# Manuale Operativo del Certificatore Accreditato In.Te.S.A. S.p.A. per la procedura di Firma Digitale nell'ambito dei Servizi di Internet Banking, dell'attività in sede e dell'attività fuori sede di UniCredit S.p.A. (e di altre Società del Gruppo)

Firmato da:
ANTONIO RAIA
Codice fiscale: RAINTN66A02L219C
Organizzazione: IN.TE.S.A. S.p.A./05262890014

Codice documento: MOU-UC

Redazione: Antonio Raia

Approvazione: Franco Tafini

Data emissione: 19/04/2017

Versione: 06

# Versione

| | | |
|---|---|---|
| **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.<br>Conseguente variazione del Codice Documento da MOU-UCB a MOU-UC | |
| Motivazioni: | Aggiornamento | |
| **Versione n. 03** | | Data emissione: 01/06/2012 |
| Descrizione modifiche: | **A.1.1, D.1.2.2:** 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.<br>**R.1.2:** Introduzione della modalità di firma in Agenzia tramite Tablet.<br>**B.1.1:** Variazione dati anagrafici Certificatore.<br>**B.1.3, H.1.1:** Variazione della limitazione d'uso.<br>**D.1.2.1:** 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.<br>**I.1.2, J.1.2:** Introduzione della richiesta di Revoca o Sospensione in Agenzia.<br>**P.1.2:** Aggiornamento denominazione del fornitore del riferimento temporale. | |
| Motivazioni: | Aggiornamento | |
| **Versione n. 04** | | Data emissione: 09/10/2015 |
| Descrizione modifiche: | **A.1.2:** Aggiornamento riferimenti normativi<br>**B.1.1:** Variazione dati identificativi del Certificato**re**<br>**R.1.3**: Firma grafometrica generata tramite tablet anche nell'ambito dell'attività fuori sede effettuata dai Promotori Finanziari di Unicredit<br>**R.1.4**: Grafico flusso procedurale (protezione dei dati biometrici) | |
| Motivazioni: | Variazione sede legale del Certificatore<br>Aggiornamenti | |
| **Versione n. 05** | | Data emissione: 13/08/2016 |
| Descrizione modifiche: | Introdotto riferimento ai servizi offerti dalle *Società del Gruppo Unicredit*<br>**B.1.3, H.1.1**:Modificato il testo della Limitazione d'uso del Certificato Qualificato<br>**R.1.3:** Aggiornamento descrizioni delle Modalità di Firma (servizi Internet Banking, attività in sede, attività fuori sede)<br>Variazione riferimenti normativi – verifica conformità | |
| Motivazioni: | Aggiornamenti servizi<br>Aggiornamenti normativi - Regolamento (UE) 910/2014 (eIDAS) | |
| **Versione n. 06** | | Data emissione: 19/04/2017 |
| Descrizione modifiche: | **D.1.2.2:** Ottimizzazione parametro di *Threshold*<br>**A.1.2:** Aggiornamento riferimenti normativi | |
| Motivazioni: | Adeguamento valore di *Threshold* per ottimizzazione della gestione del multidevice<br>Aggiornamento | |

# Sommario

# Introduzione

## 1.1. Definizioni

| | |
|---|---|
| *Certificato Qualificato* | Attestato elettronico, che contiene un insieme di informazioni che creano una stretta e affidabile correlazione fra una chiave pubblica e i dati che identificano il Titolare, conforme ai requisiti di cui all'Allegato I della direttiva 1999/93/CE, rilasciato da un Certificatore che risponde ai requisiti di cui all'Allegato II della medesima direttiva. |
| *Certificatore* | Il Certificatore Accreditato In.Te.S.A. S.p.A. che presta servizi di certificazione delle firme elettroniche o che fornisce 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. |
| *AgID*<br>*già DigitPa*<br>*già CNIPA* | Agenzia per l'Italia Digitale<br>già Ente nazionale per la digitalizzazione della Pubblica Amministrazione<br>già Centro Nazionale per l'informatica nella Pubblica Amministrazione |
| *CRL* | Lista dei Certificati Revocati, Certificate Revocation List, un elenco che riporta un insieme di certificati non più considerati validi dal Certificatore che li ha emessi. |
| *CSL* | Lista dei certificati sospesi, Certificate Suspension List, che generalmente viene inclusa nella CRL. |
| *Documento informatico* | 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 fra loro, che consente al Titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, di rendere manifesta e di verificare la provenienza ed integrità di uno o più documenti informatici. |
| *HSM* | Hardware Security Module, dispositivi hardware dedicati alla sicurezza crittografica e alla gestione delle chiavi in grado di garantire un elevato livello di protezione. |
| *Marca Temporale* | 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. |

