



**MONTE
DEI PASCHI
DI SIENA**
BANCA DAL 1472

 **GRUPPOMPS**

Servizio di Certificazione

Manuale Operativo

Codice documento: 1030 18774.1.1.1.1 - 2007 - 1 - 1
Società Progetto/Servizio Anno N. Doc Versione

Distribuzione: PUBBLICA

STORIA DELLE MODIFICHE APPORTATE

Di seguito sono descritte le modifiche apportate alla precedente versione del documento a fronte della revisione dello stesso.

CAPITOLO	PARAGRAFO	DESCRIZIONE
1	1.1	<ul style="list-style-type: none"> • Modificati i riferimenti alle norme di legge.
1	1.2	<ul style="list-style-type: none"> • Modificato "DPCM". • Inseriti "DIR, DM, DLGS 82, Delibera 4, L. 273, DM 591, DLGS 21/01/04, DLGS 159". • Eliminati "CR 22 e CR 24".
1	1.3	<ul style="list-style-type: none"> • Eliminata la frase "In questo documento si fa riferimento alle regole tecniche di attuazione della legge sulla firma digitale contenute nel [DPCM] attualmente in vigore. Qualora le regole tecniche venissero sostituite da successivo riferimento normativo i riferimenti di cui al presente manuale si intenderanno allineati alle disposizioni vigenti.".
1	1.4	<ul style="list-style-type: none"> • Aggiunti "RFC 3161, RFC 3280, ETSI 280 ed ETSI 862".
1	1.5	<ul style="list-style-type: none"> • Aggiunti gli acronimi "DPCM, ETSI, GPS, IEN, INRIM, IETF, OID, TCP, TSS, TST ed UTC".
2		<ul style="list-style-type: none"> • Eliminata la frase: "In tale sezione si fa riferimento agli obblighi derivanti dall'art. 45/3/ sezioni a b e c e alle indicazioni descritte nello standard RFC 2527, sezione 4.1 (Introduction).".
2	2.1	<ul style="list-style-type: none"> • Aggiunto riferimento all'articolo 38/3/a. • Inserito "Directory Server" nei dati identificativi del certificatore. • Modificato "legale rappresentante" nei dati identificativi del certificatore.
2	2.2	<ul style="list-style-type: none"> • Modificato codice documento.
2	2.3	<ul style="list-style-type: none"> • Aggiunto riferimento all'articolo 38/3/b. • Aggiornati i riferimenti alle norme di legge. • Sostituita la frase "In ogni caso, farà fede la versione più aggiornata delle due (in base al codice documento riportato sul frontespizio)." Con la frase "In ogni caso, farà fede la versione pubblicata sul sito web CNIPA." • Aggiunta la frase "inoltre è possibile accedere al documento col protocollo HTTPS (http su SSLv3), in modo tale che il consultatore sia garantito, grazie al meccanismo di "server authentication" insito nel protocollo SSL, circa la provenienza del documento stesso."
2	2.4	<ul style="list-style-type: none"> • Aggiunto riferimento all'articolo 38/3/c.
3	3.1	<ul style="list-style-type: none"> • Aggiunto riferimento all'articolo 38/3/d. • Eliminata la frase "Questa sezione fa riferimento agli articoli art. 45/3 d, e, f e alle indicazioni descritte nello standard RFC 2527, sezione 4.2 (General Provisions). Le regole generali fanno altresì riferimento al fatto che BMPS partecipa al circuito IdenTrust e sottostà agli obblighi che lo stesso circuito descrive, nel rispetto delle convenzioni operative che i diversi ambiti di utilizzo richiedono.".

