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

Qualified Trust Service Provider

ai sensi del Regolamento (UE) N. 910/2014 (eIDAS)

Manuale Operativo del QTSP In.Te.S.A. S.p.A.

per la procedura di Firma Digitale nell'ambito dei Servizi di Internet Banking ovvero altre Soluzioni che prevedano modalità di sottoscrizione elettronica di documenti informatici, offerti da UniCredit o altre Società del Gruppo Bancario, con riferimento all'attività in sede, fuori sede e mediante tecniche di comunicazione a distanza di UniCredit S.p.A. (e di altre Società del Gruppo)

Codice documento: MOU_UC

OID: 1.3.76.21.1.3.1.150

Redazione: Antonio Raia

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

Data emissione: 30/03/2022

Versione: 11

Firmato da:
ANTONIO RAIA
Organizzazione: IN.TE.S.A. S.p.A.

Revisioni

Versione n. 01		Data emissione: 19/07/2010
Descrizione modifiche:	Nessuna	
Motivazioni:	Prima emissione	
Versione n. 02		Data emissione: 01/11/2010
Descrizione modifiche:	Riorganizzazione societaria a seguito di fusione per incorporazione di UniCredit Banca S.p.A., UniCredit Banca di Roma S.p.A., Banco di Sicilia S.p.A., UniCredit Corporate Banking S.p.A., UniCredit Private Banking S.p.A., UniCredit Family Financing Bank S.p.A., UniCredit Bancassurance Management & Administration S.c.r.l. nella capogruppo UniCredit S.p.A. Conseguente variazione del Codice Documento da MOU-UCB a MOU-UC	
Motivazioni:	Aggiornamento	
Versione n. 03		Data emissione: 01/06/2012
Descrizione modifiche:	**A.1, D.2.3:** Introduzione di Firma grafometrica generata tramite tablet in Agenzia quali strumenti di autenticazione e autorizzazione alla generazione di firma digitale nell'ambito del Servizio di Banca Multicanale. **R.2:** Introduzione della modalità di firma in Agenzia tramite Tablet. **B.1**: Variazione dati anagrafici Certificatore. **B.3, H.1**: Variazione della limitazione d'uso. **D.2.2:** Introduzione di Mobile Token e Password Card quali strumenti di autenticazione e autorizzazione alla generazione di firma digitale nell'ambito del Servizio di Banca Multicanale. **I.2, J.2**: Introduzione della richiesta di Revoca o Sospensione in Agenzia. **P.2:** Aggiornamento denominazione del fornitore del riferimento temporale.	
Motivazioni:	Aggiornamento	
Versione n. 04		Data emissione: 09/10/2015
Descrizione modifiche:	**0**: Aggiornamento riferimenti normativi **B.1**: Variazione dati identificativi del Certificatore **R.3**: Firma grafometrica generata tramite tablet anche nell'ambito dell'attività fuori sede effettuata dai Promotori Finanziari di Unicredit **R.4**: Grafico flusso procedurale (protezione dei dati biometrici)	
Motivazioni:	Variazione sede legale del Certificatore Aggiornamenti	
Versione n. 05		Data emissione: 13/08/2016
Descrizione modifiche:	Introdotto riferimento ai servizi offerti dalle *Società del Gruppo Unicredit* **B.3, H.1**:Modificato il testo della Limitazione d'uso del Certificato Qualificato **R.3:** Aggiornamento descrizioni delle Modalità di Firma (servizi Internet Banking, attività in sede, attività fuori sede) Variazione riferimenti normativi – verifica conformità	
Motivazioni:	Aggiornamenti servizi Aggiornamenti normativi - Regolamento (UE) 910/2014 (eIDAS)	
Versione n. 06		Data emissione: 19/04/2017
Descrizione modifiche:	**D.2.3:** Ottimizzazione parametro di *Threshold* **0**: Aggiornamento riferimenti normativi	
Motivazioni:	Adeguamento valore di *Threshold* per ottimizzazione della gestione del multi-device Aggiornamento	
Versione n. 07		Data emissione: 03/06/2020
Descrizione modifiche:	**0**: Aggiornamenti **0**: Aggiornamenti **B.3**: Aggiornamento massimali assicurativi **F**: Aggiornamenti **G.3**: Aggiornamento tempistiche per la sostituzione delle chiavi di certificazione **Q.1.5**: Inserimento paragrafo Firma digitale con Notifica Push da App Mobile Banking **S**: Inserimento paragrafo Lead Time e Tabella Raci per il rilascio dei certificati **T**: aggiornamento riferimenti tecnici	
Motivazioni:	Aggiornamenti normativi e descrittivi Aggiornamento servizi	

Versione n. 08	Data emissione: 23/10/2020
Descrizione modifiche:	**Titolo:** aggiornamento **A**: modifica del titolo del MO **B.3, H.1:** Variazione della limitazione d'uso; inserito al B.1.3 riferimento a H.1.1 per la descrizione della limitazione d'uso **R.6**: Inserimento paragrafo Firma digitale in processi con tecniche di comunicazione a distanza che prevedano la presenza di operatore in remoto
Motivazioni:	Aggiornamento soluzioni di firma Aggiornamento servizi
Versione n. 09	Data emissione: 15/02/2021
Descrizione modifiche:	**D.2.4**: Inserimento paragrafo Identificazione del *Richiedente con un processo di onboarding implementato su sito pubblico/App*. **P.2**: Puntualizzazione sulla sincronizzazione dei server di validazione temporale
Motivazioni:	Aggiornamento servizi Aggiornamenti e correzione refusi
Versione n. 10	Data emissione: 31/12/2021
Descrizione modifiche:	Aggiornamento dati societari e logo del QTSP In.Te.S.A. S.p.A. **T**: Aggiornamento riferimenti normativi e tecnici
Motivazioni:	Variazione proprietà, direzione e coordinamento Aggiornamenti normativi
Versione n. 11	Data emissione: 30/03/2022
Descrizione modifiche:	**D.2.4**: Aggiornamento Paragrafo
Motivazioni:	Integrazione riconoscimento con CIE Unicredit e Buddy Bank Integrazione riconoscimento Selfie Unicredit.

Sommario

Introduzione

Definizioni

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*.
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).
QTSP	Qualified Trust Service Provider – Prestatore di Servizi Fiduciari Qualificati. Persona fisica o giuridica che presta uno o più servizi fiduciari qualificati. Già *Certificatore Accreditato*. 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 servizi qualificati di firma elettronica e di validazione temporale e altri servizi connessi con queste ultime.
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.
Firma Digitale	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.
HSM	Hardware Security Module, dispositivi per la creazione della firma digitale dedicati alla sicurezza crittografica e alla gestione delle chiavi, in grado di garantire un elevato livello di protezione.
Marca Temporale	Validazione Temporale Elettronica Qualificata: il Riferimento Temporale che consente la validazione temporale.
Registration Authority	Autorità di Registrazione: UniCredit S.p.A. che, su incarico del Certificatore, ha la responsabilità di registrare o verificare le informazioni (in particolare modo l'identità del Titolare) necessarie al Certificatore per emettere il Certificato Qualificato.
Registro dei Certificati	La combinazione di uno o più archivi informatici, tenuto dal Certificatore, contenente tutti i Certificati emessi.
Richiedente	Il Cliente di UniCredit S.p.A. o altro soggetto che può non essere cliente della Banca, ma comunque riconosciuto con i medesimi criteri., che richiede il Certificato.
Riferimento Temporale	Informazione contenente la data e l'ora, che viene associata ad uno o più documenti informatici.
Titolare	Il Cliente di UniCredit S.p.A., o soggetto autorizzato, cui il certificato digitale è rilasciato e che è autorizzato ad usarlo al fine di apporre la firma digitale.
TSA	Time Stamping Authority, autorità che rilascia le marche temporali.

Riferimenti Normativi

CAD	Decreto Legislativo n. 82 del 7 marzo 2005 (G.U. n. 112 del 16 maggio 2005), "*Codice dell'amministrazione Digitale*" e successive modificazioni e integrazioni.
DPR 445/00	Decreto del Presidente della Repubblica n. 445 del 28 dicembre 2000, "*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*" (G.U. n. 42 del 20 febbraio 2001) e successive modificazioni e integrazioni.
DPCM	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*". (G.U. n. 117 del 21 maggio 2013) e successive modificazioni e integrazioni.
Reg. eIDAS	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 e successive modificazioni e integrazioni.
DET. AGID 147/2019	Determinazione AgID N. 147/2019, "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." e successive modificazioni e integrazioni.
GDPR	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) e successive modificazioni e integrazioni.

A. Il Manuale Operativo

A.1. Il Manuale Operativo

Questo documento è il Manuale Operativo per la procedura di firma digitale del Prestatore di Servizi Fiduciari Qualificato In.Te.S.A. S.p.A. (di seguito anche solo QTSP, Certificatore o INTESA) per la procedura di Firma Digitale nell'ambito dei Servizi di Internet Banking ovvero altre soluzioni che prevedano modalità di sottoscrizione elettronica di documenti informatici, offerti da UniCredit o altre Società del Gruppo, con riferimento all'attività in sede, fuori sede o tramite tecniche di comunicazione a distanza di UniCredit (nonché, in presenza di specifici accordi tra UniCredit e società del Gruppo UniCredit che intrattengano a propria volta rapporti con In.Te.S.A. S.p.A.).

Il Manuale Operativo descrive le procedure e le relative regole utilizzate dal QTSP INTESA per l'emissione del Certificato Qualificato per la firma digitale per i Clienti di Unicredit (con utilizzo anche nei rapporti con altre Società del Gruppo, in presenza dei presupposti sopra indicati).

Le attività descritte sono svolte in conformità con il Regolamento (UE) 910/2014 (eIDAS).

Il processo prevede che il Titolare possa avviare la procedura di firma di documenti, disposizioni o contratti relativi a prodotti o servizi erogati ovvero offerti:

- nell'ambito dei Servizi di Internet Banking di UniCredit (intendendosi per tali anche i servizi ad accesso protetto che tempo per tempo siano resi disponibili comprensivi della funzionalità di sottoscrizione elettronica di documenti) ovvero altri processi che utilizzino tecniche di comunicazione a distanza, utilizzando, in combinazione a credenziali di accesso/espletamento di iter predefiniti di identificazione, la password "usa e getta" generata da dispositivi di strong authentication;
- nell'ambito dell'attività in sede di UniCredit (e di altre società del Gruppo), utilizzando la firma grafometrica acquisita tramite appositi Tablet o utilizzando (da sola o in combinazione ad un codice identificativo quale ad es. il Codice Personale del proprio servizio di Internet Banking) la password "usa e getta" generata da dispositivi di strong authentication (ad es. SMS token);
- nell'ambito dell'attività fuori sede svolta da UniCredit (e altre società del gruppo) avvalendosi delle tipologie di soggetti tempo per tempo normativamente legittimate per tale finalità, utilizzando la firma grafometrica acquisita tramite appositi Tablet o utilizzando (da sola o in combinazione ad un codice identificativo quale ad es. il Codice Personale del proprio servizio di Internet Banking) la password "usa e getta" generata da dispositivi di strong authentication (ad es. SMS token).

