
 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

**Certificatore Accreditato Postecom S.p.A.**


**Servizio Postecert Firma Digitale**

**Manuale Operativo**


 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## Indice


<b>SEZIONE I – INFORMAZIONI GENERALI.....</b>	<b>4</b>
<b>DEFINIZIONI .....</b>	<b>5</b>
INTRODUZIONE .....	7
PREMESSA.....	7
CONTESTO NORMATIVO .....	7
<b>DATI IDENTIFICATIVI DEL CERTIFICATORE.....</b>	<b>9</b>
CALL CENTER .....	9
<b>MANUALE OPERATIVO .....</b>	<b>10</b>
MODIFICHE INTRODOTTE RISPETTO ALLE EMISSIONI PRECEDENTI .....	10
RESPONSABILE DEL MANUALE OPERATIVO .....	10
<b>PROTEZIONE DEI DATI PERSONALI.....</b>	<b>12</b>
<b>TARIFFE.....</b>	<b>13</b>
<b>SEZIONE II – OBBLIGHI E RESPONSABILITÀ.....</b>	<b>14</b>
<b>OBBLIGHI .....</b>	<b>15</b>
OBBLIGHI DEL CERTIFICATORE .....	15
OBBLIGHI DEL TITOLARE .....	16
OBBLIGHI DEI RICHIEDENTI LA VERIFICA DELLE FIRME .....	17
OBBLIGHI DEL TERZO INTERESSATO .....	18
<b>RESPONSABILITÀ.....</b>	<b>20</b>
LIMITAZIONI ED INDENNIZZI .....	20
<b>SEZIONE III – CARATTERISTICHE E CICLO DI VITA DEI CERTIFICATI QUALIFICATI.....</b>	<b>22</b>
<b>CARATTERISTICHE GENERALI.....</b>	<b>23</b>
TIPOLOGIE DI CERTIFICATI QUALIFICATI .....	23
INFORMAZIONI CONTENUTE NEL CERTIFICATO QUALIFICATO .....	24
MODALITÀ CON CUI SI INDICA UN CERTIFICATO QUALIFICATO .....	24
VALIDITÀ DEL CERTIFICATO .....	24
<b>CICLO DI VITA DEI CERTIFICATI QUALIFICATI .....</b>	<b>26</b>
MODALITÀ DI IDENTIFICAZIONE E REGISTRAZIONE DEGLI UTENTI .....	26
ULTERIORI MODALITÀ DI IDENTIFICAZIONE E REGISTRAZIONE DEGLI UTENTI .....	28
MODALITÀ DI GENERAZIONE DELLE CHIAVI PER LA CREAZIONE E LA VERIFICA DELLA FIRMA.....	30
MODALITÀ DI EMISSIONE DEI CERTIFICATI.....	30
REVOCA E SOSPENSIONE DEI CERTIFICATI QUALIFICATI.....	31

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

RINNOVO DEL CERTIFICATO QUALIFICATO.....	36
<b>REGISTRO DEI CERTIFICATI .....</b>	<b>37</b>
MODALITÀ DI GESTIONE DEL REGISTRO DEI CERTIFICATI .....	37
MODALITÀ DI ACCESSO AL REGISTRO DEI CERTIFICATI .....	37
<b>SEZIONE IV – PROCEDURE OPERATIVE PER LA FIRMA E LA VERIFICA.....</b>	<b>38</b>
<b>MODALITÀ OPERATIVE PER LA GENERAZIONE E LA VERIFICA DELLE FIRME.....</b>	<b>39</b>
GENERAZIONE DELLA FIRMA.....	39
SISTEMA DI VERIFICA DELLE FIRME QUALIFICATE.....	40
FORMATO DEI DOCUMENTI INFORMATICI.....	41
<b>SEZIONE V – GESTIONE DELLE CHIAVI DI CERTIFICAZIONE E DI MARCATURA TEMPORALE ..</b>	<b>43</b>
<b>CHIAVI DI CERTIFICAZIONE.....</b>	<b>44</b>
GENERAZIONE DELLE CHIAVI DI CERTIFICAZIONE.....	44
REVOCA DEI CERTIFICATI RELATIVI A CHIAVI DI CERTIFICAZIONE.....	44
SOSTITUZIONE DELLE CHIAVI DI CERTIFICAZIONE .....	45
<b>CHIAVI DI MARCATURA TEMPORALE.....</b>	<b>46</b>
GENERAZIONE DELLE CHIAVI DI MARCATURA TEMPORALE.....	46
REVOCA DEI CERTIFICATI RELATIVI A CHIAVI DI MARCATURA TEMPORALE .....	46
SOSTITUZIONE DELLE CHIAVI DI MARCATURA TEMPORALE .....	46
<b>SEZIONE VI – MODALITÀ PER L’APPOSIZIONE E LA DEFINIZIONE DEL RIFERIMENTO</b>	
<b>TEMPORALE .....</b>	<b>47</b>
<b>RIFERIMENTO TEMPORALE .....</b>	<b>48</b>
<b>MARCATURA TEMPORALE.....</b>	<b>49</b>
MODALITÀ DI RICHIESTA DEL SERVIZIO DI MARCATURA TEMPORALE.....	50
VALIDITÀ DELLA MARCA TEMPORALE .....	50
<b>SEZIONE VII – UFFICI DELEGATI – VERIFICHE ISPETTIVE PERIODICHE .....</b>	<b>51</b>

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## SEZIONE I – INFORMAZIONI GENERALI


 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## Definizioni


Di seguito si riportano le definizioni specifiche del presente Manuale Operativo.

In aggiunta valgono le definizioni previste nella normativa vigente.

<p><b><u>Appartenenti all'Organizzazione:</u></b> dipendenti e/o associati a favore dei quali l'Organizzazione richiede l'emissione di un certificato qualificato</p>
<p><b><u>Certificazione:</u></b> il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto Titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave ed il termine di scadenza del relativo certificato</p>
<p><b><u>Chiave privata:</u></b> elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto Titolare, mediante il quale si appone la firma digitale sul documento informatico</p>
<p><b><u>Chiave pubblica:</u></b> elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal Titolare delle chiavi asimmetriche</p>
<p><b><u>Coppia di chiavi:</u></b> coppia di chiavi asimmetriche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi crittografici</p>
<p><b><u>CRL:</u></b> Vedi Lista di revoca dei certificati</p>
<p><b><u>CSL:</u></b> Vedi Lista di sospensione dei certificati</p>
<p><b><u>Dati per la creazione della firma:</u></b> l'insieme dei codici personali e delle chiavi crittografiche private, utilizzate dal firmatario per creare una firma elettronica</p>
<p><b><u>Destinatario:</u></b> destinatario di un documento e/o di una evidenza informatica firmati digitalmente</p>
<p><b><u>DigitPA (ex-CNIPA):</u></b> Organismo di controllo istituito dal Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri</p>
<p><b><u>Firma Elettronica Qualificata:</u></b> un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;</p>
<p><b><u>Firma Digitale:</u></b> un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e 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</p>
<p><b><u>Lista di revoca dei certificati (CRL):</u></b> lista firmata digitalmente, tenuta ed aggiornata dal Certificatore, contrassegnata da un riferimento temporale, contenente i certificati dalla stessa emessi e revocati</p>
<p><b><u>Lista di sospensione dei certificati (CSL):</u></b> lista firmata digitalmente, tenuta ed aggiornata dal Certificatore, contrassegnata da un riferimento temporale, contenente i certificati dalla stessa emessi e sospesi</p>
<p><b><u>Manuale Operativo:</u></b> documento pubblico depositato presso DigitPA che definisce le procedure applicate dal Certificatore nello svolgimento della propria attività</p>

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

<p><b>Marca temporale:</b> il riferimento temporale che consente la validazione temporale, ossia l'attribuzione di ora e data certa opponibile a terzi</p>
<p><b>OID (Object Identifier Number):</b> numero identificativo univoco di un documento in ambito internazionale</p>
<p><b>Organizzazione:</b> comunità organizzate di utenti (quali ad esempio aziende, società, ordini professionali, associazioni di categoria ecc.) che stipulano accordi con il Certificatore per il rilascio di certificati di firma digitale ai propri dipendenti e/o associati</p>
<p><b>Referente:</b> la persona delegata dall'Organizzazione alla gestione dei rapporti con il Certificatore, alla richiesta di registrazione degli appartenenti all'Organizzazione, nonché all'inoltro della richiesta di revoca o sospensione dei certificati</p>
<p><b>Registro dei certificati:</b> registro contenente i certificati emessi dal Certificatore, la lista dei certificati revocati e la lista dei certificati sospesi, accessibili telematicamente</p>
<p><b>Revoca del certificato:</b> operazione con cui il Certificatore annulla la validità del certificato da un dato momento, non retroattivo, in poi</p>
<p><b>Richiedente:</b> soggetto che richiede i servizi di Certificazione e che diventa Titolare una volta emesso il certificato qualificato</p>
<p><b>Riferimento temporale:</b> informazione, contenente data e ora, che viene associata ad un documento informatico</p>
<p><b>Sospensione del certificato:</b> operazione con cui il Certificatore sospende la validità del certificato per un determinato periodo di tempo</p>
<p><b>Terzo Interessato:</b> persona fisica o giuridica che da il consenso, in conformità alle norme, al rilascio di certificati qualificati nei quali sia riportata l'appartenenza ad una specifica organizzazione ovvero eventuali poteri di rappresentanza o titoli e cariche rivestite. Ha il diritto/dovere di richiedere la revoca o sospensione del certificato nel caso mutino i requisiti in base ai quali lo stesso è stato rilasciato</p>
<p><b>Titolare di firma:</b> soggetto a favore del quale è stato emesso un certificato qualificato nel rispetto della normativa vigente e del presente Manuale Operativo</p>
<p><b>TSA:</b> la Time Stamping Authority del Certificatore per il rilascio di marche temporali</p>
<p><b>Validità del Certificato:</b> efficacia ed opponibilità della chiave pubblica e dei dati contenuti nel certificato stesso</p>
<p><b>Ufficio Delegato:</b> Ufficio che svolge, per conto del Certificatore e secondo modalità da questo definite, le attività individuate e descritte nel presente Manuale. Nel corso del presente Manuale Operativo per Ufficio Delegato si intende: Ufficio di Poste Italiane abilitato al servizio; Ufficio appartenente ad una Organizzazione con la quale il Certificatore ha stipulato un accordo di servizio; gli uffici o il personale del Certificatore allo scopo deputati</p>

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## Introduzione

### Premessa

Il Manuale Operativo definisce le procedure applicate dal Certificatore nello svolgimento della propria attività di certificazione ed è rivolto a tutti i soggetti che entrano in relazione con il Certificatore:

- Titolare;
- Terzo Interessato;
- Destinatario, ovvero quanti accedono per la verifica della firma.

All'interno del presente documento, per i soggetti sopra elencati, sono definiti gli obblighi e le corrispondenti responsabilità.

Il Manuale Operativo riporta i dati identificativi del Certificatore e del Responsabile dello stesso.