3	3.1.1	<ul style="list-style-type: none"> • Modificato il titolo del paragrafo in <i>"Obblighi e responsabilità del certificatore."</i> • Modificati i riferimenti alle norme di legge nei vari punti. • Eliminata la frase <i>"Il certificatore è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri."</i> • Eliminata la frase <i>"Il certificatore che rilascia, ai sensi dell'articolo 27, certificati qualificati é tenuto inoltre a:"</i> • Inserito il punto <i>"adottare tutte le misure organizzative e tecniche idonee ad evitare danni a terzi;"</i> • Punto 2: sostituita la frase <i>"identificare con certezza la persona che fa richiesta della certificazione;"</i> con la frase <i>"identificare con certezza la persona che richiede il certificato anche nel caso in cui tale attività sia delegata a terzi"</i>. • Punto 4: sostituita la frase <i>"specificare, nel certificato qualificato su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della sussistenza degli stessi;"</i> con la frase <i>"specificare, nel certificato qualificato, su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della sussistenza degli stessi sulla base della documentazione presentata dal richiedente;"</i> • Punto 7: sostituito <i>"adottare le misure di sicurezza per il trattamento dei dati personali, ai sensi dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675"</i> con <i>"trattare i dati personali nel rispetto del [DLGS 196] e successive modificazioni, predisponendo tutele rispondenti almeno alle misure minime stabilite nello stesso decreto legislativo. Limitatamente al servizio erogato sulla base del Manuale Operativo, il certificatore non tratta "dati particolari" ovvero dati sensibili ai sensi dell'art. 4 comma 1 lettera d) o giudiziari ai sensi dello stesso articolo comma 1 lettera e)"</i>. • Punto 10: sostituita la frase <i>"garantire il funzionamento efficiente, puntuale e sicuro dei servizi di elencazione, nonché garantire un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo;"</i> con la frase <i>"garantire il funzionamento efficiente, puntuale e sicuro del registro dei certificati ed un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo;"</i> • Punto 12: sostituita la frase <i>"non copiare, né conservare le chiavi private di firma del soggetto cui il certificatore ha fornito il servizio di certificazione;"</i> con la frase <i>"non copiare, né conservare le chiavi private di firma del proprietario del certificato;"</i> • Inserito punto 11: <i>"fornire, prima dell'accordo, ai richiedenti il servizio, le informazioni relative ai termini ed alla condizioni sull'utilizzo del certificato;"</i> • Punto 12: inserito <i>"garantire che solo il personale autorizzato possa effettuare inserimenti e modifiche del re-</i>
---	-------	---

		<p><i>gistro dei certificati e che l'autenticità delle informazioni sia verificabile;" al posto di "utilizzare 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. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato."</i></p> <ul style="list-style-type: none"> • Inserito punto 13: <i>"conservare le informazioni relative al certificato qualificato per venti anni;"</i>. • Inserito punto 14: <i>"raccogliere i dati personali nel rispetto del [DLGS 196]"</i>. • Sostituita la frase <i>"Il certificatore che rilascia certificati al pubblico raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato, fornendo l'informativa prevista dalla disciplina in materia di dati personali. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono."</i> con il paragrafo <i>"Il certificatore che rilascia certificati qualificati ha l'obbligo di operare secondo quanto previsto dal Titolo II ("Regole tecniche di base") del [DPCM]; in particolare, il certificatore accreditato ha l'obbligo di attenersi anche alle disposizioni di cui al Titolo III ("Ulteriori regole per i certificatori accreditati") e IV ("Regole per la validazione temporale per la protezione dei documenti informatici") del [DPCM]. Infine il certificatore accreditato, nel caso in cui intenda lasciare l'attività, ha l'obbligo di attenersi a quanto previsto nell'art. 37 del [DLGS 82]. La responsabilità del certificatore nei confronti dei titolari di certificato e dei terzi che vi fanno affidamento sono descritte nell'art. 30 del [DLGS 82]. In particolare il certificatore garantisce:</i> <ul style="list-style-type: none"> ▪ <i>l'esattezza e completezza, alla data del rilascio, delle informazioni necessarie alla verifica della firma contenute nel certificato e rispetto ai requisiti fissati per i certificati qualificati.</i> ▪ <i>Il possesso da parte del firmatario, al momento del rilascio del certificato, dei dati per la creazione della firma corrispondente ai dati per la verifica della firma riportati o identificati nel certificato.</i> <p><i>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 (§ 4.2.1.4)."</i></p>
--	--	--