La firma digitale così descritta si realizza tramite una coppia di chiavi asimmetriche, una pubblica e una privata, che consente al Titolare di rendere manifesta l'autenticità e l'integrità di un documento informatico ad uno o più destinatari che ne possono verificare la validità.

L'art. 8 del DPCM stabilisce che un Certificatore Accreditato conservi le chiavi private dei Titolari, utilizzate per l'operazione di generazione della firma digitale, su particolari dispositivi sicuri, denominati Hardware Security Module (di seguito HSM), garantendo al contempo che esclusivamente il Titolare della chiave privata possa attivarne l'uso come specificato dall'art. 11 comma 2 del DPCM.

Il contenuto del Manuale Operativo è conforme a quanto stabilito dalle regole tecniche contenute nel DPCM, dagli artt. 26 e 29 del CAD e dal Reg. eIDAS.

Il Manuale Operativo è di proprietà di UniCredit S.p.A.

Per quanto non espressamente previsto nel presente manuale operativo, si fa riferimento alle norme tempo per tempo vigenti.

A.2. Dati identificativi del Manuale Operativo

Il presente documento costituisce la versione n. **11**, rilasciata il **30/03/2022**, del "*Manuale Operativo del QTSP In.Te.S.A. S.p.A. per la procedura di Firma Digitale nell'ambito dei Servizi di Internet Banking ovvero altre Soluzioni che prevedano modalità di sottoscrizione elettronica di documenti informatici, offerti da UniCredit o altre Società del Gruppo Bancario, con riferimento all'attività in sede, fuori sede e mediante tecniche di comunicazione a distanza di UniCredit S.p.A. (e di altre Società del Gruppo)*".

L'object identifier di questo documento è **1.3.76.21.1.3.1.150**.

Il Manuale Operativo è pubblicato:

- nell'ambito della sezione protetta del sito della Banca, *www.unicredit.it*;
- all'indirizzo Internet *https://e-trustcom.intesa.it/DOCS/mo_UniCredit.pdf*;
- all'indirizzo Internet dell'Agenzia per l'Italia Digitale, *www.agid.gov.it*.

A.3. Responsabilità del Manuale Operativo

La responsabilità del presente Manuale Operativo è del QTSP INTESA, che ne cura la stesura, la pubblicazione e l'aggiornamento in accordo e in collaborazione con Unicredit (nel seguito, anche solo *Banca*).

Ogni revisione del presente Manuale Operativo sarà sempre concordata con la Banca.

Le revisioni del Manuale Operativo saranno pubblicate nell'ambito dei siti indicati al precedente paragrafo.

A.4. Orari di disponibilità del Servizio

Il Servizio è disponibile:

- nell'ambito dell'attività fuori sede;
- 365 giorni l'anno, 24 ore su 24, nell'ambito dei servizi di Internet Banking;
- negli orari e nei giorni di apertura dei locali nei quali è svolta l'attività in sede ovvero con operatore da remoto di UniCredit S.p.A. (e di altre Società del Gruppo).

A.5. Tariffe

Il Servizio viene fornito da UniCredit ai propri Clienti senza oneri e non è pertanto soggetto a tariffazione.

B. Il Certificatore Accreditato (QTSP – Qualified Trust Service Provider)

B.1. Il QTSP INTESA

Il Servizio è erogato da INTESA che, operando in ottemperanza con quanto previsto dal DPCM, dal CAD e dal Reg. eIDAS, espleta le attività di Prestatore di Servizi Fiduciari Qualificato (nel seguito anche solo QTSP o Certificatore).

Tali attività prevedono l'emissione, la pubblicazione, la revoca e la sospensione di Certificati Qualificati per Firma Digitale.

I dati identificativi del Certificatore sono riportati nella tabella seguente:

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
Partita IVA	05262890014
Telefono	+39-011-192.16.111
Sito Internet	*www.intesa.it*
e-mail	*marketing@intesa.it*

Indirizzo (URL) registro dei certificati	*ldap://x500.e-trustcom.intesa.it*
ISO Object Identifier (OID)	1.3.76.21

B.2. Obblighi del Certificatore

Nello svolgimento della propria attività, il QTSP INTESA adotta tutte le misure organizzative e tecniche idonee ad evitare danno ad altri e opera in conformità con quanto disposto dal CAD e dal Reg. eIDAS.

In particolare, il Certificatore, in base a quanto stabilito dagli artt. 30 e 32 del CAD:

- si attiene alle misure di sicurezza per il trattamento dei dati personali ai sensi del GDPR e riceve, tramite Unicredit, previo esplicito consenso del Richiedente e/o del Titolare, i dati necessari al rilascio e al mantenimento del Certificato Qualificato per la Firma Digitale;
- rilascia il Certificato Qualificato per la Firma Digitale secondo quanto stabilito dall'art. 32 del CAD;
- informa il Richiedente, in modo compiuto e chiaro, circa la procedura di certificazione, i necessari requisiti tecnici per accedervi, le caratteristiche e le limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
- assicura che il dispositivo sicuro per la generazione delle firme (HSM) presenti le caratteristiche e i requisiti di sicurezza di cui all'art. 35 del CAD e all'art. 11 del DPCM e dall'Art. 29 del Reg. eIDAS;
- procede, su istanza del Titolare o del Terzo Interessato, alla revoca e sospensione del Certificato Qualificato per la Firma Digitale e alla pubblicazione di tale revoca o sospensione;
- tiene registrazione, anche elettronica, di tutte le informazioni relative al Certificato Qualificato per la Firma Digitale per 20 (venti) anni in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
- non esporta le chiavi private di firma del soggetto, cui ha fornito il servizio di certificazione, dagli HSM in cui sono state generate e in cui vengono utilizzate per il servizio di firma;
- informa il Titolare di una coppia di chiavi dell'obbligo di mantenere in modo esclusivo la conoscenza delle informazioni di abilitazione all'uso della chiave privata;
- aggiorna Unicredit in merito a modifiche di carattere tecnico o normativo che possano influire sull'attività svolta dalla stessa nella sua veste di Registration Authority.

B.3. Limitazioni di Responsabilità del Certificatore

Il QTSP INTESA, fatti salvi i casi di colpa o dolo (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 del Terzo Interessato di quanto indicato nel presente Manuale Operativo e/o dalla mancata osservanza da parte degli stessi della normativa vigente.

Il QTSP INTESA non potrà essere ritenuto responsabile delle conseguenze dovute a cause ad esso non imputabili, quali, a titolo esemplificativo, ma non esaustivo: calamità naturali, disfunzioni tecniche e logistiche al di fuori del suo controllo, interventi dell'Autorità, rivolte o atti di guerra che colpiscano anche o solo i soggetti delle cui attività il Certificatore 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 in relazione alla limitazione d'uso specificata nel Certificato Qualificato stesso e definita al par. H.1.

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 inviata ad AgID apposita dichiarazione di stipula.

C. La Registration Authority

C.1. La Registration Authority - UniCredit

Il Certificatore ha rilasciato mandato a svolgere la funzione di Registration Authority a *UniCredit S.p.A. Sede Sociale e Direzione Generale: Piazza Gae Aulenti, 3 - Tower A - 20154 Milano - Capitale Sociale € 20.994.799.961,81, interamente versato - Iscrizione al Registro delle Imprese di Milano-Monza-Brianza-Lodi, Codice Fiscale e P. IVA n° 00348170101- Banca iscritta all'Albo delle Banche e Capogruppo del Gruppo Bancario UniCredit - Albo dei Gruppi Bancari: cod. 02008.1 - Cod. ABI 02008.1 - Aderente al Fondo Interbancario di Tutela dei Depositi*.

In particolare, la Banca svolge le seguenti attività:

- identificazione del Richiedente e/o del Titolare;
- registrazione del Richiedente.

C.2. Obblighi della Registration Authority

La Banca, nello svolgimento della sua funzione di Registration Authority, deve vigilare affinché l'attività di riconoscimento si svolga nel rispetto della normativa vigente. La RA deve inoltre segnalare senza indugio al QTSP INTESA ogni eventuale evento o incidente inerente violazioni della sicurezza o perdite di integrità dei dati che abbiano un impatto significativo sui servizi fiduciari oggetto del presente Manuale Operativo o sui dati personali dei titolari di certificato qualificato.

La documentazione relativa all'attività di cui sopra e necessaria all'emissione del Certificato Qualificato per la Firma Digitale al Titolare viene conservata dalla Banca, secondo gli obblighi di legge, per 20 (venti) anni dall'eventuale scioglimento di tale rapporto.

D. Il Titolare del Certificato

D.1. Il Titolare del Certificato

Il Richiedente è il Cliente di UniCredit o altro soggetto che può non essere cliente della Banca, ma comunque riconosciuto con i medesimi criteri, che richiede l'emissione del Certificato Qualificato per la Firma Digitale al fine di sottoscrivere documenti, disposizioni o contratti, relativi a prodotti e servizi, venduti attraverso i servizi di Internet Banking ovvero altre soluzioni che prevedano modalità di sottoscrizione elettronica di documenti informatici, offerti da UniCredit o altre Società del Gruppo, nelle Agenzie/locali della Banca o di altre Società del Gruppo ovvero mediante tecniche di comunicazione a distanza ovvero nell'ambito dell'attività fuori sede dei Promotori Finanziari / incaricati di UniCredit S.p.A. o di altre Società del Gruppo.

Il Titolare è il Cliente della Banca, o altro soggetto come sopra descritto:

- che abbia sottoscritto il contratto relativo, o che sia titolato ad operare con il Servizio di Internet Banking, a cui è rilasciato e affidato il Certificato Qualificato per la Firma Digitale e che è autorizzato ad utilizzarlo per sottoscrivere documenti, disposizioni o contratti relativi a prodotti o servizi offerti dalla Banca o da altre Società del Gruppo, nell'ambito del Servizio di Banca Multicanale ovvero altri servizi ad accesso protetto che tempo per tempo siano resi disponibili comprensivi della funzionalità di sottoscrizione elettronica di documenti offerti da UniCredit o altre Società del Gruppo stesso.
- a cui è rilasciato e affidato il Certificato Qualificato per la Firma Digitale e che è autorizzato ad utilizzarlo per sottoscrivere documenti, disposizioni o contratti relativi a prodotti o servizi offerti dalla Banca o da altre Società del Gruppo, nell'ambito di ulteriori processi di sottoscrizione elettronica che ne contemplino l'utilizzo, tempo per tempo previsti.