## 1.2. 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. |
| *DELCNIPA 45/09* | Deliberazione CNIPA 21 maggio 2009, "*Regole per il riconoscimento e la verifica del documento informatico*" e successive modificazioni e integrazioni. |
| *DLGS196/03* | Codice in materia di protezione dei dati personali (G.U. n. 174 del 29 luglio 2003) 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. |
| *DPCM 19/07/2012* | Decreto del Presidente del Consiglio dei Ministri 19 luglio 2012, "*Definizione dei termini di validità delle autocertificazioni circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza di cui al decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003, e dei termini per la sostituzione dei dispositivi automatici di firma*" e successive modificazioni e integrazioni. |
| *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. |

## A. Il Manuale Operativo

### 1.1. Il Manuale Operativo

Questo documento è il Manuale Operativo per la procedura di firma digitale del Certificatore Accreditato In.Te.S.A. S.p.A. (di seguito anche solo Certificatore o INTESA) per la procedura di Firma Digitale nell'ambito dei Servizi di Internet Banking, dell'attività in sede e nell'attività fuori sede di UniCredit (nonché, in presenza di specifici accordi tra UniCredit e società del Gruppo UniCredit che intrattengano a propria volta rapporti con Intesa S.p.A.).
Il Manuale Operativo descrive le procedure e le relative regole utilizzate dal Certificatore 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 (o altre Società del Gruppo), utilizzando la combinazione della password "usa e getta" generata da dispositivi di strong authentication e dal Codice Personale del Servizio;
- 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 e dagli artt. 26 e 29 del CAD.
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.

### 1.2. Dati identificativi del Manuale Operativo

Il presente documento costituisce la versione n. 06, rilasciata il 19/04/2017, del "*Manuale Operativo del Certificatore Accreditato In.Te.S.A. S.p.A. per la procedura di Firma Digitale nell'ambito dei Servizi di Internet Banking, dell'attività in sede e dell'attività fuori sede 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 *http://e-trustcom.intesa.it/ca_pubblica/mo_UniCredit.pdf*;
- all'indirizzo Internet dell'Agenzia per l'Italia Digitale, *www.agid.gov.it*.

### 1.3. Responsabilità del Manuale Operativo

La responsabilità del presente Manuale Operativo è di INTESA, nella persona di Antonio Raia (art. 40 comma 3 lett. c) del DPCM), il quale ne cura la stesura, la pubblicazione e l'aggiornamento in accordo e in collaborazione con la Unicredit.
Anche le revisioni del presente Manuale Operativo dovranno essere sempre concordate con la Banca.
Le revisioni del Manuale Operativo verranno pubblicate nell'ambito dei siti indicati al precedente paragrafo A.1.2. e comunicate al Titolare nell'ambito della sezione protetta del sito *www.unicredit.it*.

### 1.4. 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 di UniCredit S.p.A. (e di altre Società del Gruppo).

### 1.5. Tariffe

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

## B. Il Certificatore Accreditato

### 1.1. Il Certificatore Accreditato INTESA

Il Servizio è erogato da INTESA che operando in ottemperanza con quanto previsto dal DPCM e dal CAD, espleta le attività di Certificatore Accreditato (di seguito 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* |
| **Fax** | +39-011-192.16.375 |
| **Email** | *marketing@intesa.it* |
| **Indirizzo (URL) registro dei certificati** | *ldap://x500.e-trustcom.intesa.it* |
| **ISO Object Identifier (OID)** | 1.3.76.21.1 |

### 1.2. Obblighi del Certificatore

Nello svolgimento della sua attività il Certificatore adotta tutte le misure organizzative e tecniche idonee ad evitare danno ad altri e opera in conformità con quanto disposto dal CAD.
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 DLGS196/03 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;
- 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.

### 1.3. Limitazioni di Responsabilità del Certificatore

Il Certificatore 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 Certificatore 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 Certificatore 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.
Nel Certificato Qualificato per la Firma Digitale emesso nell'ambito di un Servizio di Internet Banking di UniCredit, o durante l'attività fuori sede o nell'attività in sede, è inserita 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 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 base a quanto previsto dall'art. 15 comma 1 lett. i) del DPCM, il Certificatore ha stipulato un contratto assicurativo 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.
La copertura Assicurativa prevede i seguenti massimali:

- 250.000,00 (duecentocinquantamila) euro per singolo sinistro;
- 1.500.000,00 (unmilionecinquecentomila) euro per annualità.

