione delle coppie di chiavi di certificazione sono possibili solamente attraverso particolari dispositivi di autorizzazione (token usb): l'accesso privilegiato agli HSM è eseguibile soltanto attraverso le chiavi contenute in tali dispositivi di autorizzazione di cui sopra. Per maggior sicurezza, tali chiavi sono divise su più dispositivi, secondo una logica del tipo "*n di m*", in modo che solo la concomitante presenza di almeno *n* di *m* parti della chiave permettano di operare con gli opportuni privilegi. Pertanto, esse vengono custodite in apposite casseforti distinte.

La lunghezza delle chiavi di certificazione è conforme alla normativa tempo per tempo vigente.

G.2. Generazione delle chiavi del sistema di validazione temporale

La generazione delle chiavi di validazione temporale avviene in conformità a quanto stabilito dall'Art.49 del DPCM.

La lunghezza delle chiavi di certificazione è conforme alla normativa tempo per tempo vigente.

G.3. Generazione delle chiavi di sottoscrizione

Completata la fase di registrazione, durante la quale i dati dei Titolari vengono memorizzati negli archivi del Certificatore, è possibile procedere alla generazione delle chiavi di sottoscrizione.

Il Titolare potrà avviare la procedura di generazione delle chiavi e richiesta del Certificato di firma ad esse associato in una delle modalità descritte al par. *I. Modalità operative per la sottoscrizione di documenti*.

Le coppie di chiavi di sottoscrizione sono create su dispositivi di firma sicuri (*HSM – Hardware Security Module*), conformi alle specifiche di cui all'*Allegato II* del Reg. eIDAS.

La lunghezza delle chiavi di certificazione è conforme alla normativa tempo per tempo vigente.

H. Modalità di emissione dei certificati

H.1. Procedura di emissione dei Certificati di certificazione

In seguito alla generazione delle chiavi di certificazione, descritta nel par. *G.1*, sono generati i certificati delle chiavi pubbliche, conformemente con quanto disposto dal DPCM, firmati con le rispettive chiavi private e registrati nel registro dei certificati secondo le modalità previste.

I certificati delle chiavi di certificazione sono inviati all'Agenzia per l'Italia Digitale attraverso il sistema di comunicazione di cui all'Art.12, comma 1, del DPCM.

Il Certificatore genera un certificato qualificato per ciascuna delle chiavi di firma elettronica qualificata utilizzate dall'Agenzia per la sottoscrizione dell'elenco pubblico dei certificatori e lo pubblica nel proprio registro dei certificati. Il Certificatore deve poi mantenere copia della lista, sottoscritta dal dipartimento, dei certificati relativi alle chiave di certificazione e lo rende disponibile per via telematica (DPCM, Art.42, commi 1 e 3).

H.2. Procedura di emissione dei Certificati di sottoscrizione

Il QTSP INTESA emette certificati con un sistema conforme con l'Art.33 del DPCM.

Dopo la generazione della coppia di chiavi di sottoscrizione, descritta nel par. *G.3*, è generata una richiesta di nuovo certificato nel formato *PKCS#10*, che fornisce automaticamente la prova di possesso della chiave privata e la verifica del corretto funzionamento della coppia di chiavi.

Generate le chiavi, la richiesta di certificato sarà immediatamente inviata alla Certification Authority del QTSP.

La generazione dei certificati è registrata nel giornale di controllo (DPCM, Art.18, comma 4).

H.3. Informazioni contenute nei certificati di sottoscrizione

I certificati del QTSP INTESA, emessi nell'ambito del presente manuale, sono certificati qualificati ai sensi del Regolamento (UE) 910/2014 (eIDAS) e, pertanto, ne è garantita la loro interoperabilità e riconoscimento a livello comunitario.

Il Certificato Qualificato definisce con certezza il Certificatore che lo ha emesso e contiene i dati necessari per la verifica della Firma Digitale.