I certificati qualificati emessi da Postecom, nel rispetto di quanto previsto nel presente Manuale Operativo e della normativa richiamata nel seguito, sono validi ai fini dell'apposizione della Firma Digitale e Firma Elettronica Qualificata su documenti informatici opionibili ai terzi.


I dispositivi sicuri per la generazione della Firma Digitale scelti dal certificatore sono i medesimi dispositivi previsti dalle regole tecniche per la Firma Elettronica Qualificata.

All'interno del presente Manuale Operativo, quindi, Firma Elettronica Qualificata e Firma Digitale sono da considerarsi equivalenti.


### Contesto normativo

Il Manuale Operativo è conforme a quanto previsto dalla legge italiana e in particolare:

<b>D.Lgs 82/2005</b>	Decreto Legislativo 7 marzo 2005, n° 82 e successive modificazioni <i>Codice dell'amministrazione digitale</i>
<b>D.Lgs 159/2006</b>	Decreto Legislativo 4 aprile 2006, n° 159 <i>Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n.82, recante codice dell'amministrazione digitale</i>
<b>DPCM 30/03/2009</b>	Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 <i>Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici.</i>
<b>CNIPA 45/2009</b>	Deliberazione CNIPA 21 maggio 2009, n° 45 e successive modificazioni <i>Regole per il riconoscimento e la verifica del documento informatico</i>
<b>CNIPA/CR/48</b>	Circolare CNIPA 6 settembre 2005, n° CNIPA/CR/48


 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

	<i>Modalità per presentare la domanda di iscrizione nell'elenco pubblico dei certificatori di cui all'articolo 28, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445</i>
<b>D.Lgs 196/2003</b>	Decreto Legislativo 30 giugno 2003, n° 196 <i>Codice in materia di protezione dei dati personali</i>

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## Dati identificativi del Certificatore

<b>Denominazione e Ragione sociale</b>	<b>Postecom S.p.A.</b>
Rappresentante legale	Dott. Vincenzo Pompa
Sede legale	Viale Europa n.175, 00144 Roma
Telefono	+39 06 59581
Sede operativa	Viale Europa n.175, 00144 Roma
Telefono	+39 06 59581
Indirizzo E-mail	<a href="mailto:postecertfirmadigitale@postecert.it">postecertfirmadigitale@postecert.it</a>
Indirizzo Internet	<a href="http://postecert.poste.it">http://postecert.poste.it</a>
Call Center	803.160 codice 3 da rete fissa (gratuito) o al numero 199.100.160 da rete mobile (costi a seconda dell'operatore), dal lunedì al venerdì (dalle 9:00 alle 20:00) ed il sabato (dalle 9:00 alle 15:00)

 GruppoPoste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## Manuale Operativo

### Modifiche introdotte rispetto alle emissioni precedenti

Versione n.	Pagina n.	Motivo della revisione	Data
1.0		Versione definitiva interna	21 febbraio 2000
1.1	13, 22, 23	Ridefinizione aspetti organizzativi	11 aprile 2000
2.0	tutte	Ridefinizione dei contenuti del Manuale Operativo	18 giugno 2001
3.0		Aggiornati riferimenti normativi	20 dicembre 2005
3.1	8,11,23	Aggiunto riferimento Decreto Legislativo 4 aprile 2006, n. 159 Aggiunto OID della nuova chiave di certificazione, inserita modalità di verifica CRL/CSL tramite OCSP, inserito il termine di 20 anni per la conservazione della documentazione prevista per il rilascio dei certificati qualificati	14 maggio 2006
3.2	varie	Aggiornati riferimenti normativi Aggiornate modalità di riconoscimento utenti Modificate modalità di verifica di documento firmato digitalmente	26 luglio 2011
3.3	varie	Inserita variazione dati Rappresentante Legale Inserita indicazione sul mantenimento del certificato revocato o sospeso nella lista CRL/CRL anche successivamente alla naturale scadenza Inserita indicazione valori economici polizza assicurativa	06 dicembre 2011

### Responsabile del Manuale Operativo


Postecom S.p.A. è responsabile della definizione, pubblicazione ed aggiornamento del presente documento.

Nel seguito sono indicati i riferimenti da contattare per questioni riguardanti il presente documento ed il Servizio Postecert Firma Digitale:

Postecom S.p.A.

Responsabile Servizio Postecert Firma Digitale

Viale Europa 190

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

00144 – Roma –

Indirizzo PEC: [postecertfirmadigitale@postecert.it](mailto:postecertfirmadigitale@postecert.it)

Il presente Manuale Operativo è identificato attraverso il numero di versione 3.3. Il corrispondente file in formato elettronico, conservato presso i locali del Certificatore e depositato presso DigitPA, è identificabile dal nome "MOP01.pdf" ed è consultabile per via telematica all'indirizzo Internet: <http://postecert.poste.it> nella sezione "Manuali Operativi"


Questo manuale si riferisce ai servizi di:

- Certificazione chiavi pubbliche;
- Generazione di marche temporali a richiesta per documenti elettronici.

Questo Manuale Operativo è referenziato dai seguenti OID (Object Identifier Number):

- 1.3.76.11.1.2.1.1. e 2.5.29.32.0. – Policy per servizi di certificazione;
- 1.3.76.11.1.2.2.1. – Policy per certificati di marcatura temporali;
- 1.3.76.11.1.2.3.1. – Policy per certificati qualificati;
- 1.3.76.11.1.2.3.2. – Policy per certificati qualificati di firma automatica.


A tale proposito si evidenzia che a partire dal sito <http://postecert.poste.it>, Firma Digitale, Documentazione e modulistica, viene reso disponibile il documento "Guida alla comprensione degli OID presenti nei certificati rilasciati da Postecom S.p.A.".

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## Protezione dei dati personali


I dati memorizzati su database sono protetti con politiche di autorizzazione basate su policy per l'accesso degli utenti. I meccanismi adottati nell'esecuzione delle attività che seguono sono conformi alle misure minime di sicurezza per il trattamento dei dati personali emanate con il D.Lgs 196/2003; in particolare consentono:

- l'individuazione dei responsabili e degli incaricati;
- l'assegnazione di codici identificativi;
- la protezione degli elaboratori;
- l'idonea modalità di designazione degli incaricati del trattamento.


 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## Tariffe

Le tariffe applicate da Postecom sono pubblicate on line all'indirizzo <http://postecert.poste.it> area Firma Digitale.

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## SEZIONE II – OBBLIGHI E RESPONSABILITÀ

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011


## Obblighi

Chiunque intenda utilizzare un sistema di chiavi asimmetriche o di firma elettronica qualificata, è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

### Obblighi del Certificatore

Nello svolgimento della sua attività il Certificatore:

- adotta tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
- si attiene alle normativa vigente in materia di Firma Digitale e Firma Elettronica Qualificata;
- genera e pubblica, nel proprio registro dei certificati, un certificato elettronico per ciascuna delle chiavi di firma , utilizzate da DigitPA per la sottoscrizione dell'elenco pubblico dei certificatori accreditati;
- rende accessibile, per via telematica, la copia della lista, sottoscritta da DigitPA, dei certificati relativi alle chiavi di Certificazione di cui al DPCM 30/03/2009;
- predispone su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione, in particolare i termini e le condizioni relative all'uso dei certificati, la procedure di rilascio, le procedure di reclamo e di risoluzione delle controversie;
- informa i richiedenti sulla procedura di certificazione, sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
- si accerta dell'autenticità della richiesta di certificazione;
- identifica con certezza la persona che fa richiesta della registrazione ai fini della certificazione;
- nel caso di chiavi generate dal certificatore, assicura la consegna al legittimo titolare; nel caso di chiavi non generate dal certificatore, verifica il possesso della chiave privata da parte del titolare ed il corretto funzionamento della coppia di chiavi;
- genera la coppia di chiavi mediante apparati e procedure che assicurano, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e la robustezza della coppia generata, nonché la segretezza della chiave privata;
- registra, nel giornale di controllo, l'emissione dei certificati qualificati, generazione specificando il riferimento temporale relativo alla registrazione;
- non copia, né conserva le chiavi private di sottoscrizione dei Titolari;
- non si rende depositario di dati per la creazione della firma del titolare nel caso il dispositivo di firma sia rilasciato fisicamente al Titolare, in ogni caso gestisce le modalità per le quali almeno uno dei dati necessari per la creazione della firma sia sotto il controllo del Titolare che attiva la procedura di firma;
- adotta le misure di sicurezza per il trattamento dei dati personali ai sensi del DLgs 196/2003;

 GruppoPoste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011


- procede alla pubblicazione della revoca e della sospensione del certificato qualificato, in caso di richiesta da parte del Titolare o del terzo dal quale derivino i poteri di quest'ultimo, di perdita del possesso o della compromissione del dispositivo di firma, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del Titolare, di sospetti abusi o falsificazioni;
- garantisce un servizio di revoca e sospensione dei certificati elettronici, sicuro e tempestivo nonché garantisce il funzionamento efficiente, puntuale e sicuro degli elenchi dei certificati di firma emessi, sospesi e revocati;;
- tiene registrazione per venti anni, anche in forma elettronica, delle informazioni relative al certificato qualificato;
- assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati;
- utilizza sistemi affidabili per la gestione del registro dei certificati, con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal Titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza;
- fornisce o indica almeno un sistema che consenta di effettuare la verifica delle firme digitali;
- fornisce almeno in sistema che consenta la generazione delle firme digitali;
- comunica l'avvenuta revoca o sospensione del certificato al titolare e all'eventuale terzo interessato;
- rende disponibile ai propri titolari un sistema di validazione temporale conforme alle disposizioni di cui al DPCM 30/03/2009.

## Obblighi del Titolare

Il Titolare è tenuto ad assicurare la custodia dei dati per la creazione della firma e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri. E' altresì tenuto ad utilizzare personalmente il dispositivo di firma.