3	3.1.2	<ul style="list-style-type: none"> • Modificati i riferimenti alle norme di legge nei vari punti. • Sostituita la frase <i>"Il titolare ha l'obbligo di adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri (art. 29 bis, comma 1, del [DPR445])."</i> con la frase <i>"Il titolare ha l'obbligo di assicurare la custodia del dispositivo di firma e di utilizzarlo personalmente. L'utilizzo del dispositivo di firma è riconducibile al titolare a meno che non fornisca prova contraria"</i>. • Punto 1: sostituito <i>"dall'Art. 27 del [DPCM];"</i> con <i>"nel manuale operativo;"</i>; e sostituito <i>"in questo"</i> con <i>"nel"</i>. • Punto 2: eliminato <i>"segnalare al certificatore quali informazioni egli desidera non siano rese pubbliche;"</i>. Sostituito <i>"in luogo diverso dal dispositivo contenente la chiave"</i> con <i>"separatamente dal dispositivo che la contiene"</i>. • Punti 3, 4: inserito <i>"nel caso in cui intenda"</i> e sostituito <i>"con"</i> con <i>"seguire"</i>. • Inserito punto 10: <i>"utilizzare il certificato con le sole modalità e finalità descritte nel Manuale Operativo."</i>
3	3.1.3	<ul style="list-style-type: none"> • Modificato titolo paragrafo con <i>"accedono per la verifica delle"</i> al posto di <i>"verificano le"</i>. • Modificati i riferimenti alle norme di legge nei vari punti. • Punto 1: sostituiti <i>"assicurarsi"</i> con <i>"verificare"</i>. • Inserito Punto 3 (in parte modificando il punto 2): <i>"conoscere, se presenti nel certificato, le seguenti informazioni: qualifiche specifiche del titolare, limiti d'uso del certificato, limiti di valore degli atti unilaterali e dei contratti per i quali il certificato può essere utilizzato;"</i>. • Punto 4: modificato <i>"questo"</i> con <i>"il"</i> ed aggiunto <i>"e del titolare"</i>. • Aggiunto <i>"o col titolare"</i> nell'ultimo paragrafo.
3	3.1.4	<ul style="list-style-type: none"> • Inserito intero paragrafo <i>"Obblighi del terzo interessato"</i>.
3	3.2	<ul style="list-style-type: none"> • Aggiunto riferimento all'articolo 38/3/e.
3	3.2.2	<ul style="list-style-type: none"> • Aggiornati i riferimenti alle norme di legge. • Aggiunti importi in lettere. • Aggiunta la frase <i>"Le limitazioni agli indennizzi sono indicate nel contratto di servizio"</i>.
3	3.3	<ul style="list-style-type: none"> • Aggiunta riferimento all'articolo 38/3/f.
4		<ul style="list-style-type: none"> • Eliminata la frase <i>"Questa sezione fa riferimento agli articoli art. 45/3 g, h, i, m, e, n, o, p, q, r e alle indicazioni descritte nello standard RFC 2527, sezione 4.3 (identification and authentication), 4.4 (operational requirements), 4.5 (physical, procedural, and personnel security controls). Le regole generali fanno altresì riferimento al fatto che BMPS partecipa al circuito IdenTrust e sottostà agli obblighi che lo stesso descrive, nel rispetto delle convenzioni operative che i diversi ambiti di utilizzo richiedono."</i>
4	4.1	<ul style="list-style-type: none"> • Inseriti punti 1, 2, 3, 4, 5, 11. • Modificati e/o tolti nei restanti punti i riferimenti alle norme di legge. • Inserita la frase <i>"Talune figure professionali possono svolgere più funzioni tra loro compatibili."</i>

4	4.2	<ul style="list-style-type: none"> • Aggiunto riferimento all'articolo 38/3/g.
4	4.2.1	<ul style="list-style-type: none"> • Punto 1: sostituito "<i>un valido documento di identità</i>" con "<i>documento di identità o un documento di riconoscimento equipollente ai sensi dell'art. 35 del [DPR 445].</i>" • Eliminato "<i>il proprio tesserino fiscale rilasciato dal Ministero delle Finanze.</i>"; precedentemente al punto 2. • Sostituito "<i>(ai sensi dell'art. 22, comma 1, del [DPCM])</i>" con "<i>con relative condizioni contrattuali</i>" ed aggiunto "<i>in presenza dell'operatore di registrazione</i>". • Punto 4: inserito "<i>provincia</i>". • Punto 6, 7, 8, 9: inserito "<i>facoltativo</i>" al posto di "<i>se disponibile</i>". • Punto 11: inserito "<i>o del documento di riconoscimento equipollente</i>". • Inserito punto 15. • Sostituito "<i>comunicare col richiedente</i>" con "<i>trasmissioni con valore giuridico secondo quanto disposto dall'art. 45 comma 2 del [DLGS 82]</i>". • Punti 17, 18, 19, 20, 21: aggiornati i riferimenti alle norme di legge.
4	4.2.1	<ul style="list-style-type: none"> • Sostituito "<i>all'art. 11, comma 3, lettera c, del [DPCM]; nel caso in cui sia richiesta l'indicazione nel certificato di abilitazioni professionali (es. l'appartenenza ad un ordine professionale), il richiedente deve produrre idonea documentazione a dimostrazione della effettiva sussistenza secondo quanto stabilito ai sensi dell'art. 29-quinquies del [DPR445]. Una fotocopia di tale documentazione viene trattenuta dal certificatore.</i>" con "<i>alla lettera a), comma 3 dell'art. 28 del [DLGS 82] e successive correzioni ed integrazioni, nel caso in cui sia richiesta, dal titolare o dal terzo interessato, l'indicazione nel certificato di abilitazioni professionali (es. l'appartenenza ad un ordine professionale, l'iscrizione ad un albo o la qualifica di pubblico ufficiale), il richiedente deve produrre un certificato rilasciato dall'Ordine di appartenenza o un'autocertificazione ai sensi dell'art. 46 del [DPR 445]</i>". • Sostituito "<i>Il richiedente può attestare stati, fatti e qualità personali anche mediante auto-certificazione ai sensi della Legge 15/86.</i>" con "<i>L'inserimento nel certificato di tali informazioni è subordinabile a preventivi accordi del certificatore con i singoli enti cui compete la gestione e la tenuta degli albi, elenchi e registri professionali.</i>".
4	4.2.1.2	<ul style="list-style-type: none"> • Aggiornati i riferimenti alle norme di legge. • Inserito "<i>dal titolare o dal terzo interessato</i>".
4	4.2.1.3	<ul style="list-style-type: none"> • Sostituito "<i>azienda, associazione, ente, etc.</i>" con "<i>ente di diritto privato o di diritto pubblico, etc.</i>" e "<i>deve essere redatta una lettera ufficiale su carta intestata, recante data e n° di protocollo, nella quale l'organizzazione segnala al certificatore i dati di tutte le persone delle quali si chiede la certificazione</i>" con "<i>salvo diversa pattuizione tra il certificatore e l'organizzazione, deve essere presentata una comunica-</i>