Ogni Certificato Qualificato per la firma elettronica è conforme al Regolamento eIDAS e segue le indicazioni presenti nella DETERMINAZIONE AgID N. 147/2019 (*Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati*).

Tutti i Certificati Qualificati emessi nell'ambito dei servizi descritti nel presente Manuale contengono almeno una limitazione d'uso (par. *F.1.1*, ovvero par. *F.3.1* per le tipologie di firma di cui al par. *F.3*).

H.3.1. Certificati con validità temporale limitata ("one shot")

Per alcuni processi, tipicamente legati all'onboarding di clienti prospect, il QTSP Intesa offre un servizio di firma elettronica qualificata remota, generata su HSM, conforme alla normativa, mediante l'utilizzo di un certificato qualificato a validità temporale limitata: massimo 30 minuti dall'emissione o come altrimenti concordato con la LRA / Terzo Interessato.

Tali certificati, oltre a prevedere dei forti vincoli in termini temporali, sono anche caratterizzati da vincoli applicativi che ne limitano l'adozione ai soli documenti proposti dalla LRA e da limiti d'uso (par. *F.1.1*) che ne circoscrivono la validità legale ai fini della sottoscrizione dei documenti sopracitati.

Per l'apposizione della firma in modalità remota tramite questi certificati, è possibile utilizzare applicazioni di tipo on-line e funzionanti mediante i servizi erogati dal Certificatore o dalla LRA. In quest'ultimo caso il Certificatore provvede ad assicurarsi che il sistema gestito dalla LRA garantisca la conoscenza esclusiva del dato per la creazione della firma da parte del Titolare grazie ad opportuni requisiti di sicurezza.

Il Certificatore mette a disposizione web services per permettere l'integrazione con le applicazioni richiedenti i servizi di firma. Si intende che i documenti oggetto di firma siano normalmente formati da dette applicazioni in dipendenza dalle specifiche necessità.

La richiesta di firma proveniente dall'utente, vista la breve durata dei certificati one shot, nonché i forti vincoli applicativi e d'uso, viene autenticata attraverso la componente delle credenziali nota al Titolare di tipo OTP/SMS.

H.4. Codice di Emergenza

Il Certificatore garantisce, in conformità con quanto previsto dall'Art.21 del DPCM, un *codice di emergenza* da utilizzarsi per richiedere la ***sospensione urgente*** del Certificato di sottoscrizione ancora in corso di validità.

Nelle applicazioni descritte dal presente Manuale Operativo, potrà essere considerato come codice di emergenza anche il PIN scelto dal Titolare all'atto della sua registrazione.

I. Modalità operative per la sottoscrizione di documenti

Il QTSP INTESA, attraverso i servizi di FCA Bank, rende disponibile ai Titolari quanto necessario a generare firme elettroniche qualificate conformemente a quanto previsto dalla normativa vigente.

La particolare tipologia di servizio non richiede la fornitura di un'applicazione di firma da installare sul proprio personal computer, ma piuttosto delle funzionalità di firma richiamabili o accedendo all'area riservata del portale di FCA Bank, oppure direttamente allo sportello di una filiale/dealer di FCA Bank.

Le firme elettroniche qualificate ottenibili attraverso queste procedure saranno assolutamente conformi a quanto previsto dal DPCM all'Art.4 comma 2 relativamente agli algoritmi utilizzati.

Tali documenti, inoltre, come richiesto dall'Art.4 comma 3 dello stesso DPCM, non conterranno macroistruzioni o codici eseguibili, tali ad attivare funzionalità che possano, all'insaputa del sottoscrittore, modificare atti, fatti e dati nei documenti stessi rappresentati.

Vengono di seguito descritte le modalità di autenticazione diverse che, nel rispetto della normativa vigente, permettono ad un Titolare, una volta registrato, di procedere all'apposizione di firme elettroniche qualificate.