## C. La Registration Authority

### 1.1. La Registration Authority - UniCredit

Il Certificatore ha rilasciato mandato a svolgere la funzione di Registration Authority a UniCredit S.p.A. sede sociale Via Alessandro Specchi, 16, 00186, Roma - Direzione Generale: Piazza Gae Aulenti, 3 - Tower A - 20154 Milano - Capitale Sociale € 20.267.667.511,62, interamente versato - Iscrizione al Registro delle Imprese di Roma, Codice Fiscale e P. IVA 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.

### 1.2. 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 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

### 1.1. 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 online attraverso i servizi di Internet Banking di Unicredit o altre Società del Gruppo, nelle Agenzie/locali della Banca o di altre Società del Gruppo 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 o a analoghi Servizi offerti da UniCredit o altre Società del Gruppo, 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 o di analoghi Servizi 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 del Servizio di Banca Multicanale o di analoghi Servizi offerti da UniCredit S.p.A. o altre Società del Gruppo stesso.

## 1.2. Identificazione del Richiedente

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.

### 1.2.1. Firma digitale in Servizi di Internet Banking

Nell'ambito di un Servizio di Internet Banking, 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, 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.

### 1.2.2. 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 tale 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).

### 1.3. 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 di Internet Banking, nell'ambito dei quali è rilasciato, per il quale 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

### 1.1. 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.1.1;
- informazioni specifiche relative al Titolare, quali a titolo esemplificativo, ma non esaustivo, eventuali poteri di rappresentanza del Titolare.

### 1.2. 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

### 1.1. L'Utilizzatore del Certificato

Utilizzatore è chi si avvale di un Certificato Qualificato per verificare la validità di un documento firmato digitalmente.

### 1.2. Obblighi dell'Utilizzatore

L'Utilizzatore ha l'obbligo di:

- verificare la validità del Certificato contenente la chiave pubblica del Titolare firmatario del messaggio;
- verificare l'assenza del Certificato Qualificato per la Firma Digitale dalla Lista di Revoca e Sospensione dei certificati (CRL) e il momento della sua emissione;
- 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 specificati.

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

### 1.1. 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.

### 1.2. 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.

### 1.3. 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.

### 1.4. Modalità di generazione delle chiavi di marcatura temporale

La generazione delle chiavi di validazione temporale avviene secondo quanto stabilito dall'art. 50 del DPCM.
In particolare tali chiavi, per motivi di sicurezza, vengono aggiornate entro 90 (novanta) giorni dalla data della loro emissione.

## H. Certificati

I certificati INTESA sono conformi a quanto indicato nella deliberazione CNIPA n. 45 del 21 maggio 2009. In seguito a ciò è garantita la loro interoperabilità nel contesto delle attività dei certificatori accreditati italiani. INTESA emette certificati con un sistema conforme all'art. 32 del DPCM.

### 1.1. 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 nell'ambito di un Servizio di Internet Banking di UniCredit, o durante l'attività fuori sede o nell'attività in sede, 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 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.

### 1.2. Procedura di emissione dei Certificati di certificazione

In seguito alla generazione delle chiavi di certificazione, descritta nel paragrafo G.1.3, 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.

### 1.3. 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 (cfr. paragrafo C.1.2.).

## 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.

### 1.1. 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 email 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.

### 1.2. 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).

### 1.3. 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.

## 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.

### 1.1. 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.

### 1.2. 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.

### 1.3. 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).

## K. Modalità di sostituzione delle chiavi

### 1.1. 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.

### 1.2. Sostituzione delle chiavi del Certificatore

#### 1.2.1. 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.

#### 1.2.2. Sostituzione pianificata delle chiavi di certificazione

Almeno 90 (novanta) giorni prima della scadenza del Certificato relativo alla coppia di chiavi utilizzate dal sistema di emissione dei certificati, il Certificatore INTESA procederà in base a quanto stabilito dall'art. 30 del DPCM.

#### 1.2.3. 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

### 1.1. 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 emessi a fronte di accordi di certificazione con altri;
- i certificati emessi a seguito della sostituzione delle chiavi di certificazione;
- i certificati per le chiavi di firma di AgID (già DigitPA e CNIPA);
- le liste di revoca e di sospensione.

Le operazioni che coinvolgono il registro dei certificati vengono svolte soltanto dalle persone a ciò specificamente autorizzate.
Il Certificatore mantiene una copia di riferimento del registro dei certificati inaccessibile dall'esterno: questa aggiorna in tempo reale la copia operativa, accessibile da parte degli utenti con protocollo LDAP.

### 1.2. 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 1.1. del presente capitolo.

## M. Modalità di protezione della riservatezza

Le misure di sicurezza per la protezione dei dati personali sono conformi alle misure minime previste dal DLGS196/03.