D.2. Identificazione del Richiedente

D.2.1. Identificazione del Richiedente alla presenza di un operatore

Il personale della Banca o di altre Società del Gruppo, in ottemperanza con quanto previsto dalla vigente normativa in materia di Antiriciclaggio e dalle normative interne alla Banca stessa e di altre società del Gruppo, svolge tutte le operazioni necessarie all'identificazione e registrazione del Richiedente.

In dettaglio, verifica l'identità del Richiedente tramite i documenti d'identità forniti e raccoglie i seguenti dati personali:

- nome e cognome;
- data di nascita;
- comune o stato estero di nascita;
- codice fiscale o codice identificativo univoco rilasciato da autorità Statali / Federali;
- indirizzo di residenza;
- indirizzo di corrispondenza;
- numero di telefono cellulare;
- indirizzo di posta elettronica;
- numero di telefono fisso (opzionale);
- numero di fax (opzionale);
- tipo e numero del documento d'identità esibito dal Richiedente;
- autorità che ha rilasciato il documento d'identità e luogo del rilascio.

D.2.2. Firma digitale in Servizi di Internet Banking e processi con tecniche di comunicazione a distanza

Nell'ambito di un Servizio di Internet Banking e processi in oggetto, il Titolare può utilizzare codici numerici monouso (di seguito, password) generati da strumenti di strong authentication quali ad esempio Unicredit Pass, OTP via SMS, Mobile Token e altri strumenti con analoghe caratteristiche.

La password generata dallo strumento di strong authentication potrà essere utilizzata, eventualmente unitamente al Codice di identificazione Personale (ad esempio in Banca Multicanale il PIN) del Servizio di Internet Banking, quale strumento di autenticazione per sottoscrivere digitalmente, nell'ambito del Servizio stesso, documenti, disposizioni o contratti relativi a prodotti o servizi erogati ovvero offerti da UniCredit o altre Società del Gruppo.

D.2.3. Firma digitale nell'ambito dell'attività in sede e nell'ambito dell'attività fuori sede

Le procedure di autenticazione sopra descritte sono utilizzabili anche quando il Titolare si trovi ad operare in una filiale bancaria e/o alla presenza di un operatore della Banca.

In stazioni presidiate, tenendo conto anche del fatto che l'operatore avrà comunque identificato in maniera canonica (de visu) il Titolare, si è cercato di semplificare l'operatività del firmatario rispetto a quanto previsto quando opera attraverso un portale di home banking.

In questo caso il Titolare potrà inserire i codici numerici monouso generati da strumenti di strong authentication su dispositivi tablet in grado di recepire tali password.

Tutte le attività svolte vengono inoltre controllate archiviando le informazioni relative a:

- NDG (Numero direzione generale univoco all'interno della Banca) del cliente, o altro codice di identificazione univoco del Cliente;
- data e ora del momento della firma;
- tracking del sistema di autenticazione;
- stazione di firma e codice dell'operatore della Banca (nel caso di firma effettuata presso filiale bancaria).

In alternativa, come sistema di strong authentication può essere avviata una procedura finalizzata alla registrazione dei dati grafometrici che serviranno nel seguito come strumento di autenticazione per permettere l'utilizzo delle chiavi di firma.

Al Titolare, per la procedura che utilizza i dati grafometrici, in questa fase sarà richiesto di apporre da quattro a sei firme su di un tablet utilizzando una particolare penna: grazie ad uno specifico software il sistema è in grado di acquisire una serie di informazioni relative al modo di firmare del Titolare, informazioni che saranno utilizzate successivamente per permettere al Titolare di autenticarsi e accedere al servizio di firma digitale.

Il riconoscimento della firma non avverrà confrontando l'immagine della stessa, ma sfruttando tutti i parametri grafometrici precedentemente raccolti, quali:

- il ritmo,
- la velocità,
- la pressione,
- l'accelerazione,
- il movimento.

Uno degli aspetti più delicati da affrontare nei riconoscimenti di tipo grafometrico è come garantire nel tempo la qualità del servizio qualora un Titolare, per varie circostanze, dovesse modificare il suo modo di firmare (si pensi ad un giovane che diventa adulto, oppure ad un anziano che potrebbe avere una scrittura più incerta).

Il processo di enrollment garantisce che il riconoscimento della firma grafometrica non si esaurisca in un'unica sessione; infatti, anche successivamente, ogni qual volta il Titolare firmerà, le informazioni raccolte verranno utilizzate per aggiornare il suo profilo grafometrico.

Al momento della sottoscrizione di un documento, al Titolare verrà quindi richiesto di apporre una firma grafometrica su di un tablet.

I parametri grafometrici rilevati saranno comparati con quelli raccolti in precedenza durante la procedura di enrollment.

Il sistema, opportunamente tarato, considererà attendibili solo quei confronti che risulteranno avere una percentuale di verosimiglianza fra il campione e la firma appena apposta pari o superiore al 70%. Tale percentuale è stata scelta e configurata sui sistemi della Banca tenendo conto che le operazioni di identificazione avvengono esclusivamente in postazioni presidiate da operatori della Banca stessa e che, congiuntamente alla verifica della firma, vengono tracciate informazioni quali: un riferimento temporale del momento in cui l'operazione è avvenuta, il codice dell'operatore che ha assistito il Titolare al momento della firma e il numero della postazione dove la firma è stata verificata. Inoltre, in considerazione del fatto che il Titolare era stato anche identificato in maniera canonica dal personale di filiale, è possibile garantire un riconoscimento certo dello stesso senza la benché minima percentuale di errore.

Il processo di enrollment è stato studiato per garantire la massima sicurezza:

- il tablet comunica con l'applicazione software client;
- sul tablet non risiedono dati relativi alle caratteristiche grafometriche di firma del cliente;
- il client comunica poi con il server designato a verificare la validità delle firme appena apposte e alla gestione delle procedure di enrollment precedentemente descritte. Anche in questo caso tutte le connessioni sono protette e cifrate;
- il server necessita infine di un database dove sono stati memorizzati (cifrati) tutti i profili dei Titolari. Questi profili potranno essere recuperati al momento opportuno, decifrati nella memoria del server e, una volta utilizzati, immediatamente rilasciati senza che alcunché di tali profili possa essere modificato in maniera dolosa e/o colposa. Sarà sempre il server che fornirà al client l'esito del confronto (Verify_Match / Verify_No Match).

Oltre a quanto appena descritto, altri aspetti di sicurezza vengono gestiti dall'applicazione, fra questi:

- tutte le comunicazioni fra i vari sistemi coinvolti sono cifrate;
- i dati grafometrici non sono mai in chiaro, ma sempre cifrati;
- il codice del software che gestisce i dati grafometrici è sempre compilato per evitare rischi di code injection;
- il permesso all'accesso di tali sistemi viene gestito tramite un sistema di Kerberos authentication;
- tutti gli accessi ai sistemi e le operazioni effettuate vengono registrati nell'audit log del sistema e resi disponibili al giornale di controllo (postazione di lavoro, ora in cui è stata effettuato un riconoscimento, tentativi effettuati).

D.2.4. Identificazione del Richiedente con un processo di onboarding implementato su sito pubblico/App

Il Richiedente, in questo caso, dovrà utilizzare le specifiche funzioni che gli saranno rese disponibili dalla Banca sulle pagine del proprio sito pubblico o tramite App della Banca stessa.

La Banca, o altra Società del Gruppo o società terza incaricata, in ottemperanza con quanto previsto dalla vigente normativa in materia di Antiriciclaggio e dalle normative interne alla Banca stessa e di altre società del Gruppo, svolge tutte le operazioni necessarie all'identificazione e registrazione del Richiedente. In dettaglio, verifica l'identità del Richiedente tramite i documenti d'identità forniti e raccoglie i dati personali elencati al paragrafo precedente (par. D.2.1).

I controlli effettuati sui dati personali inseriti dal Richiedente riguarderanno:

- verifica sulle principali banche dati di eventuali evidenze che costituiscano motivo ostativo alla prosecuzione del processo;
- effettuazione di specifici controlli antifrode sulla autenticità e accettabilità dei documenti forniti;
- controlli di coerenza tra la persona richiedente e i documenti forniti durante l'identificazione

Al fine di identificare il Richiedente la Banca può, oltre che riconoscere il Richiedente secondo le modalità indicate al punto D.2.1, avvalersi di fornitori che permettono l'identificazione attraverso l'identità digitale SPID o la carta di identità elettronica (d'ora in avanti CIE), o la modalità denominata Videoselfie.

D.2.4.1. Identificazione con Unicredit video selfie

Il Richiedente che decida di identificarsi a mezzo Videoselfie procederà allo scatto di una fotografia del documento di identità selezionato e verranno verificate la liveness (in modo da impedire caricamenti illeciti ed essere certi che lo scatto venga eseguito in tempo reale) e l'autenticità del documento stesso.

Al Richiedente verrà poi richiesto di registrare un videoselfie nel quale eseguirà determinate azioni e, sarà quindi possibile verificare che la persona che sta eseguendo l'identificazione è la stessa presente sul documento di identità. Anche in questo caso verrà verificata la liveness del video in modo da impedire caricamenti illeciti, essere certi che lo stesso venga eseguito in tempo reale. e, in generale, che il sistema di Videoselfie stia interagendo con un soggetto reale e non via siano tentativi di falsificazioni in corso.

Il processo di VideoSelfie sopradescritto è considerato rispondente rispetto ai requisiti AML indicati dal legislatore ai fini dell'identificazione certa dell'utente finale e della verifica della sua identità.

Ritenendo quindi identificato in modo certo l'utente ai fini della norma AML, il QTSP potrà emettere un certificato qualificato caratterizzato da stringenti limitazioni di natura applicativa nonché di spendibilità del certificato stesso (c.d. limitazioni d'uso)

D.2.4.2. Identificazione utilizzando le Identità Digitali SPID (Unicredit SPID)

Nel caso in cui il Richiedente decida di identificarsi utilizzando le Identità Digitali SPID verrà richiesto al Richiedente di autenticarsi al sistema SPID tramite il suo Identity Provider. In particolare, partendo dalle pagine del sito della Banca, o utilizzando specifiche funzioni rese disponibili all'interno dell'App della Banca, il Richiedente già in possesso di credenziali SPID, rilasciate da un qualunque Identity Provider operante sul territorio italiano, potrà svolgere il processo di onboarding.