A completamento e a conferma dell'effettuazione delle operazioni di firma saranno inviati SMS. Qualora il Titolare disponga di uno smartphone abilitato alla lettura della corrispondenza, su richiesta del Titolare stesso, in alternativa, potranno essere inviati e-mail in luogo degli SMS.

I.1. Processo di Firma in stazioni non presidiate (Home banking)

Dopo aver correttamente espletato l'identificazione certa secondo le procedure descritte nel presente Manuale Operativo ed aver registrato i propri dati identificativi e di contatto (e-mail e cellulare), il Titolare può, in un momento successivo, richiedere il proprio certificato digitale e procedere poi alla firma di un documento secondo le modalità di seguito descritte.

Tale procedura è al momento applicabile solo ai certificati one-shot.

Nel seguito è descritto l'elenco degli step che vengono eseguiti per l'apposizione della firma:

1. Il Titolare riceve un'e-mail all'indirizzo di posta registrato al momento della identificazione.
   L'email contiene un'invitation (URL) che redirige l'utente all'interno di un portale in cui viene mostrato il set di documenti costituenti una specifica pratica/dossier che devono essere visionati, prima di poter procedere alla sottoscrizione degli stessi.
2. Il portale sopracitato, prima consentire l'accesso, e quindi la visualizzazione del contenuto del/i documento/i costituenti il dossier, richiede all'utente di inserire un proprio National Identification Number (es. codice fiscale o altro dato identificativo univoco del titolare rilasciato dallo Stato di appartenenza) il numero di cellulare registrato al momento dell'identificazione.
3. L'utente, una volta inserite e verificate correttamente le informazioni sopraindicate, accede ad una pagina che gli consente di vedere il contenuto del/i documento/i, navigarlo/i, e avere piena contezza di tutti i punti in cui è richiesta la propria firma.
4. Una volta che l'utente, preso atto del contenuto del/i documento/i, attiva la funzione di firma, viene inviato un OTP/SMS al numero registrato in fase di identificazione.
   Solo quando l'utente avrà inserito il codice OTP all'interno della maschera mostrata dal portale, il processo di firma procederà alla generazione di un certificato qualificato one-shot di firma automatica, caratterizzato da una durata temporale molto limitata (par. *H.3.1*), che verrà utilizzato per apporre la firma elettronica qualificata esclusivamente sul set di documenti precedentemente visionati e approvati dall'utente nelle maschere di cui al punto 3.

Qualora le pratiche/dossier da firmare fossero più di una, il Titolare deve reiterare i passi da 1 a 4 per ogni pratica/dossier.

I.2. Processo di Firma in stazioni presidiate (Sportello Dealer FCA Bank gruppo Bancario)

Il Titolare può procedere alla sottoscrizione di un documento anche presso uno sportello di un Dealer delle società appartenenti al gruppo bancario FCA Bank.

Tale caso d'uso è applicabile esclusivamente ai one-shot.

Nel seguito è descritto l'elenco degli step che vengono eseguiti per l'apposizione della firma:

1. L'utente si presenta allo sportello di una filiale FCA Bank (stazione presidiata) e viene riconosciuto secondo quanto previsto dalla normativa bancaria antiriciclaggio, da un operatore addetto all'espletamento della verifica dell'identità ai sensi dell'AML.
2. Completata l'identificazione certa ai sensi dell'AML, l'operatore, dopo aver chiesto conferma e registrato i dati identificativi del Titolare, nonché i dati di contatto, predispone e fa visualizzare al Titolare la pratica/dossier contenente il set di documenti da firmare; tale visualizzazione avviene all'interno dei dispositivi utilizzati dall'intermediario per l'espletamento delle attività afferenti alle procedure AML. Trattandosi di dispositivi normalmente adottati per l'accesso a procedure che consentono di espletare le prassi previste per l'AML, tali device garantiscono alti standard di sicurezza.
3. Il Titolare prende visione del contenuto dei documenti da firmare e fornisce il proprio consenso per procedere alla sottoscrizione. Il consenso viene esplicitato cliccando o tappando i singoli punti firma
4. Recepito il consenso del Titolare, l'operatore attiva la funzione di invio OTP/SMS sul numero di cellulare registrato in fase di identificazione (step 1 e 2).
5. Il Titolare riceve l'OTP sul proprio cellulare e quindi lo inserisce nella maschera visualizzata dalla pagina su cui, pochi istanti prima, aveva preso visione dei documenti da firmare e palesato il consenso a procedere (step 3).