Il Titolare della chiave deve inoltre:

- prendere visione del presente Manuale Operativo prima di inoltrare la richiesta di certificazione;
- garantire la veridicità di tutti i dati personali comunicati in occasione della registrazione ed identificazione, assumendo la responsabilità di cui all'art. 495-bis del codice penale, e impegnarsi a fornire tutte le informazioni richieste dal Certificatore;
- fornire tutte le informazioni necessarie alla fornitura del servizio richieste dal Certificatore garantendone, sotto la propria responsabilità, l'attendibilità ai sensi del DPR 445/2000,


 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

- comunicare al Certificatore ogni variazione dei dati forniti in fase di registrazione;
- generare, ove sia lui a farlo, la coppia di chiavi, all'interno del dispositivo sicuro per la creazione della firma rilasciato o indicato dal Certificatore;
- assicurare la custodia del dispositivo di firma e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma;
- conservare con la massima diligenza i codici riservati ricevuti dal Certificatore, al fine di garantirne l'integrità e la massima riservatezza;
- conservare le informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave;
- utilizzare esclusivamente il dispositivo sicuro per la creazione della firma fornito dal certificatore, ovvero un dispositivo scelto tra quelli indicati dal certificatore stesso;
- non apporre firme digitali su documenti contenenti macro istruzioni o codici eseguibili che ne modifichino gli atti o i fatti negli stessi rappresentati e che ne renderebbero, quindi, nulla l'efficacia;
- mantenere in modo esclusivo la conoscenza o la disponibilità di almeno uno dei dati per la creazione della firma;
- garantire la protezione della segretezza e la conservazione del dispositivo e/o dei codici utilizzati per l'attivazione della procedura di firma ed impegnarsi a richiedere l'immediata revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi di firma di cui abbia perduto il possesso o difettosi, o qualora abbia il ragionevole dubbio che i dati e/o i codici possano essere utilizzati abusivamente da persone non autorizzate;
- adottare le principali regole di comportamento per la sicurezza della propria postazione;
- inoltrare, con le modalità indicate dal Certificatore, la richiesta di revoca munita della sottoscrizione e specificandone la motivazione;
- inoltrare, con le modalità indicate dal Certificatore, la richiesta di sospensione munita della sottoscrizione e specificando la motivazione;;
- sporgere denuncia, in caso di smarrimento o sottrazione del dispositivo di firma, alle autorità competenti;
- presentarsi presso l'Ufficio Delegato o uffici del Certificatore, a seguito della richiesta di sospensione immediata del certificato, e richiedere per iscritto la revoca o la riattivazione dello stesso.

E' vietata la duplicazione della chiave privata e dei dispositivi che la contengono.

Non è consentito l'uso di una coppia di chiavi per funzioni diverse da quelle previste dalla sua tipologia.

Obblighi dei richiedenti la verifica delle firme

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

I soggetti che verificano la firma digitale apposta da un Titolare sono tenuti ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri. In particolare i destinatari devono verificare:

- la validità del certificato contenente la chiave pubblica del firmatario del documento;
- l'assenza del certificato dalle Liste di Revoca e Sospensione (CRL) dei certificati;
- che il certificato del Titolare sia verificabile con un certificato di certificazione di Postecom, presente nell' Elenco Pubblico mantenuto dal DigitPA;
- l'esistenza di eventuali limitazioni all'uso del certificato utilizzato dal Titolare, o di un eventuale valore limite di negoziazione per il quale può essere usato il certificato stesso;
- la presenza, nel documento verificato, di eventuali macro istruzioni o codici eseguibili che ne modifichino gli atti o i fatti negli stessi rappresentati e che renderebbero, quindi, nulla la sottoscrizione del documento;
- che siano adottate le principali regole di comportamento per la sicurezza della propria postazione;
- che nel certificato sia presente l'identificativo (OID), relativo al certificato qualificato come indicato nel presente Manuale Operativo;
- che la tipologia di uso della chiave del certificato sia esclusivamente "Non Ripudio".

## Obblighi del Terzo Interessato


Il Terzo Interessato deve adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

Il Terzo Interessato, sia esso persona fisica o organizzazione (impresa, associazione di categoria, enti, ecc.), provvede, mediante il Referente e previo esplicito consenso dei richiedenti, a raccogliere i dati necessari alla registrazione, organizzandoli secondo un tracciato dati precedentemente ricevuto dal Certificatore.


Il Terzo Interessato ha, inoltre, l'obbligo di richiedere la sospensione o revoca dei certificati ogni qualvolta vengano meno i requisiti in base ai quali il certificato è stato rilasciato. In caso di cessazione o modifica delle qualifiche o del titolo inserite nel certificato su richiesta del terzo interessato, la richiesta di revoca è inoltrata non appena il terzo venga a conoscenza della variazione di stato.

A titolo esemplificativo si riportano le seguenti circostanze:

- variazione o cessazione dei poteri di rappresentanza;
- variazione di ruoli e qualifiche interne;
- cessazione del rapporto di dipendenza;
- variazione dei dati identificativi (es. denominazione sociale, sede legale, etc.) o cessazione dell'organizzazione;
- ed ogni altro dato rilevante ed incidente ai fini dell'uso del certificato.

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

La richiesta di revoca o sospensione, da parte del Terzo Interessato, deve essere inoltrata al Certificatore munita di sottoscrizione e corredata di documentazione giustificativa.

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## Responsabilità

Il Certificatore è responsabile, verso i Titolari, per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività di Certificatore Accreditato.

Il Certificatore non assume responsabilità per l'uso improprio dei certificati.

Le limitazioni agli indennizzi stabilite dal Certificatore sono riportate anche nelle condizioni generali del servizio accettate dal cliente.

Postecom, in qualità di Certificatore, mette a disposizione, secondo modalità specifiche di ogni singola procedura operativa ed in relazione alle componenti del kit effettivamente acquisito, l'insieme coerente e testato della smart card con il certificato qualificato a bordo e del relativo lettore, comprensivi delle librerie e dell'applicativo software per l'apposizione e la verifica di firme qualificate.

Sui propri dispositivi, Postecom garantisce l'aderenza a quanto previsto dalla normativa vigente ed il loro funzionamento con i certificati qualificati rilasciati.

### *Art. 30 CAD Responsabilità del Certificatore*


Il certificatore che rilascia al pubblico un certificato qualificato o che garantisce al pubblico l'affidabilità del certificato è responsabile, se non prova d'aver agito senza colpa o dolo, del danno cagionato a chi abbia fatto ragionevole affidamento:

- a. sull'esattezza e sulla completezza delle informazioni necessarie alla verifica della firma in esso contenute alla data del rilascio e sulla loro completezza rispetto ai requisiti fissati per i certificati qualificati;
- b. sulla garanzia che al momento del rilascio del certificato il firmatario detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato;
- c. sulla garanzia che i dati per la creazione e per la verifica della firma possano essere usati in modo complementare, nei casi in cui il certificatore generi entrambi;
- d. sull'adempimento degli obblighi a suo carico previsti dall'articolo 32.

2. Il certificatore che rilascia al pubblico un certificato qualificato è responsabile, nei confronti dei terzi che facciano affidamento sul certificato stesso, dei danni provocati per effetto della mancata o non tempestiva registrazione della revoca o non tempestiva sospensione del certificato, secondo quanto previsto dalle regole tecniche di cui all'articolo 71, salvo che provi d'aver agito senza colpa.


3. Il certificato qualificato può contenere limiti d'uso ovvero un valore limite per i negozi per i quali può essere usato il certificato stesso, purché i limiti d'uso o il valore limite siano riconoscibili da parte dei terzi e siano chiaramente evidenziati nel certificato secondo quanto previsto dalle regole tecniche di cui all'articolo 71. Il certificatore non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite.

## Limitazioni ed indennizzi


 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

Il Certificatore ha stipulato un contratto assicurativo, per la copertura dei rischi dell'attività e dei danni causati a terzi, il cui testo è stato inviato al DigitPA. Si riportano i valori economici:

- 258.228,45 euro per singolo sinistro relativamente a persone giuridiche;
- 51.645,69 euro per singolo sinistro relativamente a persone fisiche;
- 1.032.913,80 euro per annualità assicurativa.

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## **SEZIONE III – CARATTERISTICHE E CICLO DI VITA DEI CERTIFICATI QUALIFICATI**

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## Caratteristiche generali

### Tipologie di certificati qualificati

I Titolari di un certificato qualificato sono suddivisi nelle seguenti tipologie:

- Persona fisica.
- Persona fisica titolare di qualifica professionale (appartenenza ad ordini o collegi professionali, qualifica di pubblico ufficiale, iscrizione ad albi o il possesso di altre abilitazioni professionali). Il certificato viene rilasciato previa presentazione della documentazione comprovante la qualifica professionale richiesta.
- Persona fisica appartenente ad una Organizzazione, titolare di un eventuale ruolo/funzione all'interno dell'Organizzazione di appartenenza. Il certificato viene rilasciato previa richiesta dell'Organizzazione di appartenenza, che ricopre il ruolo di terzo interessato.

### Certificati per persona fisica

In questo caso, il Richiedente dovrà fornire i soli dati necessari ai fini della registrazione e identificazione, nelle modalità previste da Postecom.


### Certificati per persona fisica titolare di qualifica professionale

Il Richiedente dovrà fornire, in aggiunta ai dati anagrafici per l'identificazione, ed i dati per la registrazione, anche la documentazione comprovante la qualifica di cui si richiede l'inserimento all'interno del certificato qualificato. La documentazione, attestante la qualifica di cui si richiede l'inserimento nel certificato qualificato, va presentata in fase di riconoscimento e non dovrà essere anteriore di oltre 30 giorni rispetto alla data della richiesta del Servizio.

### Certificati per appartenente ad una Organizzazione

Il rilascio di certificati qualificati a soggetti in qualità di appartenenti ad una Organizzazione o aventi rapporti con una Organizzazione, può avvenire secondo due modalità:

- **CASO 1:** il Certificatore e l'Organizzazione sottoscrivono una Convenzione: nell'ambito della Convenzione viene individuato il "Referente" dell'Organizzazione, che assume il compito di raccogliere i dati identificativi dei Richiedenti, compilare le richieste di emissione dei certificati e inviarle al Certificatore nelle modalità previste da Postecom.
- **CASO 2:** il Richiedente fornisce, oltre ai dati identificativi necessari, un documento ufficiale (redatto secondo il modulo fornito da Postecom), comprovante il possesso dei requisiti che si richiede vengano riportati all'interno del certificato qualificato e autorizzazione da parte dell'Organizzazione all'inserimento dei medesimi nel certificato qualificato. La documentazione

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

da presentare non dovrà essere anteriore di oltre 30 giorni alla data della richiesta di registrazione.

## Informazioni contenute nel certificato qualificato

Il certificato qualificato contiene le informazioni dichiarate, alla data del rilascio, dal Richiedente e eventualmente dal Terzo Interessato, al Certificatore, nelle modalità previste da Postecom.

Oltre ai dati anagrafici identificativi necessari, il certificato qualificato può contenere le seguenti informazioni, se pertinenti allo scopo per il quale il certificato è richiesto:

- eventuali limiti d'uso del certificato;
- eventuali qualifiche specifiche del Titolare, quali l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza.

Nel caso di certificati rilasciati agli appartenenti ad un'Organizzazione, su richiesta di quest'ultima, è indicato:

- l'appartenenza del Titolare all'Organizzazione;
- eventuale ruolo del Titolare nell'ambito di tale Organizzazione.

## Modalità con cui si indica un certificato qualificato

L'indicazione che il certificato elettronico è un certificato qualificato è presente nel campo Certificate Policy, con l'inserimento dell'identificativo (OID) relativo al certificato qualificato.

Ai certificati qualificati richiesti dai Titolari per l'apposizione di firme automatiche, Postecom attribuisce uno specifico OID riportato nel medesimo paragrafo sopra citato, al fine di permettere l'identificazione di tali tipologie di firme.