		<p>zione su carta intestata, recante data e numero di protocollo, nella quale l'organizzazione segnala al certificatore i dati di tutte le persone per le quali si chiede la emissione di un certificato".</p> <ul style="list-style-type: none"> • Punto 5: sostituito "la posizione all'interno dell'organizzazione" con "unità organizzativa di appartenenza del titolare (se applicabile)". • Sostituita la parola "lettera" con la parola "comunicazione" ed inserita la frase "per ogni singolo nominativo indicato". • Punto 7: inserito "dell'ente di diritto privato o denominazione dell'ente di diritto pubblico". • Inserito "per le organizzazioni di diritto privato,".
4	4.2.1.4	<ul style="list-style-type: none"> • Inserito intero paragrafo "Limiti d'uso e di valore".
	4.2.2	<ul style="list-style-type: none"> • Aggiornati i riferimenti alle norme di legge. • Punto 2: inserito ", comprensivo delle condizioni contrattuali che disciplinano l'erogazione del servizio,". • Sostituito "si concludono positivamente" con "determinano il personale convincimento dell'operatore di registrazione di aver correttamente identificato il richiedente". • Punto 7: sostituito "provvede a far controfirmare il modulo di registrazione alla Direzione della filiale ed archivia l'originale (il modulo viene conservato per almeno 10 anni)" con "controfirma il modulo di registrazione ed archivia l'originale. Ai sensi dell'art. 32 comma 3, lettera j) del [DLGS 82] e successive correzioni ed integrazioni, il modulo è conservato per almeno 20 anni". • Inserito punto 8: "consegna al richiedente copia del modulo compilato con le relative condizioni contrattuali". • Punto 9: sostituito "verificate" con "l'esito positivo delle verifiche svolte". • Inserito "Nel caso il richiedente ricopra più ruoli, per ciascuno dei ruoli sarà assegnato un diverso identificativo univoco e sarà rilasciato un diverso certificato.".
4	4.2.3	<ul style="list-style-type: none"> • Inserito paragrafo "Dispositivo di firma".
4	4.2.3.1	<ul style="list-style-type: none"> • Sostituito "Al termine della procedura di registrazione, il certificatore fornisce al richiedente un dispositivo di firma conforme agli art. 6 e art. 10, comma 5 del [DPCM], corredato di Personal Identification Number (PIN) e relativo software per firma digitale. Viene inoltre fornito uno strumento per la verifica delle firme conforme all'art. 10, comma 6 del [DPCM]." ex paragrafo 4.2.3, con "Il certificatore può fornire al richiedente un dispositivo sicuro per la generazione delle firme conforme alle caratteristiche ed ai requisiti di sicurezza di cui all'art. 35 del [DLGS 82] ed all'art. 9 comma 1, 2 e 3 del [DPCM] . Il dispositivo di firma può essere fornito al richiedente anche da una terza parte, purché il dispositivo sia conforme alle caratteristiche ed ai requisiti di sicurezza di cui all'art. 35 del [DLGS 82] ed all'art. 9 comma 1, 2 e 3 del DPCM] e sia espressamente indicato dal certificatore".
4	4.2.3.2	<ul style="list-style-type: none"> • Eliminato l'ex paragrafo "4.2.4 accordi di certificazione:".