Infatti, visto e considerato che le identità digitali SPID di livello 2 soddisfano i requisiti previsti dal Regolamento eIDAS n. 910/2014 in termini di identificazione del Richiedente, il QTSP INTESA rilascerà un certificato qualificato.

Tale certificato qualificato, ai sensi dell'Art 19 del D.Lgs 231/2007 e s.m.i., potrà quindi essere utilizzato per l'onboarding bancario.

Il certificato qualificato rilasciato a seguito di identificazione tramite identità digitale SPID (di livello 2) conterrà l'OID 1.3.76.16.5, registrato a cura dell'Agenzia per l'Italia Digitale (AGID), con la seguente descrizione: *"Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity"* e risulterà pienamente operativo.

D.2.4.3. Identificazione utilizzando la Carta di Identità Elettronica (Unicredit CIE)

Nel caso in cui il Richiedente decida di identificarsi attraverso la propria carta di identità elettronica (CIE) gli verrà richiesto di autenticarsi con livello almeno pari a 2, con la propria CIE. In particolare, partendo dalle pagine del sito della Banca, o utilizzando specifiche funzioni rese disponibili all'interno dell'App della Banca, il Richiedente già in possesso della CIE e delle relative credenziali, necessarie per l'accesso ai servizi delle Pubbliche Amministrazioni italiane e ai servizi erogati dagli stati membri dell'Unione Europea ai sensi del regolamento UE 910/2014 eIDAS, potrà svolgere il processo di onboarding.

Tale certificato qualificato, ai sensi dell'Art 19 del D.Lgs 231/2007 e s.m.i., potrà quindi essere utilizzato per l'onboarding bancario.

Infatti, visto e considerato che la CIE e le relative credenziali, soddisfano i requisiti previsti dal Regolamento eIDAS n. 910/2014 in termini di identificazione del Richiedente, il QTSP INTESA rilascerà un certificato qualificato.

Tale certificato qualificato, ai sensi dell'Art 19 del D.Lgs 231/2007 e s.m.i., potrà quindi essere utilizzato per l'onboarding bancario.

Il Richiedente dovrà quindi prendere visione del Manuale Operativo del Certificatore.

Al Richiedente dopo aver terminato l'identificazione verrà rilasciato un certificato di firma qualificata, tale certificato permetterà la firma di un set documentale di natura contrattuale, eventualmente già corredato da sottoscrizioni della Banca (ad esempio, la proposta di apertura di un nuovo Conto Corrente), utilizzando, per la necessaria autenticazione del richiedente a tali fini, i codici OTP usa e getta ricevuti dallo stesso via SMS sul proprio cellulare.

Si precisa che il numero di cellulare utilizzato per l'invio dell'SMS è stato verificato nell'ambito dei tre processi di identificazione descritti nei punti precedenti.

Terminato positivamente il processo di richiesta del nuovo rapporto il contratto sarà ritenuto perfezionato e il rapporto attivo. Il Richiedente potrà prendere visione del contratto anche all'interno dell'ambiente protetto del servizio online attivato.

D.2.4.4. Specificità processo di onboarding implementato per Buddy Bank

Nel seguito vengono descritte delle lievi specificità afferenti ai processi di riconoscimento in ambito BuddyBank.

a. BuddyBank Videoselfie

La procedura di identificazione Buddy Bank del Richiedente terminerà solo successivamente, quando un operatore di Back Office della Banca completerà i necessari controlli. Tuttavia, in considerazione del fatto che ci troviamo di fronte ad un circoscritto utilizzo della firma digitale tale da non produrre alcun effetto giuridico qualora la verifica dell'identità del titolare del certificato non terminasse con esito positivo, già in questa fase del processo verrà emesso un certificato qualificato al Richiedente. Tale certificato permetterà la firma di un set documentale di natura contrattuale, eventualmente già corredato da sottoscrizioni della Banca (ad esempio, la proposta di apertura di un nuovo Conto Corrente), utilizzando per la necessaria autenticazione del richiedente a tali fini i codici OTP usa e getta ricevuti dallo stesso via SMS sul proprio cellulare verificato.

La sottoscrizione così apposta dal richiedente assumerà piena efficacia solo a seguito della conclusione positiva dei controlli in corso necessari sulla documentazione di identificazione da parte dell'operatore di Back Office della Banca.

La Banca comunicherà al Richiedente l'esito del proprio iter di controllo e:

- nel caso di esito positivo, il contratto si perfezionerà ed il rapporto sarà attivato. Solo in questo momento verrà apposta sul contratto una marca temporale per suggellare la conclusione positiva dell'iter. A quel punto, il Richiedente potrà anche prendere visione del Contratto firmato digitalmente, disponibile all'interno dell'ambiente protetto del servizio online attivato. Il Certificato sarà pienamente operativo.
- nel caso di esito negativo, lo stesso verrà comunicato al cliente, il certificato risulterà revocato ed il contratto non potrà quindi perfezionarsi. In tal caso si conserverà solo la documentazione corredata dalla sottoscrizione della Banca – che è stata oggetto di consegna al cliente, con obbligo per lo stesso di scaricarla e memorizzarla - e di tutti gli eventi verrà tenuta traccia solo negli appositi log.

Qualora la Banca pur avendo accertato l'identità del Richiedente non ritenesse comunque opportuno procedere con la stipula di un contratto, si procederà alla sola revoca del certificato emesso, ma non alla distruzione dei documenti precedentemente sottoscritti che confluiranno in archiviazione a termine di legge.

Con l'obiettivo di distinguere chiaramente questi certificati da quelli emessi con identificazioni avvenute in presenza di un operatore, il certificato qualificato del titolare deve contenere uno specifico OID che nel nostro caso sarà: 1.3.76.21.1.5.1.1.1.

b. BuddyBank SPID

Nel caso in cui il Richiedente decida di identificarsi utilizzando le Identità Digitali SPID verrà richiesto al Richiedente di autenticarsi al sistema SPID tramite il suo Identity Provider. In particolare, partendo dalle pagine del sito della Banca, o utilizzando specifiche funzioni rese disponibili all'interno dell'App della Banca, il Richiedente già in possesso di credenziali SPID, rilasciate da un qualunque Identity Provider operante sul territorio italiano, potrà svolgere il processo di onboarding.

Infatti, visto e considerato che le identità digitali SPID di livello 2 soddisfano i requisiti previsti dal Regolamento eIDAS n. 910/2014 in termini di identificazione del Richiedente, il QTSP INTESA rilascerà un certificato qualificato.

Tale certificato qualificato, ai sensi dell'Art 19 del D.Lgs 231/2007 e s.m.i., potrà quindi essere utilizzato per l'onboarding bancario.

Il certificato qualificato rilasciato a seguito di identificazione tramite identità digitale SPID (di livello 2) conterrà l'OID 1.3.76.16.5, registrato a cura dell'Agenzia per l'Italia Digitale (AGID), con la seguente descrizione: "Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity" e risulterà pienamente operativo.

Anche in questo caso, una volta avvenuta l'identificazione certa del titolare, la sottoscrizione così apposta dal richiedente assumerà piena efficacia solo a seguito della conclusione positiva dei controlli in corso necessari sulla documentazione di riscontro da parte dell'operatore di Back Office della Banca.

La Banca comunicherà al Richiedente l'esito del proprio iter di controllo e:

- nel caso di esito positivo, il contratto si perfezionerà ed il rapporto sarà attivato. Solo in questo momento verrà apposta sul contratto una marca temporale per suggellare la conclusione positiva dell'iter. A quel punto, il Richiedente potrà anche prendere visione del Contratto firmato digitalmente, disponibile all'interno dell'ambiente protetto del servizio online attivato. Il Certificato sarà pienamente operativo.
- nel caso di esito negativo, lo stesso verrà comunicato al cliente, il certificato risulterà revocato ed il contratto non potrà quindi perfezionarsi. In tal caso si conserverà solo la documentazione corredata dalla sottoscrizione della Banca – che è stata oggetto di consegna al cliente, con obbligo per lo stesso di scaricarla e memorizzarla - e di tutti gli eventi verrà tenuta traccia solo negli appositi log.

Qualora la Banca pur avendo accertato l'identità del Richiedente non ritenesse comunque opportuno procedere con la stipula di un contratto, si procederà alla sola revoca del certificato emesso, ma non alla distruzione dei documenti precedentemente sottoscritti che confluiranno in archiviazione a termine di legge.

c. BuddyBank CIE

Nel caso in cui il Richiedente decida di identificarsi attraverso la propria carta di identità elettronica (CIE) gli verrà richiesto di autenticarsi con livello almeno pari a 2, con la propria CIE. In particolare, partendo dalle pagine del sito della Banca, o utilizzando specifiche funzioni rese disponibili all'interno dell'App della Banca, il Richiedente già in possesso della CIE e delle relative credenziali, necessarie per l'accesso ai servizi delle Pubbliche Amministrazioni italiane e ai servizi erogati dagli stati membri dell'Unione Europea ai sensi del regolamento UE 910/2014 eIDAS, potrà svolgere il processo di onboarding.

Tale certificato qualificato, ai sensi dell'Art 19 del D.Lgs 231/2007 e s.m.i., potrà quindi essere utilizzato per l'onboarding bancario.

Infatti, visto e considerato che la CIE e le relative credenziali, soddisfano i requisiti previsti dal Regolamento eIDAS n. 910/2014 in termini di identificazione del Richiedente, il QTSP INTESA rilascerà un certificato qualificato.

Tale certificato qualificato, ai sensi dell'Art 19 del D.Lgs 231/2007 e s.m.i., potrà quindi essere utilizzato per l'onboarding bancario.

Anche in questo caso, una volta avvenuta l'identificazione certa del titolare, la sottoscrizione così apposta dal richiedente assumerà piena efficacia solo a seguito della conclusione positiva dei controlli in corso necessari sulla documentazione di riscontro da parte dell'operatore di Back Office della Banca.

La Banca comunicherà al Richiedente l'esito del proprio iter di controllo e:

- nel caso di esito positivo, il contratto si perfezionerà ed il rapporto sarà attivato. Solo in questo momento verrà apposta sul contratto una marca temporale per suggellare la conclusione positiva dell'iter. A quel punto, il Richiedente potrà anche prendere visione del Contratto firmato digitalmente, disponibile all'interno dell'ambiente protetto del servizio online attivato. Il Certificato sarà pienamente operativo.
- nel caso di esito negativo, lo stesso verrà comunicato al cliente, il certificato risulterà revocato ed il contratto non potrà quindi perfezionarsi. In tal caso si conserverà solo la documentazione corredata dalla sottoscrizione della Banca – che è stata oggetto di consegna al cliente, con obbligo per lo stesso di scaricarla e memorizzarla - e di tutti gli eventi verrà tenuta traccia solo negli appositi log.