In coerenza alla normativa vigente, il certificato qualificato, contiene inoltre l'attributo **qcStatements**, identificate nel documento ETSI TS 101 862 come segue:

- 1) id-etsi-qcs-QcCompliance (OID: 0.4.0.1862.1.1);
- 2) id-etsi-qcs-QcLimitValue (OID: 0.4.0.1862.1.2) – presente se sono applicabili limiti nelle negoziazioni;
- 3) id-etsi-qcs-QcRetentionPeriod (OID: 0.4.0.1862.1.3) – il valore indicato all'interno dei certificati è pari "20";
- 4) id-etsi-qcs-QcSSCD (OID: 0.4.0.1862.1.4)


Inoltre Postecom, a partire dal sito [postecert.poste.it](http://postecert.poste.it) mette a disposizione il documento "Guida alla comprensione degli OID presenti nei certificati rilasciati da POSTECOM S.P.A.", che descrive le varie tipologie di certificato elettronico.

## Validità del certificato

L'inizio e la fine del periodo di validità delle chiavi sono contenute all'interno dei relativi certificati.

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

Il periodo di validità dei certificati qualificati è determinato in funzione della robustezza delle chiavi di creazione e verifica impiegate e dei servizi cui essi sono destinati. Detto periodo non eccede comunque i 5 anni.

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## Ciclo di vita dei certificati qualificati

### Modalità di identificazione e registrazione degli utenti

Le procedure per il rilascio di un certificato qualificato prevedono:

- che il Richiedente sia registrato presso il Certificatore,
- che il Richiedente venga identificato con certezza dal Certificatore o dai suoi delegati.

Le attività di identificazione e registrazione, oltre che svolte in maniera diretta dal personale del Certificatore, possono essere delegate a terzi che agiscono sotto il controllo e la responsabilità del Certificatore stesso.

Da questo punto in avanti sarà utilizzato il termine Ufficio Delegato con riferimento agli uffici abilitati al servizio di identificazione e registrazione. La funzione di Ufficio Delegato può essere svolta:

- ➔ dal personale del Certificatore;
- ➔ da uno degli Uffici di Poste Italiane, dislocato sul territorio nazionale, abilitato al servizio;
- ➔ da soggetti a cui Postecom delega l'attività di identificazione con un apposito accordo di servizio.

Il Richiedente, a seguito della registrazione, si reca presso un Ufficio Delegato portando con sé i documenti necessari all'identificazione, la documentazione contrattuale e di registrazione, l'eventuale ulteriore documentazione necessaria in relazione alla tipologia di certificato richiesto..

L'Operatore addetto all'identificazione ritira la documentazione presentata dal Richiedente e:


- ➔ controlla la validità del documento di identità prodotto sia in originale che in copia e verifica l'identità del richiedente;
- ➔ verifica la corrispondenza dei dati contenuti nelle copie con il documento in originale;
- ➔ verifica la completezza e la correttezza dei dati di registrazione.

L'Operatore, dopo aver compiuto le verifiche descritte:

- ➔ fa sottoscrivere, in duplice copia, il contratto al Richiedente, il quale, dopo averlo letto, lo firma per accettazione. Il Richiedente è tenuto a verificare puntualmente la correttezza delle informazioni di registrazione;
- ➔ firma e timbra le due copie del contratto;
- ➔ consegna una copia del contratto al Richiedente e trattiene l'altra.

Postecom tiene registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato dal momento della sua emissione per venti (20) anni al fine di fornire prova della certificazione nei casi previsti.

Nei casi in cui il richiedente il servizio non sia un privato ma un'Organizzazione (pubblica o privata) per gli appartenenti all'organizzazione medesima, il rilascio di certificati qualificati è oggetto di accordo tra il Certificatore e l'Organizzazione stessa.

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

Nell'ambito di tale accordo sono preventivamente individuate, sulla base delle specifiche esigenze dell'Organizzazione, nonché dei requisiti tecnici del Certificatore, le tipologie di certificati da emettere, le condizioni e le modalità di richiesta e di rilascio dei certificati.

L'organizzazione, per i titolari appartenenti all'organizzazione stessa, assume le seguenti responsabilità:

- fornire al Certificatore i dati dei Titolari dei certificati qualificati, dopo averli raccolti nel rispetto del DLvo 196/2003;
- comunicare al Certificatore tutte le variazioni nei dati dei Titolari e di richiedere la revoca dei certificati emessi a favore dei propri appartenenti, qualora venga a conoscenza della variazione delle informazioni contenute negli stessi..

In funzione delle specifiche modalità operative, la smart card potrà essere consegnata al Titolare contestualmente alla sua identificazione oppure successivamente.

### **Documenti richiesti ai fini dell'identificazione e registrazione**

L'identificazione del Richiedente avviene attraverso l'esibizione di uno dei seguenti documenti di riconoscimento:

- carta di identità
- Patente di guida
- Passaporto
- Tessere di riconoscimento purché munite di fotografia e di timbro, rilasciate da un'amministrazione dello stato


I suddetti documenti devono essere validi e presentati in originale, corredati della relativa fotocopia.

Il richiedente deve inoltre produrre gli estremi del codice fiscale rilasciato dall'autorità fiscale dello Stato di residenza del titolare o, in mancanza, di un analogo codice identificativo, quale ad esempio un codice di previdenza sociale o un codice identificativo generale. Nel caso di mancanza di detto codice si utilizzerà il numero del passaporto.

In caso di impossibilità di individuare un codice identificativo personale non sarà possibile proseguire l'iter di rilascio del dispositivo di firma.

Nel caso in cui il Richiedente desideri citare nel certificato la sussistenza di eventuali abilitazioni professionali o ruoli rivestiti, deve essere presentata prova del possesso della qualifica dichiarata, in conformità alle norme, disposizioni ed ordinamenti vigenti.

Il Richiedente assume la responsabilità della veridicità dei dati e dei documenti forniti per l'identificazione e registrazione.

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## Ulteriori modalità di identificazione e registrazione degli utenti

### Registrazione per gli utenti registrati al servizio di cui al DPCM 6/5/2009

Qualora l'utente sia stato precedentemente identificato ai sensi del Decreto del Presidente del Consiglio dei Ministri 6 maggio 2009 recante "Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini" e la richiesta di rilascio della firma avvenga all'interno del sistema Postacertificat@, successivamente all'autenticazione, a partire dal sito del servizio Postacertificat@, dell'utente attraverso le proprie credenziali personali, ai fini del rilascio del certificato di firma digitale basato su un certificato qualificato, farà fede l'identificazione effettuata tramite il Concessionario del servizio Postacertificat@, ai fini del rilascio della casella.

L'utente, successivamente alla sua autenticazione al sistema, confermerà i dati di registrazione e accetterà le Condizioni Generali del Servizio.

Il servizio di Firma Digitale per il rilascio di certificati di firma elettronica qualificata è conforme alle Regole Tecniche di cui al DPCM 30/03/2009 Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009, alle prescrizioni del presente Manuale Operativo e, in generale, alla normativa applicabile in tema di Firma Elettronica Qualificata e Firma Digitale.

### Registrazione per gli utenti che dispongono di Carta Nazionale dei Servizi


La richiesta di registrazione potrà – nei casi specifici previsti dal Certificatore – essere effettuata anche da utenti precedentemente identificati con la Carta Nazionale dei Servizi.

In questo caso l'identificazione si intende assolta in modalità telematica, essendo il titolare della CNS già stato identificato ai fini del rilascio di tale carta.

### Registrazione per gli utenti previo Dichiarazione sostitutiva dell'atto di notorietà

Il certificatore si riserva – in particolari contesti – di rendere disponibile una modalità di registrazione basata sull'identificazione effettuata da un Pubblico Ufficiale in base a quanto disposto dalle normative che disciplinano la loro attività, ivi comprese le disposizioni di cui al D.L. 3 Maggio 1991, n. 143 e successive modifiche ed integrazioni.

Nei casi previsti, l'utente che intende effettuare l'identificazione attraverso tale modalità dovrà recarsi presso il Pubblico Ufficiale munito di un documento di identità in corso di validità, del modulo di richiesta con annesse clausole contrattuali e della modulistica specifica messa a disposizione da Postecom (dichiarazione sostitutiva dell'atto di notorietà). Presso il Pubblico Ufficiale l'utente dovrà sottoscrivere la dichiarazione sostitutiva dell'atto di notorietà in cui dichiarerà di avere sottoscritto il modulo di richiesta al Servizio (contenente i dati anagrafici inseriti in fase di registrazione al servizio), assumendone le responsabilità riguardo la veridicità dei dati e contenuti nel modulo di richiesta, incluso il proprio codice fiscale. Tale dichiarazione dovrà essere compilata e sottoscritta anche dal Pubblico Ufficiale, nelle parti

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

di sua competenza, e dovrà essere trasmessa al Certificatore unitamente al Modulo di richiesta del servizio comprensivo delle clausole contrattuali.

### **Registrazione per gli utenti già riconosciuti per il rilascio dei servizi finanziari/bancari**

Nel caso in cui l'utente sia stato già identificato per il rilascio dei servizi finanziari e bancari rilasciati dal Gruppo Poste Italiane – Bancoposta – (e che all'interno di tale richiesta non sia esplicitamente richiamato il Servizio di Firma Digitale) in aderenza alla normativa anti riciclaggio e disponga di un dispositivo/codice personali, la fase di identificazione si intende assolta, e verrà utilizzata dal Certificatore ai fini del rilascio del certificato qualificato di firma digitale .

In tale caso i certificati rilasciati conterranno una limitazione d'uso riportanti il contesto di utilizzo nell'ambito dei servizi del Gruppo Poste Italiane

### **Delega alle Pubbliche Amministrazioni dell'attività di identificazione e registrazione**


Nel caso di Pubbliche Amministrazioni per le quali l'identità dei dipendenti sia riscontrabile in maniera certa e diretta da parte delle Amministrazioni in base ai propri processi di gestione del personale dipendente, le attività di identificazione e registrazione del personale dipendente possono essere delegate in toto all'amministrazione stessa che le esercita per il tramite del suo Referente/i.

In questo caso la specifica Convenzione tra il Certificatore Postecom ed la Pubblica Amministrazione (in qualità di terzo interessato ai sensi dell' articolo 32 del D.lgs 7 marzo 2005 n. 82), riporterà l'impegno dell'Amministrazione stessa (attraverso il/i soggetto/i "Referente/i" incaricato/i di richiedere a Postecom i certificati qualificati) di fornire sotto la propria responsabilità i dati dei titolari in maniera completa e corretta e corrispondenti all'effettiva identità dei propri dipendenti.

Fermo restando quanto disposto all'art. 32, comma 4, del D.lgs 7 marzo 2005, n. 82, il Referente/i nelle attività di richiesta di emissione dei certificati assume ogni responsabilità di tipo amministrativo e penale in merito alla correttezza e completezza dei dati forniti nonché in relazione alle modalità utilizzate al fine di garantire la corrispondenza tra i dati forniti e le effettive identità dei richiedenti il certificato qualificato di firma digitale.

Il Referente raccoglie quindi e invia a Postecom i dati anagrafici degli utenti utilizzando il tracciato fornito da Postecom. Il tracciato così composto sarà inviato a Postecom previo sottoscrizione con firma qualificata firma digitale da parte del Referente/i.