## 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 capitolo 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/CSL; 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/CSL. 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

### 1.1. 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.

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

I sistemi di marcatura temporale del Certificatore sono sincronizzati con l'*I.N.RI.M. - Istituto Nazionale di Ricerca Metrologica* di Torino (già *Istituto Elettrotecnico Nazionale Galileo Ferraris*) per la rilevazione sicura dell'ora. Questa funzionalità viene realizzata da un software specifico installato su ogni server che, mediante il protocollo Network Time Protocol (di seguito NTP), si collega al server remoto configurato.
L'NTP è uno dei metodi più accurati e flessibili per distribuire l'informazione di tempo e di data sulla rete Internet. Esso permette di mantenere sincronizzati tra loro computer collegati tramite reti locali, metropolitane o addirittura mondiali (Internet) utilizzando una struttura di tipo gerarchico a piramide.
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 sono sincronizzati, attraverso un generatore di codice di data, dai campioni atomici a fascio di cesio utilizzati per generare la 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.
Il software installato presso il Certificatore si collega al server remoto ad intervalli regolari di tempo e, dopo aver ottenuto l'ora corrente, provvede a correggere il clock della macchina locale mediante sofisticati algoritmi.

I riferimenti temporali apposti dalle applicazioni sono stringhe in formato data (GG/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 all'art. 51 del DPCM.
Ogni registrazione effettuata sul giornale di controllo contiene un riferimento temporale che, essendo generato con la modalità qui descritta, è opponibile a terzi (art. 62 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 (come previsto dall'art. 21 comma 8 e 15 della Deliberazione CNIPA n. 45 del 21 maggio 2009), possono essere verificati utilizzando il software Acrobat Reader 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.

### 1.1. 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 Servizio 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 la digitazione combinata della password generata dal dispositivo di strong authentication e del Codice Personale.
Le firme digitali così generate sono conformi ai requisiti previsti per gli algoritmi di firma dall'art. 4 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.

### 1.2. Modalità di Firma nell'ambito dell'attività in sede

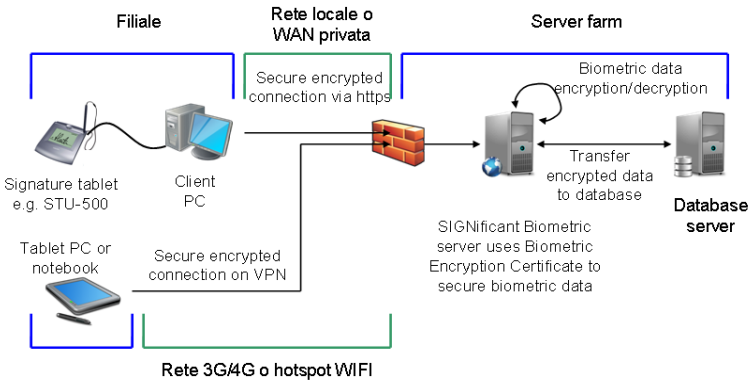
Il Titolare, al momento della firma, si troverà nei locali nei quali UniCredit (o altra Società del Gruppo) svolge la propria attività in sede al cospetto del personale incaricato, che lo avrà identificato.
A seguito del riconoscimento, il Titolare dovrà poter esaminare il documento e avviare la procedura 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, inserendo 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.

### 1.3. 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, inserendo 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.

### 1.4. Protezione dei dati

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




## S. Riferimenti Tecnici

| | |
|---|---|
| *ETSI TS 101 733* | ETSI TS 101 733 V1.4.0 "Electronic Signatures and Infrastructure (ESI): Electronic Signature Formats" (2002-09)" |

| | |
|---|---|
| *ETSI TS 102 023* | Deliverable ETSI TS 102 023 "Policy requirements for time-stamping authorities" - April 2002 |
| *HASH* | Funzione che prende in input una stringa di lunghezza variabile e ritorna una stringa di lunghezza fissa |
| *ISO/IEC 9594-8 2001:(E)* | Information Technology – Open Systems Interconnection – The Directory: Authentication 01/08/2001 Framework; ITU - T Recommendation X.509 (2001) ISO/IEC 9594-8 |
| *LDAP* | Lightweight Directory Access Protocol |
| *OID* | Object Identifier, sequenza di numeri, registrata secondo la procedura definita dallo standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia |
| *RFC 1305* | Network Time Protocol (Version 3) Specification, Implementation |
| *RFC 5280* | RFC 5280 (2002), "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" |
| *RFC 3161* | RFC 3161 (2001), "Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)" |
| *RFC 2527* | RFC 2527 (1999), "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" |
| *RFC 3039* | RFC 3039 (2001) Internet X.509 Public Key Infrastructure Qualified Certificates Profile |
| *URL* | Uniform Resource Locator |