Qualora la Banca pur avendo accertato l'identità del Richiedente non ritenesse comunque opportuno procedere con la stipula di un contratto, si procederà alla sola revoca del certificato emesso, ma non alla distruzione dei documenti precedentemente sottoscritti che confluiranno in archiviazione a termine di legge.

Si precisa che il numero di cellulare utilizzato per l'invio dell'SMS è stato verificato nell'ambito dei tre processi di identificazione descritti nei punti precedenti.

D.3. Obblighi del Titolare

Il Titolare del Certificato Qualificato per la Firma Digitale è tenuto a conservare le informazioni di abilitazione all'uso della chiave privata di firma in modo adeguato e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente i dati che permettono la creazione della Firma Digitale in base a quanto previsto dall'art. 11, comma 5 del DPCM.

Il Titolare deve attenersi a tutte le disposizioni del DPCM che lo riguardano, in particolare ha l'obbligo di:

- effettuare la richiesta del Certificato Qualificato per la Firma Digitale secondo le modalità descritte dal presente Manuale Operativo;
- custodire il PIN con la massima cura e riservatezza in base a quanto stabilito nell'ambito dei Servizi in dipendenza dei quali è rilasciato, per i quali è previsto l'uso del Certificato Qualificato per la Firma Digitale;
- custodire con la massima cura e riservatezza lo strumento di strong authentication in suo possesso, seguendo tutti gli accorgimenti indicati nell'ambito dei relativi contratti di comodato d'uso ovvero di Internet Banking per i quali è previsto l'uso del Certificato Qualificato per la Firma Digitale;

- conservare il PIN separatamente dallo strumento di strong authentication, restando responsabile di ogni conseguenza dannosa che possa derivare dall'abuso o dall'uso illecito del PIN e/o del dispositivo di strong authentication;
- fare immediata denuncia alle Autorità competenti e alla Banca, in caso di smarrimento o sottrazione del PIN e/o dello strumento di strong authentication, secondo le modalità indicate nei contratti di Internet Banking o per i quali è previsto l'uso del Certificato Qualificato per la Firma Digitale e nel contratto di comodato d'uso del dispositivo di sicurezza fisico;
- inoltrare la richiesta di revoca o sospensione del Certificato Qualificato per la Firma Digitale secondo quanto indicato nel presente Manuale Operativo;
- porre in essere tutte le misure di diligenza atte ad evitare danni a terzi legati all'uso improprio di quanto fornito dal Certificatore;
- utilizzare il dispositivo di firma esclusivamente per la sottoscrizione di documenti, disposizioni o contratti relativi a prodotti o servizi erogati ovvero offerti da UniCredit (ovvero da altre Società del gruppo UniCredit).

E. Il Terzo Interessato

E.1. Il Terzo Interessato - UniCredit

UniCredit verifica che il Richiedente sia in possesso di tutti i requisiti necessari e lo autorizza a richiedere il rilascio del Certificato Qualificato per la Firma Digitale.

Nello svolgimento di tale attività, Unicredit assume la veste di Terzo Interessato.

In veste di Terzo Interessato, UniCredit svolge attività di supporto al Titolare; in particolare sarà la Banca ad indicare al Certificatore:

- eventuali ulteriori limitazioni d'uso del Certificato Qualificato per la Firma Digitale oltre a quelle previste al paragrafo H.1;
- informazioni specifiche relative al Titolare, quali a titolo esemplificativo, ma non esaustivo, eventuali poteri di rappresentanza del Titolare.

Il Terzo Interessato non si sostituisce alle responsabilità e alle competenze della Certification Authority che rimangono immutate e in completa gestione a quest'ultima.

Si rimanda alla tabella RACI e al Lead Time di Processo per l'analisi della dinamica delle responsabilità della CA, della RA e LRA. (vedi Par. S)

E.2. Obblighi del Terzo Interessato

Il Terzo Interessato ha l'obbligo di richiedere la revoca del Certificato ogni qualvolta vengano meno i requisiti in base ai quali il Certificato stesso è stato rilasciato al Titolare.

F. L'Utilizzatore del Certificato (Relying Party)

F.1. L'Utilizzatore del Certificato

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 modo conforme al Regolamento eIDAS.

F.2. Obblighi dell'Utilizzatore

L'Utilizzatore, nel verificare un documento firmato elettronicamente, ha l'obbligo di:

- verificare lo stato di validità del Certificato Qualificato, che non deve essere scaduto, sospeso o revocato al momento che l'utilizzatore ritiene rilevante (es. dell'apposizione della firma, ovvero della verifica;
- verificare la validità del percorso di certificazione, basato sull'elenco pubblico dei certificatori e su eventuali certificati derivanti da accordi di mutua certificazione tra il proprio Certificatore e quelli altrui;
- verificare l'esistenza di eventuali limitazioni all'uso del Certificato utilizzato dal Titolare, in base a quanto indicato nel Manuale Operativo e, in particolare, verificare che l'oggetto della sottoscrizione sia riconducibile alle tipologie di documento ivi specificate.

G. Chiavi di Sottoscrizione, di Certificazione e di Marcatura temporale

G.1. Chiavi di Sottoscrizione, di Certificazione e di Marcatura temporale

L'uso delle chiavi e dei relativi certificati emessi è regolato da quanto disposto dall'art. 8 del DPCM, con particolare riferimento alle modalità con cui il Titolare di una coppia di chiavi di firma possa conservare le informazioni di abilitazione all'uso delle chiavi stesse.

Le chiavi si distinguono secondo le seguenti tipologie:

- chiavi di sottoscrizione, destinate alla generazione e verifica delle firme apposte o associate ai documenti;
- chiavi di certificazione, destinate alla generazione e verifica delle firme apposte ai certificati qualificati e alle loro Liste di Revoca o Sospensione, ovvero alla sottoscrizione dei certificati relativi a chiavi di marcatura temporale;
- chiavi di marcatura temporale, destinate alla generazione e verifica delle marche temporali.

G.2. Modalità di generazione delle chiavi di sottoscrizione

Il Richiedente, identificato e registrato con le procedure descritte (cfr. paragrafo D.1.2), potrà attivare la procedura di generazione delle chiavi di sottoscrizione accedendo a tale funzionalità attraverso un Servizio di Internet Banking di UniCredit oppure in Agenzia UniCredit o altre Società del Gruppo oppure nell'ambito delle attività fuori sede dei Promotori Finanziari / incaricati di UniCredit o altre Società del Gruppo in base al processo di seguito indicato:

- visualizzazione e presa visione del Manuale Operativo;
- visualizzazione dei dati anagrafici del Richiedente che saranno inseriti nel Certificato Qualificato per la Firma Digitale;
- avvio della procedura di generazione delle chiavi e richiesta del Certificato (in questa fase viene generato l'identificativo unico del Titolare).

L'utilizzo combinato del Codice Personale (quando richiesto dalla procedura di firma) e della password generata dal dispositivo di strong authentication per quanto concerne il Servizio di Internet Banking o la firma grafometrica apposta sul tablet costituiscono l'insieme di dati di cui il Titolare deve mantenere in modo esclusivo la conoscenza e il possesso ai sensi dell'art. 8 comma 5 lett. d) del DPCM; essi saranno richiesti ogni qualvolta egli voglia firmare un documento digitale secondo quanto richiesto dall'art. 35, comma 2 del CAD.

Le chiavi di sottoscrizione, create con tale procedura, sono generate su di un dispositivo sicuro, Hardware Security Module, messo a disposizione dal Certificatore, conforme a quanto previsto dall'art. 35 del CAD.

La coppia di chiavi per la creazione e la verifica della firma viene attribuita ad un solo Titolare che ne mantiene sempre il controllo esclusivo tramite la conoscenza dei dati essenziali per il suo utilizzo.

G.3. Modalità di generazione delle chiavi di certificazione

La generazione delle chiavi all'interno dei dispositivi di firma da parte del Responsabile di Certificazione, come previsto dall'art. 7 del DPCM, viene preceduta dall'inizializzazione dei dispositivi di firma utilizzati dal Certificatore per il sistema di generazione dei certificati con i quali si firmano i certificati dei Titolari e quelli del sistema di validazione temporale.

G.4. Modalità di generazione delle chiavi di marcatura temporale

La generazione delle chiavi di validazione temporale avviene secondo quanto stabilito dall'art. 50 del DPCM.

Tali chiavi, per motivi di sicurezza, vengono aggiornate entro 90 (novanta) giorni dalla data della loro emissione (DPCM, art. 49).

H. Certificati

I certificati INTESA sono conformi a quanto indicato nel Reg. eIDAS e nelle Linee Guida AgID (Determinazione N. 147/2019). In seguito a ciò è garantita la loro interoperabilità nel contesto delle attività dei certificatori accreditati italiani ed europei. INTESA emette certificati con un sistema conforme all'art. 32 del DPCM.

H.1. Certificato Qualificato per la Firma Digitale

Il Certificato Qualificato per la Firma Digitale è un insieme di informazioni utilizzato per distribuire in modo sicuro le chiavi pubbliche.

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 Digitale contiene, a titolo esemplificativo, ma non esaustivo le seguenti informazioni:

- numero di serie;
- ragione o denominazione sociale del Certificatore;
- codice identificativo unico del Titolare presso il Certificatore;
- nome, cognome, data di nascita, codice fiscale del Titolare o codice identificativo univoco rilasciato da autorità Statali / Federali;
- valore della chiave pubblica;
- algoritmi di generazione e verifica utilizzabili;
- inizio e fine del periodo di validità del certificato;
- algoritmo di sottoscrizione del certificato;
- tipologia delle chiavi;
- limitazioni nell'uso della coppia di chiavi.

Tutti i Certificati Qualificati per la Firma Digitale, emessi per l'utilizzo nei casi di cui al par. A.1., contengono almeno la seguente limitazione d'uso: "*Il presente certificato è utilizzabile esclusivamente per la sottoscrizione di disposizioni/documenti e contratti relativi a prodotti e servizi venduti e/o erogati nell'ambito dell'attività in sede e fuori sede ovvero nell'ambito soluzioni con tecniche di comunicazione a distanza /di servizi di Internet Banking di UniCredit S.p.A. (e altre società del Gruppo UniCredit sulla base di accordi).*" – "*This certificate can only be used for signing provisions/documents and contracts relating to products and services sold and/or delivered as part of on-site and off-site or as part of the UniCredit S.p.A. Banking services (and other companies of the UniCredit Group on the basis of agreements).*"

In conformità all'art. 19 DPCM, il Certificatore mantiene le informazioni relative alla richiesta di emissione del Certificato Qualificato per la Firma Digitale per almeno 20 (venti) anni dalla data di scadenza dello stesso. Tali informazioni sono conservate dalla Banca per conto del Certificatore.