Il Referente assume inoltre il compito di richiedere la sospensione e la revoca dei certificati ogni qualvolta vengano meno i requisiti in base ai quali i certificati sono stati rilasciati, oppure si verificano variazioni dei dati presenti nei certificati stessi e riguardanti l'Organizzazione.

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## Modalità di generazione delle chiavi per la creazione e la verifica della firma

La generazione delle chiavi di sottoscrizione avviene all'interno del dispositivo sicuro di firma che può essere personalizzato:

- dal Certificatore,
- dal Titolare seguendo le istruzioni e utilizzando i sistemi messi a disposizione dal Certificatore, Il Titolare deve avvalersi solo del dispositivo di firma indicato e/o consegnato dal Certificatore.

La generazione della coppia di chiavi è effettuata mediante apparati e procedure che assicurano, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e la robustezza della coppia generata, nonché la segretezza della chiave privata.

Il sistema di generazione delle chiavi assicura:

- la rispondenza della coppia ai requisiti imposti dagli algoritmi di generazione e di verifica utilizzati;
- l'equiprobabilità di generazione di tutte le coppie possibili;
- l'identificazione del soggetto che attiva la procedura di generazione;

### Dispositivo sicuro di firma

I dispositivi sicuri utilizzati per la generazione delle firme sono sottoposti a certificazione ai sensi dello schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione.

Una coppia di chiavi per la creazione e la verifica della firma è attribuita ad un solo Titolare.


La duplicazione della chiave privata o dei dispositivi che la contengono è vietata.

La generazione della firma avviene all'interno del dispositivo sicuro di firma, così che non sia possibile l'intercettazione della chiave privata utilizzata.

Il dispositivo sicuro di firma può essere attivato esclusivamente dal titolare mediante codici personali prima di poter procedere alla generazione della firma.

Se il soggetto appone la sua firma per mezzo di una procedura automatica, deve utilizzare una coppia di chiavi diversa da tutte le altre in suo possesso. Se la procedura automatica fa uso di un insieme di dispositivi, deve essere utilizzata una coppia di chiavi diversa per ciascun dispositivo utilizzato dalla procedura automatica.

## Modalità di emissione dei certificati

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## Personalizzazione del dispositivo a cura del Certificatore

- A seguito del corretto svolgimento delle attività di identificazione e registrazione degli utenti, la relativa documentazione viene inoltrata a Postecom secondo le specifiche modalità operative previste.
- Il Certificatore, verificata la completezza e congruità dei dati, effettua la personalizzazione del dispositivo di firma e l'emissione del certificato qualificato.
- Il dispositivo di firma e la busta cieca, contenente le credenziali segrete di accesso e sblocco della carta (PIN/PUK) e il codice di emergenza (codice di sospensione immediata), vengono inviate separatamente al Titolare.
- Modalità di autenticazione alternative, anche basate su codici OTP, possono essere rese disponibili per l'apposizione della firma nei casi in cui le chiavi vengano conservate su dispositivi sicuri presso il Certificatore. In particolare l'utente in fase di richiesta del servizio dovrà indicare, il numero di cellulare (che in fasi successive potrà anche modificare) sul quale ricevere il codice OTP, specifico per ogni transazione di firma.

Per l'apposizione della singola firma, l'utente dovrà autenticarsi utilizzando le proprie credenziali (user id e password) ed inserire il codice OTP, ricevuto sul numero di cellulare indicato, legato alla specifica operazione di firma. Tale codice avrà una validità di 120 secondi.

## Personalizzazione del dispositivo a cura del Titolare


- Il Richiedente, seguendo le istruzioni fornite ed utilizzando i sistemi messi a disposizione dal Certificatore per la specifica modalità operativa, siti eventualmente presso l'Ufficio Delegato, genera la richiesta di certificazione e la inoltra a Postecom.
- Il Richiedente deve utilizzare esclusivamente il dispositivo sicuro per la generazione delle firme fornito dal certificatore, ovvero un dispositivo scelto tra quelli indicati dal certificatore stesso; La duplicazione della chiave privata o dei dispositivi che la contengono è vietata.
- Il Certificatore, ricevuta la richiesta di generazione del certificato, la verifica, attiva il processo di generazione e di invio del certificato qualificato al Titolare che ne ha fatto richiesta.
- Al Titolare viene consegnato il codice di emergenza per la sospensione immediata.

## Revoca e sospensione dei certificati qualificati

La revoca di un certificato qualificato è l'operazione con cui il Certificatore annulla la validità di un certificato, da un dato momento, non retroattivo, in poi.

La sospensione di un certificato qualificato è l'operazione con cui il Certificatore sospende la validità del certificato.

Le informazioni sulla revoca e sospensione dei certificati sono pubblicate dal Certificatore e rese disponibili tramite le liste di revoca e sospensione (CRL/CSL).

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

La revoca o la sospensione di un certificato qualificato viene effettuata, dal Certificatore, mediante l'inserimento del suo codice identificativo in una delle liste di certificati revocati e sospesi (CRL/CSL).

Le liste di revoca e sospensione sono pubblicate ed accessibili all'indirizzo riportato all'interno del certificato.

Se la revoca avviene a causa della possibile compromissione della segretezza della chiave privata, il Certificatore procede tempestivamente alla pubblicazione dell'aggiornamento della lista.

All'interno di una stessa lista sono contenuti sia i certificati revocati, sia quelli sospesi. Questi ultimi si differenziano nella motivazione della revoca, che in tal caso equivale a "sospensione".

Il Certificatore provvede a rimuovere, dalla lista, i certificati che non sono più sospesi a seguito della riattivazione, nel qual caso, conformemente alle disposizioni vigenti, il certificato, ai fini del valore giuridico delle firme ad esso associate, è da considerarsi come mai sospeso.

Il certificato, revocato o sospeso, rimane nella lista di revoca e sospensione (CRL/CSL) anche successivamente alla sua naturale scadenza.

In caso di revoca di un certificato qualificato sospeso, la data della revoca decorre dalla data di inizio del periodo di sospensione.

La revoca, la sospensione e la riattivazione di un certificato sono registrate nel Giornale di controllo ed hanno effetto a partire dal momento della pubblicazione della lista che le contiene. Il momento di pubblicazione della lista è asseverato mediante l'apposizione di un riferimento temporale.

Inoltre potranno essere disponibili ulteriori modalità di accesso alle informazioni di revoca o sospensione, in particolare attraverso l'OCSP.

Il certificato qualificato può essere revocato o sospeso su iniziativa del:

- ➔ Certificatore
- ➔ Titolare
- ➔ Terzo Interessato

Il certificato qualificato è revocato o sospeso dal certificatore, ove quest'ultimo abbia notizia della compromissione della chiave privata o del dispositivo sicuro per la generazione delle firme.


Il Certificatore, qualora venga a conoscenza di sospetti abusi, falsificazioni, negligenze, si riserva la facoltà di revocare o sospendere i certificati, previa comunicazione motivata, salvo i casi d'urgenza, ai Titolari degli stessi.

Il certificatore comunica tempestivamente l'avvenuta revoca, sospensione o cessazione dello stato di sospensione al titolare e all'eventuale terzo

## **Richiesta di Revoca**

Il Titolare deve procedere alla richiesta di revoca nei seguenti casi:

- ➔ perdita del possesso del dispositivo di firma (smarrimento, furto);
- ➔ guasto o malfunzionamento del dispositivo di firma;

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

- compromissione della segretezza della chiave privata;
- variazione di uno qualunque dei dati presenti nel certificato (ad esempio, nei casi di Titolare appartenente ad Organizzazione, fine del rapporto di lavoro con l'Organizzazione o perdita del ruolo dichiarato nel certificato).

Il Terzo Interessato ha l'onere di richiedere la revoca dei certificati qualificati ogni qualvolta vengano meno i requisiti in base ai quali questi ultimi sono stati rilasciati ai Titolari. In caso di cessazione o modifica delle qualifiche o del titolo inserite nel certificato su richiesta del terzo interessato, la richiesta di revoca è inoltrata non appena il terzo venga a conoscenza della variazione di stato.

Il Terzo Interessato ha la facoltà di richiedere la revoca dei certificati nel caso di abusi, falsificazioni o di uso non conforme degli stessi agli scopi per i quali sono stati emessi, e per ogni altra motivazione dallo stesso ritenuta valida.

Il Titolare e il Terzo Interessato hanno la facoltà di richiedere la revoca di un certificato per un qualunque motivo dagli stessi ritenuto valido ed in qualsiasi momento.

La richiesta di revoca deve essere inoltrata, al Certificatore, munita di sottoscrizione del Titolare o del Terzo Interessato.

Al fine di permettere l'aggiornamento delle liste di revoca e sospensione e quindi garantire la coincidenza tra l'effettività della revoca e la decorrenza desiderata, la richiesta di revoca deve pervenire, al Certificatore almeno 2 (due) giorni feriali prima della decorrenza indicata nella richiesta stessa.

La data di decorrenza della revoca deve coincidere con un giorno feriale.

Il Titolare o il Terzo Interessato possono inoltrare la richiesta di revoca del certificato qualificato attraverso le seguenti modalità:

➤ Richiesta cartacea con firma autografa presso l'Ufficio Delegato


Il Titolare/Terzo Interessato compila e sottoscrive un apposito modulo cartaceo, presentandolo, presso l'Ufficio Delegato, almeno 2 (due) giorni feriali prima del termine di decorrenza indicato nella richiesta stessa.

Il Certificatore, ricevuta la richiesta dall'Ufficio Delegato e verificata la sua autenticità, provvede alla revoca del certificato tramite inserimento nell'apposita lista dei certificati revocati e sospesi (CRL/CSL) e pubblicazione della lista stessa.

➤ Richiesta sottoscritta digitalmente

Il Titolare/Terzo Interessato inoltra la richiesta al Certificatore almeno 2 (due) giorni feriali prima del termine di decorrenza indicato nella stessa, o compilando e firmando digitalmente l'apposito modulo elettronico reso disponibile dal certificatore.

La richiesta è verificata dal Certificatore, che solo a fronte della verifica positiva, provvede alla revoca del certificato tramite inserimento nell'apposita lista dei certificati revocati e sospesi (CRL/CSL) e pubblicazione della lista stessa.

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

Se il certificatore non ha la possibilità di accertare in tempo utile l'autenticità della richiesta, procede alla sospensione del certificato.

Il certificatore conserva le richieste di revoca per 20 (venti) anni.

## Richiesta di Sospensione

Il Titolare e il Terzo Interessato hanno la facoltà di richiedere la sospensione di un certificato per un qualunque motivo dagli stessi ritenuto valido ed in qualsiasi momento.

Il Certificatore sospende il certificato ogni qualvolta, ricevuta una richiesta di revoca da parte del Titolare o del Terzo Interessato, non ha la possibilità di accertare in tempo utile l'autenticità della richiesta stessa.

Il Certificatore, qualora venga a conoscenza di sospetti usi non conformi, si riserva la facoltà di sospendere i certificati, previa comunicazione ai Titolari, salvo i casi d'urgenza.