6. Dopo l'inserimento dell'OTP (e la corretta verifica dello stesso) il processo di firma procederà alla generazione di un certificato qualificato one-shot di firma automatica, caratterizzato da una durata temporale molto limitata (par. *H.3.1*), che verrà utilizzato per apporre la firma elettronica qualificata esclusivamente sul set di documenti precedentemente visionati ed approvati dall'utente nelle maschere di cui allo step 3.
7. Qualora le pratiche/dossier da firmare fossero più di uno, il Titolare e l'Operatore devono reiterare i passi da 2 a 6 per ogni pratica/dossier.

I.3. Autenticazione di tipo OTP/SMS

Questa modalità di autenticazione richiede all'utente, già precedentemente identificato, di utilizzare il proprio telefono cellulare (stesso numero fornito e registrato in fase di identificazione) per poter ricevere dal QTSP un codice monouso (OTP).

Tale OTP dovrà essere inserito nell'applicazione di firma al fine di confermare la propria identità e volontà a firmare lo specifico documento.

Al ricevimento del suddetto OTP, ne viene verificata la correttezza e, in caso di esito positivo, viene autorizzata l'operazione di firma elettronica qualificata.

Pertanto, quando il Titolare vorrà firmare un documento accedendo tramite il portale di firma messo a disposizione dalla Banca, nel caso di certificato triennale, utilizzerà un'autenticazione a due fattori attraverso l'inserimento di un PIN (informazione che solo l'utente conosce) e un OTP ricevuto via SMS sul numero di telefono che solo l'utente possiede.

J. Modalità operative per la verifica della firma

I documenti sottoscritti con le modalità descritte in precedenza saranno esclusivamente in formato PDF: tale formato di sottoscrizione è considerato infatti di facile utilizzo nell'ambito delle applicazioni bancarie o finanziarie.

La verifica dei documenti sottoscritti potrà essere agevolmente effettuata utilizzando il software *Acrobat Reader DC*, applicazione in grado di verificare tutte le tipologie di firma elettronica qualificata in formato PDF prodotte nell'Unione Europea in conformità con il Regolamento eIDAS.

Acrobat Reader DC è scaricabile gratuitamente dal sito di Adobe, *www.adobe.com/it/.*

K. Modalità di revoca e sospensione dei certificati

In conformità al Reg. eIDAS, le informazioni sullo stato del certificato sono disponibili via protocollo OCSP, all'URL indicato sul certificato stesso.

La revoca e la sospensione dei certificati possono essere asseverate anche dal loro inserimento nella lista CRL (Art.22 del DPCM). Il profilo delle CRL è conforme con lo standard RFC 5280. Tale lista, firmata dalla Certification Authority emittente il certificato, viene aggiornata con periodicità prestabilita e conforme alla normativa vigente.

La lista CRL è disponibile anche sul registro dei certificati.

Nei casi in cui la revoca ovvero la sospensione avvengano su iniziativa del Certificatore o del Terzo Interessato (artt. 23, 25, 27 e 29 del DPCM), il Certificatore notifica al Titolare la richiesta e il momento in cui entrerà in vigore l'evento richiesto.

In fase di richiesta, saranno specificate la data e l'ora a partire dalla quale il certificato risulterà revocato (Art.24, comma 1, DPCM).

K.1. Revoca dei certificati

Un certificato in corso di validità può essere revocato su richiesta del Titolare, del Terzo Interessato o della Certification Authority (cioè il QTSP).