H.2. Procedura di emissione dei Certificati di certificazione

In seguito alla generazione delle chiavi di certificazione, descritta nel paragrafo G.3, vengono generati i certificati delle chiavi pubbliche, firmati con le rispettive chiavi private e registrati nel Registro dei Certificati secondo le modalità previste dall'art. 17 del DPCM.

H.3. Gestione del codice di emergenza

Per ciascun Certificato Qualificato per la Firma Digitale emesso, il Certificatore fornisce, coerentemente a quanto indicato dall'art. 21 del DPCM, un codice di emergenza riservato da utilizzare per richiedere la sospensione urgente del Certificato.

In questo caso, sarà utilizzato come codice di emergenza il codice generato dallo strumento di strong authentication di cui il Titolare dispone (par. D.2).

I. Revoca del Certificato Qualificato per la Firma Digitale

La revoca del Certificato Qualificato per la Firma Digitale viene asseverata dal suo inserimento nella Lista dei Certificati Revocati, Certificate Revocation List (di seguito CRL) in base a quanto previsto dall'art. 22 del DPCM.

La CRL, firmata dal Certificatore, viene aggiornata con periodicità prestabilita e ad ogni revoca o sospensione. La lista è disponibile sul registro dei certificati.

I.1. Revoca su iniziativa del Certificatore

Salvo i casi di motivata urgenza, il Certificatore che intende revocare il Certificato Qualificato ne dà preventiva comunicazione al Titolare all'indirizzo di corrispondenza o all'indirizzo e-mail indicato in fase di rilascio della Firma Digitale, specificando i motivi della revoca nonché la data e l'ora a partire dalla quale la revoca è efficace (art. 23 DPCM).

La Revoca sarà comunicata dal Certificatore anche al Terzo interessato che la renderà disponibile al Titolare, nell'ambito della sezione protetta del sito di Unicredit.

Il Certificatore procederà tempestivamente alla revoca del Certificato Qualificato per la Firma Digitale qualora venisse a conoscenza di cause limitative della capacità di agire del Titolare, di sospetti utilizzi fraudolenti, di abusi o di falsificazioni.

I.2. Revoca su richiesta del Titolare

Il Titolare che abbia ottenuto il rilascio del Certificato nell'ambito dei Servizi di Internet Banking di UniCredit può richiederne la revoca accedendo ad una specifica sezione resa disponibile nell'ambito del Servizio stesso oppure mettendosi in contatto con il Servizio Clienti di UniCredit; il Certificatore procede alla revoca che viene comunicata al Titolare nell'ambito del Servizio di Internet Banking (art. 24 DPCM).

Il Titolare che abbia ottenuto il rilascio del Certificato in Agenzia UniCredit può richiederne la revoca compilando l'apposito modulo reso ivi disponibile; il Certificatore procede alla revoca che viene comunicata al Titolare, in Agenzia (art. 24 DPCM).

I.3. Revoca su richiesta del Terzo Interessato

La revoca può essere richiesta da Unicredit, nella sua veste di Terzo Interessato. Tale revoca può essere richiesta, a titolo esemplificativo, ma non esaustivo, nel caso in cui il Titolare non sia più in possesso dei requisiti per accedere al servizio di firma.

Il Certificatore, accertata la correttezza della richiesta, darà notizia della revoca al Titolare interessato tramite l'indirizzo di corrispondenza o di posta elettronica comunicato al momento della richiesta del Certificato Qualificato per la Firma Digitale (art. 25 DPCM).

Al Titolare che abbia richiesto il Certificato nell'ambito del Servizio di Internet Banking di UniCredit, la Revoca potrà essere comunicata anche nell'ambito della sezione protetta del sito di UniCredit.

Nel caso in cui il Titolare non risulti intrattenere alcun rapporto con Unicredit, il Certificato Qualificato per la Firma Digitale sarà revocato.

Per effetto di questa revoca il Titolare non potrà più firmare alcun documento con le chiavi di sottoscrizione precedentemente a lui assegnate.

Restano ovviamente validi tutti i documenti sottoscritti precedentemente alla revoca del Certificato Qualificato per la Firma Digitale.

Le attività di Revoca, richieste dal Terzo Interessato, vedranno la piena responsabilità funzionale e gestionale della Certification Authority, la quale comunicherà, come descritto sopra, ai soggetti interessati, la notifica di avvenuta Revoca.

J. Sospensione del Certificato Qualificato per la Firma Digitale

La sospensione è prevista nel caso in cui si renda necessario verificare se un Certificato Qualificato per la Firma Digitale debba essere revocato.

La richiesta di sospensione può essere avanzata da tutte le entità previste dagli artt. 27, 28 e 29 del DPCM: Certificatore, Titolare, Terzo Interessato.

In assenza di comunicazioni da parte del Titolare, il Certificato verrà automaticamente revocato dopo un periodo di 90 (novanta) giorni dalla sospensione e comunque alla scadenza del periodo di sospensione indicato.

J.1. Sospensione su iniziativa del Certificatore

Salvo i casi di motivata urgenza, il Certificatore che intende sospendere il Certificato Qualificato ne dà preventiva comunicazione al Titolare all'indirizzo di corrispondenza o di posta elettronica indicato al momento della richiesta del Certificato Qualificato per la Firma Digitale, specificando i motivi della sospensione nonché la durata, la data e l'ora a partire dalla quale la sospensione è efficace (art. 27 DPCM).

La sospensione sarà comunicata dal Certificatore anche al Terzo interessato che la renderà disponibile al Titolare, nell'ambito della sezione protetta del sito di Unicredit.

Il Certificatore procederà tempestivamente alla revoca del Certificato Qualificato per la Firma Digitale qualora venisse a conoscenza di cause limitative della capacità di agire del Titolare, di sospetti utilizzi fraudolenti, di abusi o di falsificazioni.

J.2. Sospensione su richiesta del Titolare

Il Titolare che abbia ottenuto il Certificato nell'ambito di un Servizio di Internet Banking di UniCredit può richiederne la sospensione accedendo ad una specifica sezione resa disponibile nell'ambito del Servizio stesso; il Certificatore procede alla sospensione che viene comunicata al Titolare nell'ambito del Servizio di Internet Banking in questione (art. 28 DPCM).

Il Titolare, che in precedenza aveva richiesto la sospensione del Certificato, potrà richiederne il ripristino utilizzando la specifica funzione disponibile nell'ambito della sezione protetta del sito di Unicredit, seguendo le modalità indicate.

Il Titolare che abbia ottenuto il rilascio del Certificato in Agenzia UniCredit può richiederne la sospensione compilando l'apposito modulo reso ivi disponibile; il Certificatore procede alla sospensione che viene comunicata al Titolare, in Agenzia UniCredit (art. 28 DPCM).

Altre modalità potranno essere indicate direttamente dalla Banca stessa nell'ambito dei servizi offerti.

J.3. Sospensione su richiesta del Terzo Interessato

La sospensione può essere richiesta da Unicredit, nella sua veste di Terzo Interessato. Il Certificatore, accertata la correttezza della richiesta, darà notizia della sospensione al Titolare interessato tramite l'indirizzo di posta elettronica comunicato al momento della richiesta del Certificato Qualificato per la Firma Digitale.

La sospensione sarà comunicata anche nell'ambito della sezione protetta del sito di Unicredit (art. 29 DPCM).

Le attività di Sospensione, richieste dal Terzo Interessato, vedranno la piena responsabilità funzionale e gestionale della Certification Authority, la quale comunicherà, come descritto sopra, ai soggetti interessati, la notifica di avvenuta Sospensione.

K. Modalità di sostituzione delle chiavi

K.1. Sostituzione del Certificato Qualificato e delle chiavi del Titolare

Il Certificato Qualificato per la Firma Digitale emesso dal Certificatore ha validità di 36 (trentasei) mesi dalla data di emissione.

La richiesta di un nuovo Certificato potrà essere effettuata, in base alle modalità previste dal Manuale Operativo, solo nel caso di Certificato scaduto o revocato dal Titolare

Il Titolare già registrato dovrà comunque segnalare tempestivamente al Certificatore ogni variazione dei dati di registrazione che sia intervenuta nel frattempo.

K.2. Sostituzione delle chiavi del Certificatore

K.2.1. Sostituzione in emergenza delle chiavi del sistema di generazione dei certificati

La procedura da seguire in caso di disastro presso la sede centrale del Certificatore è illustrata al capitolo O.

K.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, utilizzate dai sistemi di emissione dei certificati di sottoscrizione e dei certificati di TSA, il Certificatore INTESA procederà in base a quanto stabilito dall'art. 30 del DPCM.

K.2.3. Sostituzione in emergenza delle chiavi del sistema di validazione temporale

La procedura da seguire in caso di disastro presso la sede centrale del Certificatore è illustrata al capitolo O.

L. Registro dei certificati

L.1. Modalità di gestione del Registro dei certificati

Nel Registro dei Certificati, il Certificatore pubblica:

- i certificati delle chiavi di sottoscrizione e del sistema di validazione temporale;
- i certificati delle chiavi di certificazione;
- i certificati per le chiavi di firma di AgID (già DigitPA e CNIPA);
- le liste di revoca e di sospensione (CRL).

Le operazioni che coinvolgono il registro dei certificati vengono svolte soltanto dalle persone a ciò specificamente autorizzate.

L.2. Accesso logico al Registro dei certificati

Per motivi di sicurezza, tale registro non è accessibile dall'esterno.

È possibile, comunque, accedere a repliche di tale registro utilizzando l'indirizzo *ldap://x500.e-trustcom.intesa.it* nel quale sono contenute le sole informazioni necessarie al controllo di validità della firma.

Il Certificatore consente inoltre l'accesso a tali informazioni di validità (CRL) via Internet, attraverso il protocollo http.

Il Certificatore garantisce in ogni caso l'integrità e la coerenza di tali copie con il registro dei certificati definito al paragrafo L.1. del presente capitolo.

Ai sensi della Determinazione Commissariale 119/2016 e del Regolamento eIDAS, le informazioni di revoca e sospensione sono anche disponibili attraverso il protocollo OCSP.

M. Modalità di protezione della riservatezza

Le misure di sicurezza per la protezione dei dati personali sono conformi alle misure minime previste dal Reg. UE 2016/679 (GDPR).