La richiesta di sospensione deve essere inoltrata, al Certificatore, munita di sottoscrizione del Titolare o del Terzo Interessato. Al fine di permettere l'aggiornamento delle liste di revoca e sospensione e quindi garantire la coincidenza tra l'effettività della sospensione e la decorrenza desiderata, la richiesta di sospensione deve pervenire al Certificatore almeno 2 (due) giorni feriali prima del termine di decorrenza indicato nella stessa.

Le date di inizio deve coincidere con giorni feriali. Il certificato rimane nello stato di sospensione fino alla sua scadenza.

Fa eccezione il caso di richiesta, da parte del solo Titolare, di sospensione immediata del certificato.. Il Certificatore provvede a processare tempestivamente la richiesta, inserendo il certificato nella lista di revoca. Successivamente, il Titolare, qualora intenda revocare o riattivare il certificato sospeso, dovrà presentarsi di persona presso l'Ufficio Delegato. Il Titolare o il Terzo Interessato possono inoltrare la richiesta di sospensione del certificato qualificato attraverso le seguenti modalità:


### ➤ Richiesta cartacea con firma autografa presso l'Ufficio Delegato

Il Titolare/Terzo Interessato compila e sottoscrive un apposito modulo cartaceo, presentandolo, presso l'Ufficio Delegato, almeno 2 (due) giorni feriali prima dell'inizio della decorrenza indicata nella richiesta stessa.

Il Certificatore, ricevuta la richiesta dall'Ufficio Delegato e verificata la sua autenticità, provvede alla sospensione del certificato tramite inserimento nell'apposita lista dei certificati revocati e sospesi (CRL/CSL) e pubblicazione della lista stessa.

### ➤ Richiesta sottoscritta digitalmente

Il Titolare/Terzo Interessato inoltra la richiesta al Certificatore almeno 2 (due) giorni feriali prima dell'inizi della decorrenza o compilando e firmando digitalmente l'apposito modulo elettronico reso disponibile dal certificatore.

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

La richiesta è verificata dal Certificatore, che provvede alla sospensione del certificato tramite inserimento nell'apposita lista dei certificati revocati e sospesi (CRL/CSL) e pubblicazione della lista stessa.

Il certificatore conserva le richieste di sospensione per 20 (venti) anni.

### **Richiesta per la sospensione immediata**

Per ciascun certificato qualificato emesso il certificatore fornisce al titolare almeno un codice riservato, da utilizzare per richiedere la sospensione del certificato nei casi di emergenza, quali smarrimento o sottrazione del dispositivo di firma. In tali casi il Titolare deve sporgere denuncia alle autorità competenti.

Il codice di emergenza viene comunicato al Titolare tramite modalità che ne assicurino la segretezza (ad es. stampa e invio su buste "cieca").

La richiesta di sospensione immediata nei casi di emergenza può essere inoltrata tramite l'apposito servizio web, e prevede che il Titolare fornisca il codice di emergenza (*codice di sospensione immediata*) e il codice identificativo attribuito dal Certificatore.

Il Certificatore provvederà a processare tempestivamente la richiesta, inserendo il certificato nella lista di revoca/sospensione e pubblicando la lista stessa.

La richiesta di sospensione inoltrata nelle modalità descritte, potrà essere seguita da una richiesta scritta di revoca o di riattivazione del certificato, inoltrata dal Titolare, presso l'Ufficio Delegato.

### **Richiesta per la riattivazione di un certificato precedentemente sospeso**

La riattivazione di un certificato sospeso ne determina nuovamente la validità (pertanto la cancellazione dalle Liste di revoca e sospensione). Un certificato viene riattivato nelle seguenti modalità:

- con una richiesta scritta di riattivazione, presentata presso l'Ufficio Delegato e per un certificato precedentemente sospeso. La richiesta di riattivazione non sarà accettata se il certificato di firma digitale risulta revocato.


### **Disponibilità dei servizi di revoca o sospensione**

Il Certificatore predisponde, per ogni modalità di inoltro delle richieste di revoca o sospensione, una diversa disponibilità del servizio ad essa connessa:

- in caso di richiesta di revoca o sospensione presentata presso l'Ufficio Delegato, gli orari di disponibilità del servizio sono resi noti al pubblico dall'Ufficio stesso;
- per le richieste di sospensione immediata inoltrate via Internet, il servizio di accettazione delle richieste stesse è disponibile 24 ore su 24;

### **Aggiornamento delle CRL e delle CSL**

Le liste di revoca o sospensione dei certificati sono aggiornate in seguito ad ogni richiesta di revoca o sospensione.

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

La pubblicazione delle Liste di revoca e sospensione avviene, comunque, al massimo ogni 24 (ventiquattro) ore.

## Rinnovo del certificato qualificato

Il rinnovo deve essere effettuato, necessariamente, prima che il corrispondente certificato sia scaduto. La procedura, messa a disposizione dal Certificatore, a partire dal sito [postecert.poste.it](http://postecert.poste.it), prevede :

- generare la nuova coppia di chiavi e la relativa richiesta di certificazione;
- generare il pacchetto contenente la richiesta di certificazione e la chiave pubblica, firmato con la chiave privata di sottoscrizione relativa al certificato in prossimità di scadenza.


Il Titolare trasmette la richiesta al Certificatore che, dopo averne verificato la legittimità e la validità, provvede alla generazione del certificato.

Il certificato viene quindi inoltrato al Titolare, il quale provvede alla sua registrazione sul dispositivo di firma.

Tale modalità è valida esclusivamente per il primo rinnovo. Successivamente, il Titolare che intende continuare ad avvalersi del servizio di certificazione, dovrà richiedere una nuova smart card e certificato.

Periodicità e modalità alternative potranno essere definite negli accordi stipulati tra le Parti.

Qualora il certificato risulti già scaduto o revocato sarà necessario effettuare una nuova richiesta di emissione.

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## Registro dei certificati

Il Certificatore pubblica nel Registro dei certificati:

1. lista dei certificati revocati (CRL);
2. lista dei certificati sospesi (CSL).

Inoltre, il Certificatore, dietro consenso da parte del Titolare, pubblica i certificati emessi nel Registro dei Certificati.

### Modalità di gestione del Registro dei certificati

Il Certificatore mantiene una copia di riferimento del Registro dei certificati inaccessibile dall'esterno (Directory Server Master), allocata su un sistema sicuro installato in locali protetti.

Sistematicamente, verifica la conformità tra la copia operativa (Directory Server Shadow) e la copia di riferimento del Registro, annotando ogni discordanza nel Registro operativo.

Modifiche al contenuto del Registro dei certificati sono effettuate esclusivamente da personale autorizzato. Tali operazioni sono inoltre registrate sul Giornale di controllo.

La data e l'ora di inizio e fine di ogni intervallo di tempo nel quale il Registro dei certificati non risulta accessibile dall'esterno, nonché quelle relative a ogni intervallo di tempo nel quale una sua funzionalità interna non risulta disponibile, sono annotate sul Giornale di controllo e comunicate a DigitPA e agli utenti, come previsto dall'art. 32, comma 3, lettera m-bis) del D.lgs 7 marzo 2005, n. 82.

Il Certificatore cura l'allineamento tra copia di riferimento e copia operativa e mantiene una copia di sicurezza (backup) del Registro dei certificati.

Il Certificatore provvede all'aggiornamento del Registro dei certificati quando:


- ➔ emette nuovi certificati;
- ➔ pubblica le Liste di revoca/sospensione con la periodicità definita nel paragrafo "Aggiornamento delle CRL e delle CSL" del presente Manuale Operativo;

### Modalità di accesso al Registro dei certificati


Il registro dei certificati di Poste.com è un Internet Directory Server compatibile con le specifiche X.500 1993 e che supporta LDAP v.3.

Il Registro dei certificati è pubblicamente consultabile 24 ore al giorno, 7 giorni la settimana, salvo manutenzione programmata, all'indirizzo ldap://certificati.postecert.it.

Le liste pubblicate dei certificati revocati e sospesi, nonché i certificati qualificati resi accessibili alla consultazione del pubblico, sono utilizzabili da chi le consulta per le sole finalità di applicazione delle norme che disciplinano la verifica e la validità della firma qualificata di firma digitale.

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## **SEZIONE IV – PROCEDURE OPERATIVE PER LA FIRMA E LA VERIFICA**

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

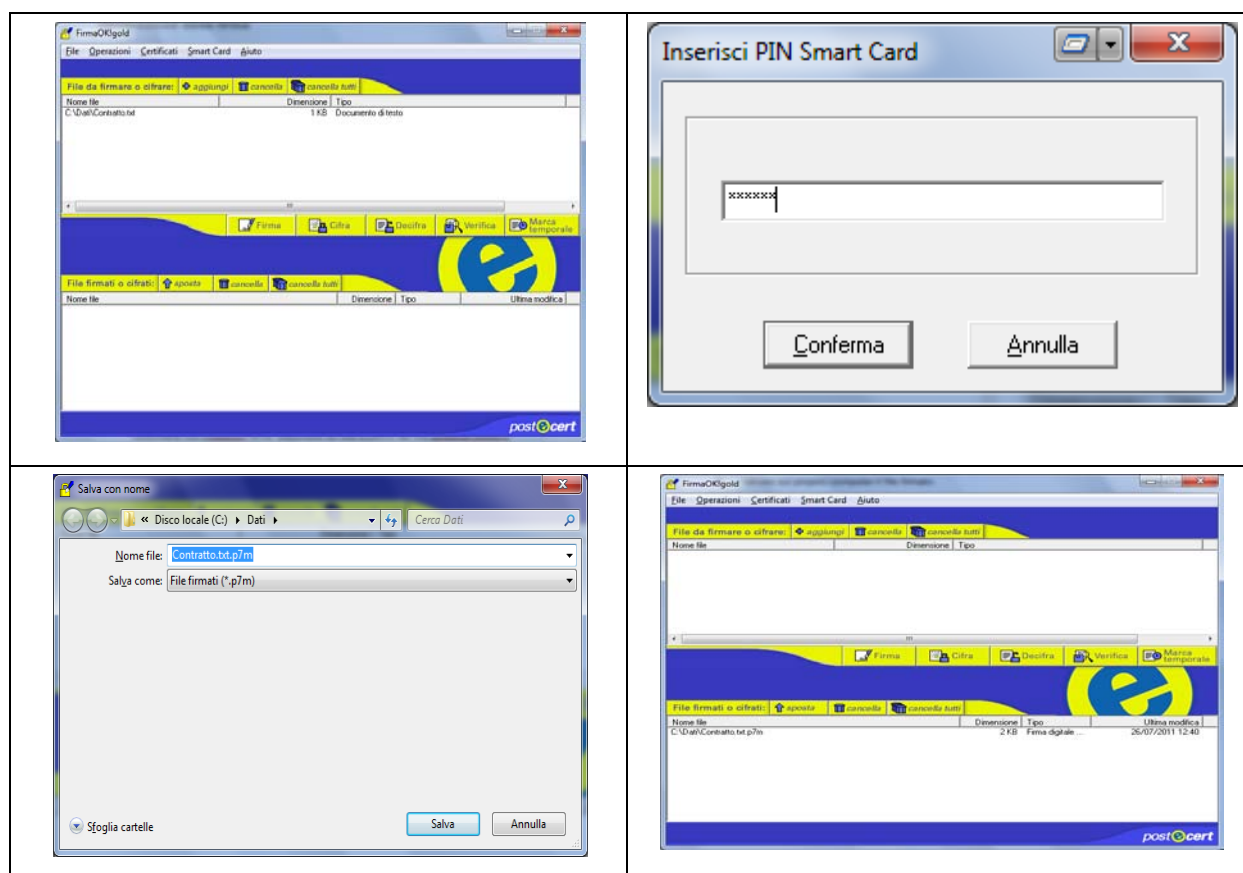
## Modalità operative per la generazione e la verifica delle firme

### Generazione della firma


Postecom, agli utenti del Servizio che acquistano il servizio/prodotto di firma, offre un apposito applicativo che espone una serie di funzionalità, tra le quali la firma di documenti informatici, la possibilità di verificare documenti firmati digitalmente e di cifrare/decifrare qualsiasi file.