Il certificato revocato non può essere in alcun modo riattivato.

K.1.1. Revoca su richiesta del Titolare

Il Titolare può richiedere la revoca accedendo ad una specifica sezione resa disponibile nell'ambito dei servizi di FCA Bank oppure mettendosi in contatto diretto con il Servizio Clienti FCA Bank.

Il QTSP, avvertito da FCA Bank, che nel frattempo avrà anche bloccato i codici di accesso del Titolare, provvederà alla immediata revoca del certificato.

K.1.2. Revoca su richiesta del Terzo Interessato

Nei casi in cui FCA Bank si configura come Terzo Interessato può richiedere la revoca del certificato.

Il QTSP, accertata la correttezza della richiesta, darà notizia della revoca ai Titolari interessati utilizzando i canali di comunicazione definiti con il Titolare all'atto della registrazione o successivamente aggiornati e comunicati dal Titolare al QTSP, anche per mezzo di FCA Bank (par. *C.2. Obblighi del Titolare*).

K.1.3. Revoca su iniziativa del Certificatore

Il Certificatore che intende revocare il Certificato Qualificato, salvo casi di motivata urgenza, ne dà preventiva comunicazione via e-mail o PEC a FCA Bank (casi Terzo interessato) e contemporaneamente sarà data comunicazione al Titolare utilizzando l'indirizzo e-mail fornito in fase di richiesta del certificato ovvero all'indirizzo di residenza, specificando i motivi della revoca nonché la data e l'ora a partire dalla quale la revoca è efficace.

K.1.4. Revoca dei certificati relativi a chiavi di certificazione

Nei casi di:

- compromissione della chiave di certificazione,
- cessazione dell'attività,

il Certificatore procede con la revoca dei certificati di certificazione corrispondenti e dei certificati di sottoscrizione firmati con la stessa chiave di certificazione.

Entro 24 ore, il Certificatore notificherà la revoca all'Agenzia per l'Italia digitale e ai Titolari.

K.2. Sospensione dei certificati

Sulle modalità di sospensione e di notifica della medesima vale quanto detto per le modalità di revoca al precedente par. *K.1*.

La sospensione di un certificato è prevista nel caso in cui si debba fare un supplemento di indagine per verificare se debba effettivamente essere revocato (ad esempio nei casi in cui si tema lo smarrimento / furto del Token OTP, o si debbano fare riscontri per avere certezza dell'effettiva cessazione del Titolare dalla mansione per la quale gli era stato emesso il certificato, ecc.).

La richiesta di sospensione può essere avanzata da tutte le entità previste dal DPCM agli Artt. 27, 28 e 29 (Certificatore, Titolare, Terzo Interessato).

In assenza di comunicazioni da parte del Titolare, il certificato verrà automaticamente revocato dopo un periodo di sospensione di 90 (novanta) giorni o comunque entro la data di scadenza del certificato stesso.

La data di decorrenza della revoca coinciderà, in ogni caso, con la data di decorrenza della sospensione.

La sospensione dei certificati è applicabile solo ai certificati in corso di validità.

K.2.1. Sospensione su richiesta del Titolare

Il Titolare può richiedere la sospensione accedendo ad una specifica sezione resa disponibile nell'ambito dei servizi di FCA Bank oppure mettendosi in contatto diretto con il Servizio Clienti FCA Bank.

Il Certificatore procede alla sospensione che verrà comunicata al Titolare utilizzando specifiche funzioni rese disponibili all'interno dei servizi o portali di FCA Bank.

Il Titolare successivamente potrà richiedere il ripristino del certificato secondo le modalità rese disponibili sempre da FCA Bank.

In assenza di comunicazioni ulteriori, il certificato sospeso sarà automaticamente revocato al termine del periodo di sospensione e la data di revoca coinciderà con la data di decorrenza della sospensione.