N. Procedura di gestione delle copie di sicurezza

Gli archivi informatici oggetto di copie di sicurezza sono quelli di seguito indicati:

- registro dei Certificati: archivio digitale contenente quanto specificato al paragrafo L;
- informazioni Operative: archivio digitale in cui sono memorizzate tutte le informazioni ricevute dal Titolare al momento della registrazione e della richiesta di un certificato e 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 Certificatore (art. 36 del DPCM);
- archivio Digitale delle Marche Temporali: contiene le marche temporali generate dal sistema di validazione temporale (art. 49 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 in modo da renderlo incompatibile con i requisiti previsti dall'art. 51 del DPCM.

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

O. Procedura di gestione degli eventi catastrofici

Il Responsabile della sicurezza gestisce un piano di 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 back up del Certificatore, 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 della sede principale, 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 (ventiquattro) ore di personale atto ad attivare la funzionalità di emissione delle CRL. Di detto personale viene curato l'addestramento circa la gestione dei dispositivi software e hardware e delle situazioni di emergenza. È previsto inoltre l'intervento, entro il medesimo lasso di tempo, dei depositari delle componenti la chiave privata del Certificatore ai fini di ricostruirla nel dispositivo di firma del sito di backup.

In tutte le località interessate dalla gestione degli eventi catastrofici è depositata copia cartacea del piano di emergenza.

P. Procedure per la validazione temporale

P.1. Servizio di validazione temporale

Il Certificatore appone una marca temporale ai documenti, disposizioni o contratti sottoscritti digitalmente dal Titolare.
L'apposizione di una marca temporale è un processo integrato nell'attività di firma di un documento, pertanto al Titolare non è richiesta alcuna attività.

P.2. Modalità per l'apposizione e la definizione del riferimento temporale

Tutte le macchine del QTSP INTESA sono sincronizzate al riferimento temporale fornito dall'I.N.RI.M. - Istituto Nazionale di Ricerca Metrologica di Torino (già Istituto Elettrotecnico Nazionale Galileo Ferraris). Questa funzionalità è realizzata mediante il protocollo NTP (Network Time Protocol). L'I.N.RI.M fornisce un servizio di sincronizzazione per sistemi informatici collegati alla rete Internet, basato su due server NTP primari installati nel Laboratorio di Tempo e Frequenza Campione. Essi, a loro volta, sono sincronizzati alla scala di tempo nazionale italiana UTC(IT). Lo scarto di tempo tra i server NTP dell'I.N.RI.M e la scala di tempo nazionale italiana viene tenuto sotto controllo ed è normalmente inferiore ad alcuni millisecondi. La precisione di sincronizzazione ottenibile dipende dalla tipologia della rete e dalla distanza interposta tra il server NTP e il calcolatore che si vuole sincronizzare; i valori di scarto tipici sono inferiori al millisecondo per sistemi appartenenti alla stessa rete e possono arrivare a qualche centinaio di millisecondi per reti remote.

I server dedicati ai servizi di marcatura temporale hanno inoltre un controllo software tra l'orario della macchina e un cospicuo numero di server NTP distribuiti a livello planetario: l'utilità di controllo, installata su ognuno dei server utilizzati dal QTSP INTESA nell'ambito della validazione temporale, periodicamente verifica l'allineamento del clock di sistema questi NTP Server di riferimento Se l'allineamento temporale non risulta conforme alle specifiche tecniche di riferimento tempo per tempo vigenti, il servizio di marcatura temporale erogato dallo specifico server che risultasse disallineato viene arrestato.

I riferimenti temporali apposti dalle applicazioni sono stringhe in formato data (DD/MM/YYYY hh:mm:ss), con la precisione del secondo, che rappresentano l'ora locale, in base alla configurazione della macchina. Tali riferimenti sono conformi al DPCM Art.51.

Ogni registrazione effettuata sul giornale di controllo contiene un riferimento temporale che, essendo generato con la modalità qui descritta, è opponibile a terzi (Art.41 del DPCM).

Q. Modalità operative per la verifica della Firma Digitale

I documenti (intendendosi per tali, ove previste, anche le disposizioni) e i contratti sono sottoscritti con firma digitale nell'ambiente dei Servizi di Internet Banking di UniCredit (ovvero dei corrispondenti Servizi di altre Società del Gruppo UniCredit), nonché nell'ambito dell'attività in sede di UniCredit (o di altre società del Gruppo), così come nell'ambito dell'attività fuori sede svolta attraverso le tipologie di soggetti tempo per tempo normativamente legittimate. I documenti in formato PDF possono essere verificati utilizzando il software *Acrobat Reader DC*, scaricabile gratuitamente sul sito *www.unicredit.it* oppure sul sito *www.adobe.com/it*.

R. Modalità operative per la generazione della Firma Digitale

Il Certificatore mette a disposizione del Titolare quanto necessario a generare la firma digitale conformemente a quanto prescritto dalle norme vigenti in materia.

R.1. Modalità di Firma nell'ambito dei servizi di Internet Banking

La specificità dei Servizi di Internet Banking di UniCredit (così come i servizi analoghi di altre Società del Gruppo) non prevede la consegna di un'applicazione di firma da installare sul personal computer dell'utente aderente ai Servizi stessi: tutte le funzionalità che permettono la sottoscrizione di uno o più documenti digitali potranno essere richiamate direttamente all'interno delle apposite sezioni protette del sito di UniCredit (o di altri siti di Società del Gruppo).

Dopo aver eseguito l'accesso al Servizio di Internet Banking, il Titolare dovrà poter esaminare il documento da firmare e avviare la procedura di firma tramite l'immissione della password generata dal dispositivo di strong authentication.

Le firme digitali così generate sono conformi ai requisiti previsti per gli algoritmi di firma dall'art. 43 comma 2 del DPCM.

Tali documenti, nel rispetto di quanto previsto sempre dall'art. 4 comma 3 del DPCM, non contengono inoltre macroistruzioni o codici eseguibili tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati, evitando al sottoscrittore di dover effettuare tale verifica.

R.2. Modalità di Firma nell'ambito dell'attività in sede

Il Titolare, al momento della firma, si troverà nei locali nei quali UniCredit (o altra Società del Gruppo) svolge la propria attività in sede al cospetto del personale incaricato, che lo avrà identificato.

A seguito del riconoscimento, il Titolare dovrà poter esaminare il documento e avviare la procedura di firma, apponendo una firma su di un dispositivo tablet (in modo analogo a come aveva firmato nella fase di enrollment descritta al paragrafo D.1.1.2) oppure, in alternativa alla firma grafometrica, immettendo la password "usa e getta" generata da un dispositivo di strong authentication.

Il Titolare potrà anche firmare su un diverso dispositivo che può essere fornito dalla Banca, utilizzando una password "usa e getta", generata da un dispositivo di strong authentication, nonché, ove previsto, un codice identificativo (ad es. il Codice Personale del proprio servizio di Internet banking).

Le firme digitali così generate sono conformi ai requisiti previsti per gli algoritmi di firma dall'art. 43 comma 2 del DPCM.

Tali documenti, nel rispetto di quanto previsto all'art. 4 comma 3 del DPCM, non contengono inoltre macroistruzioni o codici eseguibili tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati, evitando al sottoscrittore di dover effettuare tale verifica.

R.3. Modalità di Firma nell'ambito dell'attività fuori sede

Il Titolare, al momento della firma, si troverà all'esterno dei locali nei quali UniCredit (o altra Società del Gruppo UniCredit) esercita la propria attività in sede, e al cospetto del soggetto del quale Unicredit (o altra Società del Gruppo) si avvale per la propria attività fuori sede, che lo avrà identificato.

A seguito del riconoscimento, il Titolare dovrà poter esaminare il documento e avviare la procedura di firma, apponendo una firma su di un dispositivo tablet (in modo analogo a come aveva firmato nella fase di enrollment descritta al paragrafo D.1.1.2) oppure, in alternativa alla firma grafometrica, immettendo la password "usa e getta" generata da un dispositivo di strong authentication.

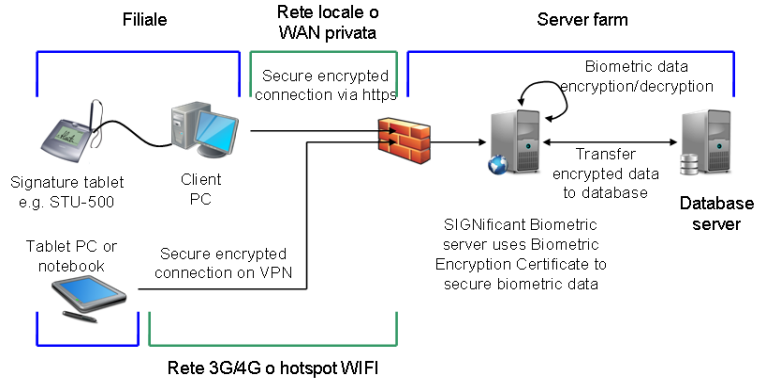
Il Titolare potrà anche firmare su un diverso dispositivo che può essere fornito dalla Banca, utilizzando la combinazione della password "usa e getta", generata da un dispositivo di strong authentication, con un codice identificativo (ad es. il Codice Personale del proprio servizio di Internet banking).

Le firme digitali così generate sono conformi ai requisiti previsti per gli algoritmi di firma dall'art. 43 comma 2 del DPCM.

Tali documenti, nel rispetto di quanto previsto all'art. 4 comma 3 del DPCM, non contengono inoltre macroistruzioni o codici eseguibili tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati, evitando al sottoscrittore di dover effettuare tale verifica.

R.4. Gestione del flusso dei dati biometrici

Di seguito, il grafico riassuntivo del flusso dei dati biometrici per le tre modalità sopra descritte.



R.5. Firma digitale con Notifica Push su App Mobile Banking

La Banca si è dotata anche di ulteriori e innovativi strumenti tecnologici per permettere la firma di documenti, disposizioni o contratti relativi a prodotti o servizi erogati ovvero offerti da UniCredit o altre Società del Gruppo. Tra questi, la firma tramite l'App Mobile Banking Unicredit.

Il processo di attivazione dell'App Mobile Banking Unicredit prevede, a garanzia della sicurezza, che:

- il Cliente possa utilizzare in modalità dispositiva la propria App Mobile Banking solo previa attivazione della stessa su un solo dispositivo Mobile;
- l'utilizzo dell'App Mobile Banking per la sottoscrizione possa essere effettuato da ciascun Cliente su di un solo dispositivo Mobile; pertanto, nel caso in cui il Cliente decidesse di attivare l'App Mobile Banking in modalità dispositiva su uno Smartphone differente rispetto a quello precedentemente utilizzato, prima di poter effettuare una nuova attivazione, sarà necessario completare la disattivazione dell'App sul precedente dispositivo Mobile;
- l'attivazione dell'App Mobile Banking effettui una verifica incrociata dei recapiti del Cliente (numero di telefono e indirizzo e-mail) e richiede una *Strong Authentication* finale (inserimento della penultima quartina della Carta di Debito / Genius Card in possesso del Cliente o Codice di Sicurezza generato dal dispositivo Mobile Token e/o altri dispositivi con analoghe caratteristiche). Nel caso in cui i recapiti del Cliente risultassero già verificati all'interno dell'Anagrafica UniCredit, non sarà possibile modificarli autonomamente dal proprio dispositivo Mobile in sede di Attivazione;
- tramite Attivazione dell'App Mobile Banking venga effettuata un'associazione univoca tra App installata in modalità dispositiva, dispositivo Mobile utilizzato e utenza associata allo specifico Cliente.