L'operazione di generazione della firma permette di:

- selezionare la coppia di chiavi di firma, in corso di validità, da utilizzare;
- visualizzare il documento informatico che si intende firmare;
- inserire il proprio PIN per poter accedere all'area protetta che contiene la chiave privata;
- salvare sul proprio computer il file firmato.

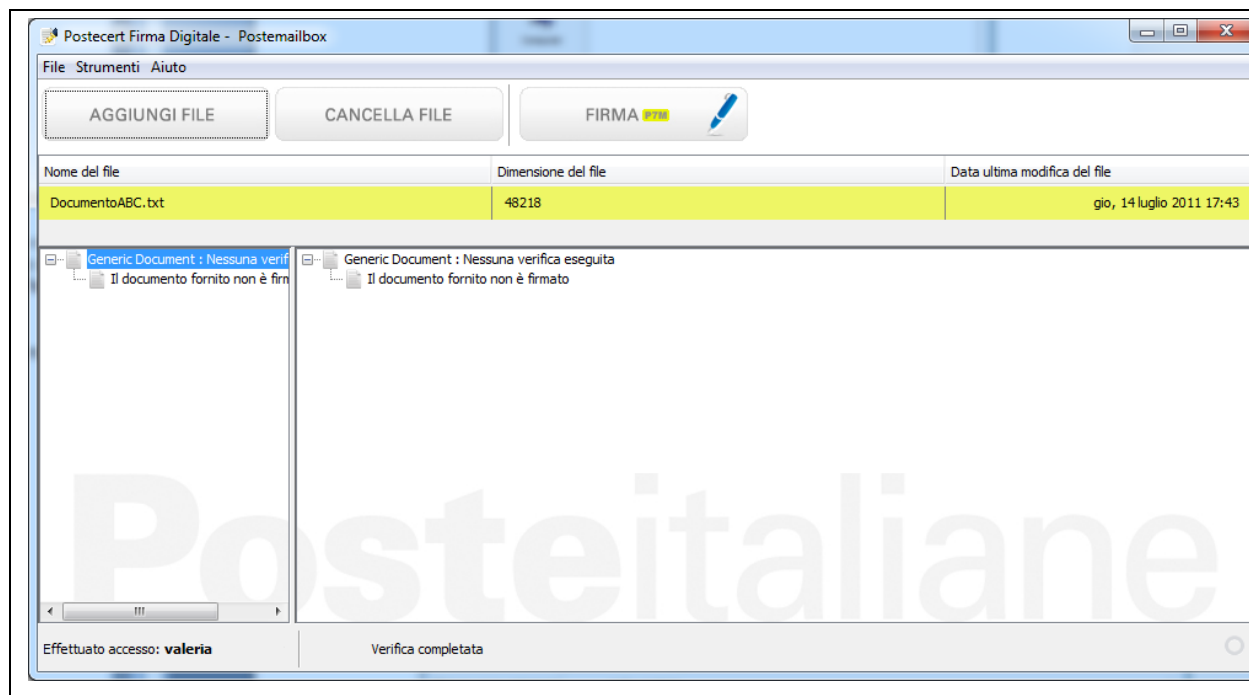


Come ulteriore modalità è previsto un servizio di "firma digitale" con chiavi private presso il Certificatore, tramite il quale gli utenti possono apporre la firma ad un documento informatico,

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

accedendo alle proprie chiavi con password utente e codice OTP ricevuto sul cellulare indicato in fase di richiesta del Servizio.

Si allega una schermata iniziale dell'applicazione per l'uso della firma digitale con chiavi private presso il Certificatore Postecom.



I manuali d'uso completo delle applicazioni sono disponibili sul sito [postecert.poste.it](http://postecert.poste.it)

## Sistema di verifica delle firme qualificate


Il documento elettronico firmato digitalmente, può essere verificato dal destinatario:

- tramite l'applicativo client fornito da Postecom ai propri titolari dei certificati qualificati;
- limitatamente alla verifica delle firme basate su certificati emessi da Postecom, accedendo alla funzionalità che Postecom rende disponibile on-line a partire dal sito [postecert.poste.it](http://postecert.poste.it).

I suddetti sistemi soddisfano i requisiti normativi previsti dalla Deliberazione CNIPA n.45 del 21/05/2009.

Nell'ambito della verifica vengono effettuate le seguenti operazioni:

- convalida integrità - accerta che il documento non sia stato modificato dopo la firma;
- verifica credibilità - verifica se il documento è stato firmato da un soggetto "credibile" nell'ambito della lista dei certificati di root delle CA iscritte nell'Elenco Pubblico dei Certificatori tenuto dal DigitPA;
- verifica validità - controlla che il certificato non sia scaduto;
- verifica CRL/CSL - verifica che il certificato non risulti revocato o sospeso;

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

- verifica alla data – verifica la validità del certificato a partire dalla data presente nel file firmato (se marca temporale) o a partire dalla data impostata dall'utente;
- visualizzazione delle informazioni presenti nel certificato

Il sistema di verifica consente, per via telematica, l'aggiornamento delle informazioni pubblicate nell'elenco pubblico dei certificatori

Nel corso della verifica il destinatario deve controllare la presenza di eventuali limitazioni d'uso nel certificato del sottoscrittore; deve verificare inoltre la presenza nel documento verificato di eventuali macro istruzioni o codici eseguibili che renderebbe nullo il documento firmato digitalmente.

## Formato dei documenti informatici

Gli applicativi di *Office Automation*, utilizzati per la generazione di documenti informatici, mettono a disposizione nativamente alcune funzionalità, che possono rendere dinamico il contenuto del documento e dipendente dal contesto e dal momento della sua visualizzazione (ad esempio l'aggiornamento automatico di una data presente nel documento o altre macroistruzioni similari).

Il DPCM 30/3/2009 Art.3, comma 3, sancisce che l'apposizione della firma digitale su documenti elettronici contenenti "macroistruzioni o codici eseguibili, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati", non produce gli effetti previsti dalla normativa vigente per la firma elettronica qualificata.


Il Certificatore, attraverso le applicazioni distribuite, visualizza al Titolare, in fase di sottoscrizione, un messaggio informativo sulla possibile presenza di "macro o codice eseguibile tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati". Il titolare deve accertarsi che il documento presenti un formato di tipo statico e non incorpori, quindi, campi dinamici come sopra descritti.

A titolo esemplificativo, è possibile suggerire l'utilizzo di formati quali: puro testo ".txt", immagine ".tif", portable document format ".pdf" (se privo di campi modulo o java script). Nel caso di documenti tipo word, si consiglia sempre di verificare la presenza di codice eseguibile o macroistruzioni.

Si riportano per comodità le principali verifiche da applicare:

### MS Office 2000:


- Menu Strumenti, selezionare Macro, poi Protezione.
- Scegliere il livello di protezione desiderato. Selezionando una protezione Alta, si consente l'esecuzione automatica esclusivamente delle macro firmate digitalmente e provenienti da fonti attendibili. Non verranno eseguite le macro non firmate. Selezionando una protezione Media si consente l'esecuzione automatica delle macro firmate digitalmente da fonti attendibili e di visualizzare la finestra di dialogo relativa alla protezione da virus macro che consente di disattivare le macro non firmate.

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011


Seppur disattivate, le macro sono comunque presenti nel documento che ci si appresta a firmare; per tale ragione si consiglia di impostare il livello di protezione medio, così da avere evidenza della presenza delle stesse.

#### MS Office 2007

- Menu principale, selezionare Opzioni di Word/Excel, Centro Protezione poi Impostazioni Centro protezione.
- Selezionare Impostazioni Macro e poi Disattiva tutti le macro senza notifica. In questo modo nessuna macro verrà eseguita all'interno del documento. Effettuare una selezione analogo per Impostazione ActiveX e Componenti Aggiuntivi.

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## **SEZIONE V – GESTIONE DELLE CHIAVI DI CERTIFICAZIONE E DI MARCATURA TEMPORALE**

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## Chiavi di certificazione

Il Certificatore si avvale delle seguenti chiavi di certificazione:

- chiavi di certificazione per firmare digitalmente i certificati relativi alle chiavi di sottoscrizione, le liste di revoca e sospensione(CRL/CSL);
- chiavi di certificazione per firmare digitalmente i certificati relativi alle chiavi di marcatura temporale.

Le chiavi di certificazione possono inoltre essere utilizzate per le seguenti finalità:

- rilascio di certificati di autenticazione per la Carta Nazionale dei Servizi (CNS);
- certificati elettronici per usi diversi dalla Firma Digitale basata su certificato qualificato referenziati in apposite policy identificate con specifici OID riportati nel certificato, oltre che caratterizzati da *keyUsage* diversi da *nonRepudiation*.

### Generazione delle chiavi di certificazione

La generazione delle chiavi di certificazione è effettuata esclusivamente in presenza del Responsabile del Servizio della Certificazione e Validazione Temporale, che le utilizzerà. La generazione della coppia di chiavi di certificazione avviene all'interno del dispositivo di firma, personalizzato, dalla postazione predisposta a tale funzione, dal Certificatore.

Per ciascuna chiave di certificazione il certificatore genera un certificato sottoscritto con la chiave privata della coppia cui il certificato si riferisce.

### Revoca dei certificati relativi a chiavi di certificazione

Il Certificatore procede alla revoca del certificato relativo ad una coppia di chiavi di certificazione esclusivamente nei seguenti casi:


- compromissione della chiave privata, intesa come diminuita affidabilità nelle caratteristiche di sicurezza della chiave privata;
- guasto del dispositivo di firma;
- cessazione dell'attività, salvo il caso in cui sia individuato un certificatore sostitutivo.

La revoca del certificato relativo ad una coppia di chiavi di certificazione è notificata a DigitPA ed a tutti i possessori di certificati qualificati, sottoscritti con la chiave privata appartenente alla coppia revocata, entro le 24 ore.

I certificati qualificati, per i quali venga revocato il certificato relativo alla chiave con cui sono stati sottoscritti, vengono anch'essi revocati.