K.2.2. Sospensione su richiesta del Terzo Interessato

Nei casi in cui FCA Bank si configura come Terzo Interessato può richiedere la sospensione del certificato.

Il QTSP, accertata la correttezza della richiesta, sospenderà tempestivamente il certificato e ne darà notizia della sospensione ai Titolari interessati utilizzando i canali di comunicazione definiti con il Titolare all'atto della registrazione o successivamente aggiornati e comunicati dal Titolare al QTSP, anche per mezzo di FCA Bank (par. *C.2. Obblighi del Titolare*).

K.2.3. Sospensione su iniziativa del Certificatore

Il Certificatore, salvo i casi di motivata urgenza, potrà sospendere il certificato dandone preventiva comunicazione al Titolare all'indirizzo e-mail fornito in fase di richiesta del certificato, comunicato in fase di registrazione, ovvero all'indirizzo di residenza, specificando i motivi della sospensione e data e ora a partire dalle quali tale sospensione sarà efficace.

Nel caso in cui il certificato preveda il Terzo Interessato, una comunicazione analoga verrà inviata anche a quest'ultimo da parte del Certificatore.

L. Modalità di sostituzione delle chiavi

L.1. Sostituzione dei certificati qualificati e delle chiavi del Titolare

I certificati qualificati di firma elettronica emessi dal Certificatore nell'ambito dei contesti descritti nel presente Manuale Operativo sono di due tipologie:

a) ***Long term***: durata di 36 (trentasei) mesi dall'emissione
b) ***One shot***: durata limitata a massimo 30 (trenta) minuti dall'emissione o come altrimenti concordato con la LRA / Terzo Interessato

Al termine dei sopracitati periodi, nel caso si intenda procedere con il rinnovo del certificato, si renderà necessaria la generazione di una nuova coppia di chiavi di sottoscrizione e contestualmente l'emissione di un nuovo certificato.

In questo caso la procedura seguita per l'emissione del nuovo certificato sarà simile a quella indicata in fase di primo rilascio, al netto della fase di identificazione del Titolare che non dovrà essere ripetuta se la procedura è effettuata prima della scadenza del certificato.

L.2. Sostituzione delle chiavi del Certificatore

L.2.1. Sostituzione in emergenza delle chiavi di certificazione

Il procedimento utilizzato in caso di guasto del dispositivo di firma (HSM) contenente le chiavi di certificazione (CA e TSCA) o di disastro presso la sede centrale è trattato al par. *P. Procedura di gestione degli eventi catastrofici*.

L.2.2. Sostituzione pianificata delle chiavi di certificazione

Con un periodo di tempo congruo alla normativa vigente, prima della scadenza del certificato relativo alle coppie di Chiavi di certificazione (CA e TSCA), utilizzate dai sistemi di emissione dei certificati di sottoscrizione e dei certificati di TSA, il Certificatore procederà in base a quanto stabilito dall'Art.30 del DPCM.

L.2.3. Sostituzione delle chiavi del sistema di validazione temporale (TSA)

Per quanto riguarda la sostituzione delle chiavi del sistema di validazione temporale sono applicate le medesime indicazioni contenute nell'analoga sezione del *Manuale Operativo Intesa* pubblicato sul portale del QTSP: *https://www.intesa.it/manuali-operativi-e-trustcom/*.

M. Registro dei certificati

M.1. Modalità di gestione del Registro dei certificati

Nel registro dei certificati, INTESA pubblica:

- I certificati delle chiavi di sottoscrizione e del sistema di validazione temporale.

- I certificati delle chiavi di certificazione (CA e TSCA).
- I certificati emessi a seguito della sostituzione delle chiavi di certificazione.
- Certificati per le chiavi di firma dell'Agenzia per l'Italia Digitale (DPCM Art.42, comma 1).
- Le liste di revoca e sospensione (CRL).

Le operazioni che coinvolgono il registro dei certificati vengono svolte soltanto dalle persone a ciò autorizzate, presenti in quantità adeguata a impedire azioni illecite da parte di un limitato numero di addetti.