Dovendo procedere con una firma digitale in questa modalità, il Titolare dovrà, prima di procedere, accedere all'app precedentemente installata.

Il processo di Login all'interno dell'App Mobile Banking richiederà una verifica incrociata di tre informazioni, di seguito riportate, che consentono l'identificazione univoca del Cliente:

- Codice Adesione
- Codice PIN di accesso al Servizio Internet Banking (es. Banca Multicanale) / Fingerprint/ Riconoscimento del volto: è un codice di accesso numerico / biometrico che dovrà essere necessariamente inserito dal Cliente ad ogni Login
- Codice OTP: è un codice OTP (Mobile Token) che viene generato automaticamente dall'App in fase di Login (si specifica infatti che l'App, una volta attivata su un dispositivo Mobile, è in grado di generare Codici Token di Sicurezza).

L'App invierà queste tre informazioni ai Sistemi Banca per opportune verifiche, autorizzando pertanto la Login del Cliente solo nel caso in cui l'esito di tali verifiche sia positivo.

Se lo Smartphone del Cliente supporta la tecnologia per il riconoscimento dell'impronta digitale o del volto, questi potrà utilizzare la modalità denominata "FingerPrint/FaceId o Riconoscimento del volto" sia per identificarsi in sede di accesso al Servizio di Banca Multicanale tramite Applicazione Mobile Banking, sia per autorizzare operazioni/processi previsti per tale modalità.
In alternativa, potrà usare un codice personale di identificazione scelto in fase di attivazione dell'App denominato "mPin". Tale codice si compone di soli caratteri numerici e ha una lunghezza compresa tra 6 e 10 cifre.

R.5.1. Firma digitale in filiale su tablet con Notifica Push su App Mobile Banking

Il Cliente procede con la firma del documento direttamente in Filiale, tramite utilizzo di uno dei tablet di UniCredit messo a disposizione della clientela:

- nel momento in cui l'operatore di Filiale invia il documento da firmare sul tablet, il Cliente riceverà, sul dispositivo Mobile sul quale ha attivato l'App Mobile Banking, una Notifica Push che lo invita a confermare la firma del documento visualizzato tramite tablet;
- selezionando la Notifica Push ricevuta, si aprirà nel tablet la schermata di riepilogo del contratto / modulo in attesa di sottoscrizione;
- il Cliente dovrà procedere all'autorizzazione alla sottoscrizione sull'App tramite inserimento del proprio Codice mPin / FingerPrint / Riconoscimento del volto;
- avuta l'autorizzazione a procedere, il documento verrà inviato in firma sui sistemi di firma remota;
- il tablet messo a disposizione del Cliente visualizza la "Thank You Page", a conferma dell'avvenuta firma digitale del documento.

R.5.2. Firma tramite Banca via Internet, o su un chiosco installato presso una filiale della Banca con Notifica Push

Il Cliente potrà procedere, volendo, con la firma del documento utilizzando i servizi di Internet Banking direttamente a casa con il proprio PC o in filiale su appositi chioschi messi a disposizione della clientela.
In questo caso il Cliente potrà procedere con la firma del documento eseguendo i passi seguenti:

- il Cliente accede alla sua area riservata e alla sezione attività, visualizzando tutta la lista/e dei contratti / moduli da firmare;
- seleziona il modulo da firmare e seleziona tutte le checkbox in pagina;
- il cliente visualizza in pagina la richiesta di invio di una PUSH Notification sulla rispettiva APP;
- sul desktop compare la schermata di notifica inviata e in attesa conferma;
- il Cliente riceverà, sul dispositivo Mobile sul quale ha attivato l'App Mobile Banking, una Notifica Push che lo invita a confermare la firma del contratto sul desktop;
- selezionando la Notifica Push ricevuta, si aprirà la schermata di riepilogo del contratto / modulo di attesa di autorizzazione;
- il Cliente dovrà procedere all'autorizzazione sull'App tramite l'inserimento del proprio Codice mPin / FingerPrint / Riconoscimento del volto;
- il Cliente procede con l'OK di conferma sull'app;
- si procede quindi all'invio del documento agli appositi sistemi di firma remota;
- a seguire, il Cliente visualizza la "Thank You Page" sulla Banca via Internet, che conferma l'avvenuta firma digitale del documento.

R.5.3. Firma utilizzando esclusivamente l'App della Banca su proprio device

Il Cliente procede con la firma del contratto tramite utilizzo della App Mobile della Banca.

- il Cliente dovrà necessariamente procedere all'autenticazione dell'App tramite inserimento del proprio Codice mPin / FingerPrint / Riconoscimento del volto;
- il Cliente accederà alla sezione attività e procederà, come di seguito descritto, alla firma del documento;
- il Cliente visualizzerà il documento da firmare in formato PDF, secondo il processo già in essere;
- il Cliente dovrà proseguire con "accetta e prosegui" di tutti i punti firma del contratto / documento;
- il Cliente dovrà procedere all'autorizzazione della firma tramite inserimento del proprio Codice mPin / FingerPrint / Riconoscimento del volto;
- confermando l'autorizzazione, si procede all'invio del documento ai sistemi di firma;
- il Cliente visualizza la "Thank You Page" che conferma l'avvenuta firma digitale del documento.

R.6. Firma digitale in processi con tecniche di comunicazione a distanza che prevedano la presenza di operatore in remoto

Il Cliente, intestatario di rapporti in qualità di consumatore e Titolare del certificato qualificato di firma elettronica rilasciato nell'ambito di quanto descritto nel presente manuale operativo, ha la possibilità di sottoscrivere digitalmente a distanza documenti predisposti dalla Banca anche per l'accensione di nuovi rapporti diversi dal conto corrente a condizione che presenti uno dei seguenti requisiti:

- credenziali di accesso di servizi di internet banking
- adesione ad altre soluzioni predisposte dalla Banca per la sottoscrizione digitale anche in sede (es Firma Mia)

presupposti di identificazione (cellulare univocamente verificato ed e-mail verificata), elementi di contatto verificati per il rilascio del certificato di firma.
Qualora il Cliente, pur essendo già identificato, non fosse in possesso di un certificato qualificato, potrà farne richiesta preventivamente all'operatore stesso, il quale, dopo averlo identificato, provvederà a inviare all'indirizzo e-mail del Cliente la necessaria documentazione per la richiesta di certificazione.
L'operatore chiederà al Cliente di prenderne visione e di procedere , se interessato, con la richiesta del certificato; tale richiesta sarà registrata e conservata per 20 anni come prova della volontà del Cliente di procedere con l'emissione di un certificato qualificato a proprio nome.

R.6.1. Modalità di interazione e processo

IL processo è basato su un contatto telefonico (inbound e/o outbound), oggetto di registrazione sulla base dei sistemi e delle dotazioni tecnologiche tempo per tempo adottate dalla Banca, tra un Cliente con le caratteristiche sopra indicate ed un operatore della Banca stessa e consente la sottoscrizione di documenti anche contrattuali (fatta esclusione per quelli necessari all'apertura di un nuovo conto corrente) nel rispetto delle normative vigenti con riferimento alla promozione ed alla vendita di prodotti/servizi mediante tecniche di comunicazione a distanza (es. diritto di ripensamento).
Il Cliente viene riconosciuto in modalità strong per il tramite verifica di credenziale di un servizio di Internet Banking ovvero mediante una serie di domande predisposte per verificarne l'identità attraverso la verifica di una pluralità di parametri (variabili nel tempo e per persona) specificamente collegati alla sua relazione con la Banca, ad es. codice identificativo di uno dei rapporti in essere.
Una volta identificato, l'operatore procede con la raccolta delle esigenze del cliente e/o la promozione di prodotto.
Nel corso della telefonata registrata, verrà inviata al Cliente, all'indirizzo e-mail verificato, la documentazione precontrattuale, ove previsto, nonché il documento che dovrà essere oggetto di sottoscrizione, per consentirgli la preventiva presa visione e valutazione.
Il documento da sottoscrivere sarà caratterizzato da specifici elementi volti a garantire immodificabilità e univocità, sia rispetto al contenuto, sia rispetto alle modalità/canale di sottoscrizione (impronta digitale del documento -hash – e stringa identificativa del contatto con l'operatore), nonché garantire l'origine e l'integrità.
Il Cliente potrà quindi visualizzare autonomamente il documento, prendendone visione e verificandone tutti i contenuti, prima di dichiarare all'operatore di voler procedere ad esprimere il proprio consenso a fini di determinarne la sottoscrizione.
L'operatore, sempre nel corso di telefonata registrata, visualizza sull'apparecchiatura della Banca il documento inviato al cliente e provvede a:

- registrare sullo stesso documento i consensi via via espressi dal cliente;
- inserire la password usa e getta dettata dal Cliente e derivante da SMS sul cellulare univocamente verificato in precedenza ovvero altro dispositivo in suo possesso, quale autentica per l'apposizione delle firme digitali corrispondenti.

Una volta completato l'iter con l'apposizione della firma digitale e della marca temporale al documento, la Banca lo metterà a disposizione del Cliente in apposita sezione dell'Internet Banking ovvero lo invierà all'indirizzo e-mail verificato.
Il documento verrà conservato a norma unitamente alla e-mail inviata preventivamente alla sottoscrizione.

S. 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*	*Unicredit (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 o Sospensione del Certificato vs. RA o LRA*	*Intesa (acting as) Registration Authority (RA) o Unicredit Local RA (acting as)*	*Emette ordine di revoca o sospensione del Certificato vs CA, previa verifica identità*	*Certification Authority*	*Evasione Richiesta di Revoca o Sospensione*
Utente, Richiedente, Titolare Certificato	*Richiesta di Riattivazione del Certificato vs. RA o LRA*	*Intesa (acting as) Registration Authority (RA) o Unicredit Local RA (acting as)*	*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***

T. 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
Rec ITU-R	Recommendation ITU-R TF.460-6, Annex 1 – Time Scales.
ETSI TS 119 461	ETSI TS 119 461 v1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects

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