Il Certificatore procede alla revoca dei certificati relativi a chiavi di certificazione, inserendoli nella Lista di revoca (CRL), che rende pubblica dopo avervi apposto un riferimento temporale.


La revoca è annotata nel Giornale di controllo.

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## Sostituzione delle chiavi di certificazione

La procedura di sostituzione delle chiavi di certificazione assicura che non siano stati emessi certificati qualificati con data di scadenza posteriore al periodo di validità del certificato relativo alla coppia sostituita.

I certificati generati a seguito della sostituzione delle chiavi di certificazione sono inviati al DigitPA, che provvede all'aggiornamento della lista dei certificati delle chiavi di certificazione contenuta nell'Elenco Pubblico dei Certificatori ed al suo inoltro ai Certificatori per la pubblicazione.

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## Chiavi di marcatura temporale

Le chiavi di marcatura temporale sono destinate alla generazione e verifica delle marche temporali.

La marca temporale è un'evidenza informatica sottoposta a firma, contenente le informazioni previste dal DPCM 30/03/2009.

Ogni coppia di chiavi utilizzata per la validazione temporale è univocamente associata ad un sistema di validazione temporale e dal relativo certificato deve essere possibile individuare tale sistema.

### Generazione delle chiavi di marcatura temporale

Per limitare il numero di marche temporali generate con la medesima coppia, le chiavi di marcatura temporale sono sostituite, ed un nuovo certificato è emesso, dopo non più di un mese di utilizzo, indipendentemente dalla durata del loro periodo di validità e senza revocare il corrispondente certificato. Il responsabile del servizio attiva la generazione delle chiavi di marcatura temporale all'interno del dispositivo di firma.

### Revoca dei certificati relativi a chiavi di marcatura temporale

Il Certificatore procede alla revoca del certificato, relativo ad una coppia di chiavi di marcatura temporale, esclusivamente nei seguenti casi:


- ➔ compromissione della chiave privata, intesa come diminuita affidabilità nelle caratteristiche di sicurezza della chiave privata;
- ➔ guasto del dispositivo di firma.

Il Certificatore procede alla revoca dei certificati relativi a chiavi di marcatura temporale, inserendoli nella Lista di revoca (CRL), che rende pubblica dopo avervi apposto un riferimento temporale.


La revoca viene annotata nel Giornale di controllo.

### Sostituzione delle chiavi di marcatura temporale

La sostituzione delle chiavi di marcatura temporale avviene mensilmente.

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## **SEZIONE VI – MODALITÀ PER L'APPOSIZIONE E LA DEFINIZIONE DEL RIFERIMENTO TEMPORALE**

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## Riferimento temporale


Postecom, quale Certificatore Accreditato, appone sul Giornale di Controllo riferimenti temporali emessi in accordo a quanto previsto dal DPCM 30/03/2009, che attestano una data ed ora certe ed opponibili a terzi.

La data e l'ora contenute nel riferimento temporale apposto al Giornale di Controllo, sono specificate con riferimento al Tempo Universale Coordinato (UTC). L'ora assegnata ad un riferimento temporale corrisponde al momento della sua generazione, con una differenza inferiore al minuto secondo rispetto alla scala di tempo UTC.

Si considera come sorgente del riferimento temporale l'orologio di sistema, la cui precisione è garantita dalla sua sincronizzazione con una sorgente esterna, che mantiene un'informazione temporale corrispondente alla scala temporale UTC.

La sorgente esterna è costituita da un dispositivo orologio sincronizzatore orario. Tale dispositivo recupera - tramite un ricevitore a modulazione di frequenza, a sintonia digitale di elevate prestazioni, montato su circuito stampato - i segnali orari generati dall'Istituto Elettrotecnico Nazionale "Galileo Ferraris" di Torino, trasmessi dalle stazioni in modulazione di frequenza di RADIO UNO. Il dispositivo è dotato di un microcomputer (CPU), che imposta la sintonia della radio ed effettua, tramite un filtro digitale, il riconoscimento dei segnali orari utilizzati per regolare il proprio oscillatore interno di elevata precisione. La data completa (anno, mese, giorno, ora, minuti, secondi) è trasmessa al sistema, ogni secondo, su porta seriale.

Il dispositivo utilizzato ha ottenuto il certificato di taratura dall'istituto Galileo Ferraris, che ne attesta la capacità di mantenere la sincronizzazione con il tempo UTC, con l'accuratezza di  $\pm 1$  millisecondo.

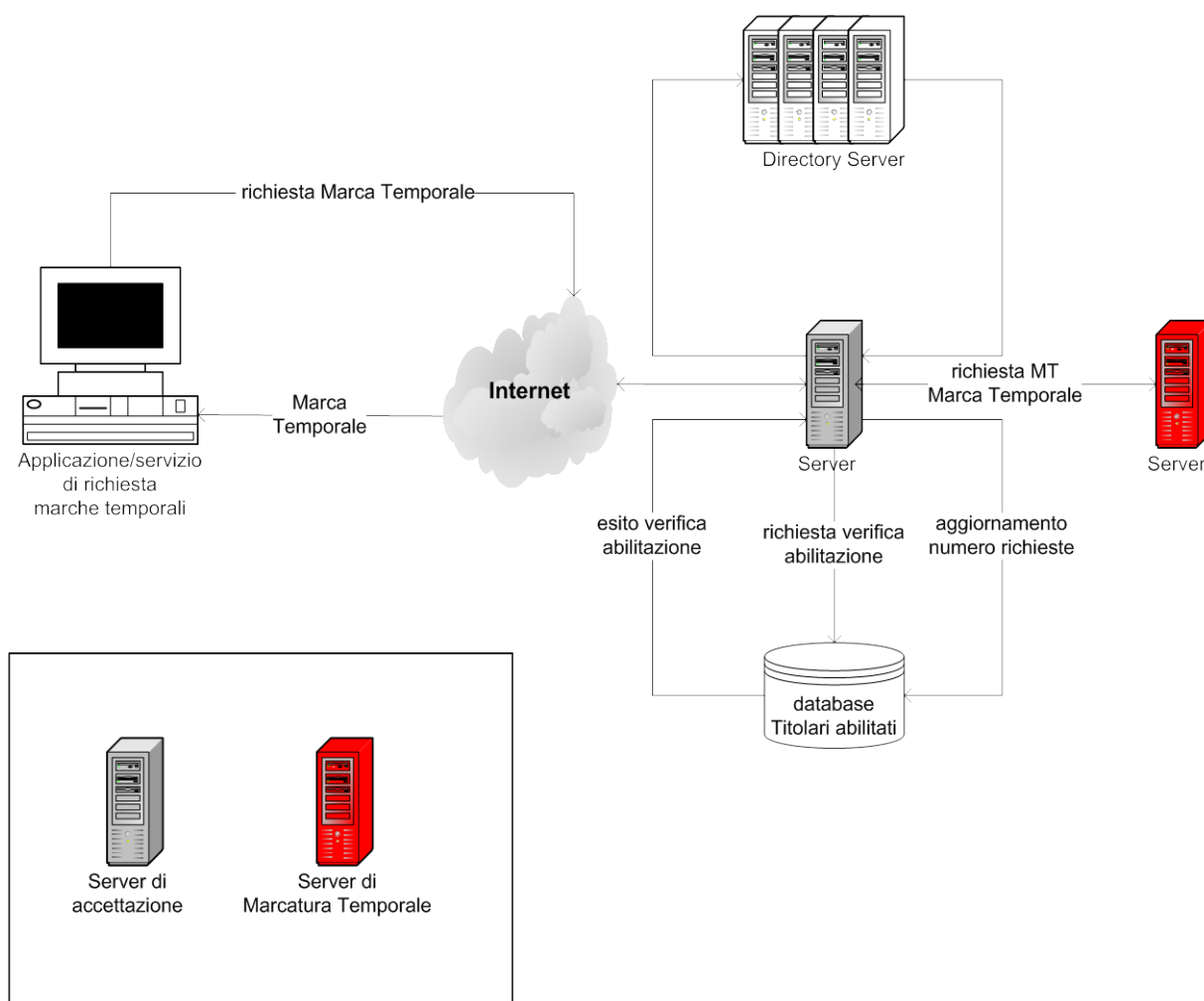
 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## Marcatura temporale


Il Servizio di Marcatura Temporale prevede il rilascio di marche temporali associate a documenti informatici e consente di attribuire, al documento informatico, un riferimento temporale opponibile a terzi.

La marcatura temporale è un particolare riferimento temporale, realizzato in conformità con quanto disposto dal titolo IV del DPCM 30/03/2009,

Il sistema di validazione temporale (TSA – *Time Stamping Authority*) è sviluppato in conformità allo standard RFC 3161. L'architettura prevede un server di accettazione delle richieste, che richiede l'emissione delle marche ad un server di marcatura temporale.



Il server di accettazione è un'applicazione server stand alone, in esecuzione su di una piattaforma Windows, in ascolto su una porta TCP/IP. Tramite tale porta, riceve le richieste dalle applicazioni/servizi e invia di ritorno le relative risposte, in conformità allo standard IETF corrispondente. Il formato della struttura dati, emessa dal server di marcatura temporale, è conforme alla normativa vigente. Il *time stamp token* emesso e la firma ad esso apposta sono incapsulati nella struttura dati firmata «SignedData».

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011


## Modalità di richiesta del servizio di marcatura temporale

Il servizio di marcatura temporale nasce come servizio centralizzato, il cui destinatario è, a sua volta, un servizio o un'applicazione. L'applicazione chiamante genera l'impronta del documento elettronico utilizzando l'algoritmo di hash previsto, firma le richieste di marche temporali e le trasmette, via http, al server di accettazione del servizio centralizzato di Postecom, che restituisce la marca temporale emessa. Le modalità di inoltro della richiesta e di utilizzo di tale servizio, vengono regolate da appositi accordi tra le Parti.


Il servizio di marcatura temporale è disponibile ai soli utenti abilitati: il sistema di TSA di Postecom, verificata l'autenticità della richiesta e l'abilitazione del Titolare, emette la marca temporale e la restituisce al servizio/applicazione chiamante.

## Validità della marca temporale

Tutte le marche temporali emesse vengono conservate da Postecom per un periodo non inferiore a venti (20) anni. La marca temporale è valida per l'intero periodo di conservazione.

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## **SEZIONE VII – UFFICI DELEGATI – VERIFICHE ISPETTIVE PERIODICHE**

 Gruppo Poste Italiane	<b>Manuale Operativo</b>	MOP01
	<b>Servizio Postecert Firma Digitale</b>	Versione 3.3 Data 06 Dicembre 2011

## Verifiche periodiche

Postecom concorda con gli Uffici Delegati un piano di attività di verifiche periodiche tese ad assicurare il rispetto delle procedure concordate in merito alla delega delle funzioni di identificazione dei titolari e di raccolta e trasmissione dei dati di registrazione.

In particolare, qualora l'accordo di delega coinvolga anche la fornitura di apposite soluzioni di personalizzazione locale delle smart card, le verifiche saranno tese a verificare la permanenza dei requisiti per il loro utilizzo sicuro e limitato al personale autorizzato.