Il Certificatore mantiene una copia di riferimento del registro dei certificati inaccessibile dall'esterno; questa aggiorna in tempo reale la copia operativa, accessibile da parte degli utenti con protocollo LDAP.

La verifica di rispondenza tra copia di riferimento e copia operativa è fatta sistematicamente.

M.2. Accesso logico al Registro dei certificati

La copia di riferimento è collocata all'interno di una rete dedicata protetta da adeguati dispositivi, per cui non è accessibile ad altri che dal server di emissione dei certificati, che vi registra i certificati emessi e le CRL.

L'accesso sulle copie operative è possibile all'indirizzo *ldap://x500.e-trustcom.intesa.it* con protocollo LDAP.

Il Certificatore consente anche l'accesso alle CRL attraverso il protocollo http, all'URL indicato nel campo CDP (CRL Distribution Point) del certificato.

M.3. Accesso fisico ai locali dei sistemi preposti al registro dei certificati

Gli addetti abilitati alla gestione diretta del registro dei certificati possono accedere al locale ove il sistema è installato e operarvi solo se in modalità dual control ad evitare azioni illecite.

Gli addetti alla gestione dei sistemi, alla gestione della rete, alla manutenzione, ecc., possono accedere al locale ove il sistema è installato e, per gli addetti specifici, operarvi solo in presenza di addetti abilitati alla gestione del registro dei certificati secondo le modalità precedentemente esplicitate per gli operatori abilitati.

N. Modalità di protezione dei dati personali

Le misure di sicurezza per la protezione dei dati personali sono conformi alle misure previste dal Regolamento Europeo 679/2016 (GDPR) e successive modificazioni e integrazioni.

O. Procedura di gestione delle copie di sicurezza

Gli archivi informatici che sono oggetto di copie di sicurezza sono i seguenti:

- REGISTRO DEI CERTIFICATI, archivio digitale contenente quanto specificato al par. *M*.
- INFORMAZIONI OPERATIVE, archivio digitale in cui sono memorizzate tutte le informazioni ricevute dal Titolare al momento della registrazione e della richiesta di un certificato nonché le richieste di revoca e sospensione, corredate delle relative documentazioni.
- GIORNALE DI CONTROLLO, archivio costituito dall'insieme delle registrazioni effettuate automaticamente dai sistemi installati presso il servizio di certificazione del QTSP (Art.36 del DPCM).
- ARCHIVIO DIGITALE DELLE MARCHE TEMPORALI, contiene le marche temporali generate dal sistema di validazione temporale (Art.53, comma 1, del DPCM).
- REGISTRO OPERATIVO DEGLI EVENTI DI VALIDAZIONE TEMPORALE, registro sul quale sono automaticamente memorizzati gli eventi attinenti le attività di validazione temporale per i quali è prevista la registrazione di qualunque anomalia o tentativo di manomissione che possa pregiudicare il funzionamento del sistema di validazione temporale (Art.52 del DPCM).

La conservazione, per tutte le copie di sicurezza descritte, è conforme a quanto previsto dalle normative vigenti in materia.

P. Procedura di gestione degli eventi catastrofici

Il QTSP INTESA è dotato di un piano di emergenza per la gestione degli eventi catastrofici che prevede le seguenti fasi:

- *gestione dell'emergenza*: in questa fase è garantita la continuità di accesso alle CRL; la loro emissione può subire ritardi derivanti dalla necessità di attivare il server di backup della CA, situato nel sito di back up;
- *gestione del transitorio*: in questo periodo è assicurata l'emissione dei certificati e il ripristino di ulteriori soluzioni di *disaster recovery*;
- *ritorno dell'esercizio a regime*: nel medesimo sito originale o in un altro alternativo, ma definitivo.

Va premesso che la presenza di repliche della copia operativa del registro dei certificati distribuite in più punti consente comunque, in caso di interruzione di funzionamento di una delle sedi, di accedere al contenuto del registro dei certificati aggiornato fino al momento dell'interruzione.

Per poter fare fronte alla gestione dell'emergenza è prevista la replica nel sito di backup del registro dei certificati, dei dati del sistema di emissione dei certificati e l'intervento entro 24 ore di personale atto ad attivare la funzionalità di emissione delle CRL. Di detto personale è curato l'addestramento, oltre che alla gestione del SW e HW, anche della situazione di emergenza.

Q. Modalità per l'apposizione e la definizione del riferimento temporale

Per quanto riguarda le modalità di apposizione e la definizione del riferimento temporale, si applicano le stesse indicazioni contenute nel *Manuale Operativo Intesa* pubblicato sul portale del QTSP al seguente URL: https://www.intesa.it/manuali-operativi-e-trustcom/.

Q.1. Modalità di richiesta e verifica marche temporali

Il Certificatore appone una marca temporale (*validazione temporale elettronica qualificata*, ai sensi del Reg. eIDAS) su tutti i documenti sottoscritti dal Titolare nell'ambito dei servizi descritti da questo Manuale Operativo.

Salvo i casi previsti al par. *F.3*, l'apposizione di detta marca è un processo integrato con l'operazione di firma e non richiede nessuna attività specifica da parte del Titolare.

La verifica della marca temporale apposta è contestuale alla verifica della firma.

R. Lead Time e Tabella Raci per il rilascio dei certificati

Di seguito si riporta la Tabella relativa al "Lead Time di Processo" per la gestione delle richieste di Emissione, Revoca, Sospensione e Riattivazione dei Certificati.

Soggetto	Richiesta	Ente Coinvolto	Azione Ente Coinvolto	Ente Coinvolto	Azione Ente Coinvolto
Utente, Richiedente, Titolare Certificato	*Richiesta di Emissione del Certificato vs. LRA*	*FCA Bank (acting as) Local RA*	*Emette ordine di pubblicazione del Certificato vs CA previa verifica identità*	*Certification Authority*	*Evasione Richiesta di Certificazione*
Utente, Richiedente, Titolare Certificato	*Richiesta di Revoca / Sospensione del Certificato vs. RA o LRA*	*Intesa (acting as) Registration Authority (RA) o FCA Bank (acting as LRA)*	*Emette ordine di Revoca / Sospensione del Certificato vs CA previa verifica identità*	*Certification Authority*	*Evasione Richiesta di Revoca / Sospensione*
Utente, Richiedente, Titolare Certificato	*Richiesta di Riattivazione del Certificato vs. RA o LRA*	*Intesa (acting as) Registration Authority (RA) o FCA Bank (acting as LRA)*	*Emette ordine di riattivazione del Certificato vs CA previa verifica identità*	*Certification Authority*	*Evasione Richiesta di Riattivazione*

Di seguito si riporta la Tabella RACI relativa alla individuazione delle responsabilità degli enti coinvolti nelle richieste di Emissione, Revoca, Sospensione e Riattivazione dei Certificati.

Soggetto Coinvolto	Responsible	Accountable	Consulted	Informed
Registration Authority	***X***			
Local Registration Authority	***X***			
Certification Authority		***X***		
Utente, Richiedente, Titolare del Certificato			***X***	***X***

S. Riferimenti Tecnici

ETSI-319.401	ETSI EN 319 401 v2.3.1 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI-319.411-1	ETSI EN 319 411-1 V1.3.1 - 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 V2.3.1 - 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-319.412-1	ETSI EN 319 412-1 V1.4.4 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
ETSI-319.412-2	ETSI EN 319 412-2 V2.2.1 - 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 V2.3.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
Rec ITU-R	Recommendation ITU-R TF.460-6, Annex 1 – Time Scales.
RFC5905	Network Time Protocol (Protocollo 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

------- FINE DEL DOCUMENTO -------