		<p><i>A seguito di un accordo di certificazione ai sensi dell'art. 21 del [DPCM], è previsto il rilascio di un certificato a favore di un altro certificatore. In questo caso, l'identificazione e la registrazione del richiedente avvengono in modo analogo a quanto già descritto nelle sezioni precedenti, con le seguenti differenze: vengono raccolte informazioni aggiuntive sul richiedente (tra cui il DN identificativo del certificatore richiedente); vengono svolte verifiche aggiuntive, inclusa la verifica che il certificatore richiedente sia iscritto nell'elenco pubblico dei certificatori tenuto da CNIPA ai sensi dell'art. 15 del [DPCM]; non è prevista la fornitura al certificatore richiedente di alcun dispositivo di firma." a favore di questo paragrafo 4.2.3.2 "Prima di essere utilizzato per generare firme digitali, il dispositivo di firma deve essere "personalizzato" ai sensi dell'art. 9, comma 4 del [DPCM], con modalità stabilite dal certificatore. In generale, la personalizzazione del dispositivo di firma è svolta sotto il controllo dell'utente e si basa su interazioni sicure con il certificatore (generalmente connessioni tramite la rete Internet protette da protocolli che garantiscano un alto livello di sicurezza come quello definito SSLv3) in questa fase, il richiedente è riconosciuto dal certificatore tramite un codice personale riservato o una password. La personalizzazione del dispositivo di firma può essere anche fatta dal certificatore o da una terza parte che operi su delega del certificatore (tale delega è disciplinata da un accordo scritto)."</i></p>
4	4.3	<ul style="list-style-type: none"> • Inserito riferimento all'articolo 38/3/h. • Aggiornati i riferimenti alle norme di legge. • Inserito "Le chiavi hanno le caratteristiche previste dagli artt. 4 e 53, comma 1 del [DPCM]." • Inserito "La generazione delle chiavi avviene all'interno del dispositivo sicuro per la generazione delle firme. Nel caso in cui la generazione avvenga al di fuori di tale dispositivo, il sistema di generazione è conforme alle disposizioni di cui all'art. 8 del [DPCM]."
4	4.3.1	<ul style="list-style-type: none"> • Aggiornati i riferimenti alle norme di legge. • Inserito "Previa autorizzazione del CNIPA, le chiavi di certificazione possono essere utilizzate per finalità diverse da quelle indicate all'art. 4, comma 4, lettera b)."
4	4.3.2	<ul style="list-style-type: none"> • Aggiornati i riferimenti alle norme di legge.
4	4.3.3	<ul style="list-style-type: none"> • Sostituito "Le chiavi di sottoscrizione (IdenTrust Identity Profile) sono generate sul dispositivo di firma stesso (smart card) a cura del certificatore. Il dispositivo di firma (smart card) viene consegnato all'utente unitamente al PIN di attivazione. Tale codice sarà utilizzato dall'utente per accedere al dispositivo, in fase di attivazione dello stesso. Al termine della fase di richiesta e registrazione del certificato sul dispositivo, l'utente deve cambiare il codice PIN, per rendere il dispositivo definitivamente operativo. Questo codice di accesso, che consente l'utilizzo della chiave privata, deve essere fornito dal titolare ogni volta che egli intende apporre una firma tramite l'uso del dispositivo, secondo quanto ri-

		<p><i>chiesto dall'art. 10, comma 4."</i> con <i>"Le chiavi di sottoscrizione degli utenti sono generate dagli utenti stessi o dal certificatore, rif. art. 6, comma 2, del [DPCM], attivando con il software approvato dal certificatore il dispositivo sicuro per la generazione della firma fornito o indicato dallo stesso certificatore. La generazione delle chiavi di sottoscrizione sul dispositivo sicuro per la generazione della firma richiede da parte dell'utente la digitazione del PIN del dispositivo."</i></p>
4	4.4	<ul style="list-style-type: none"> • Cambiato titolo in <i>"Modalità di emissione dei certificati"</i>. • Aggiunto riferimento all'articolo (38/3/i/l). • Punto 1: inserito <i>"richiesta contenente la"</i>. • Punto 4: sostituito <i>"di"</i> con <i>"sicuro per la generazione della"</i>. • Inserito <i>"Procedure analoghe, sempre aderenti alla normativa vigente, possono essere adottate in accordo con il cliente per particolari tipologie di servizi."</i>
4	4.4.1	<ul style="list-style-type: none"> • Sostituito <i>"dal protocollo SSL (Secure Sockets Layer)"</i> con <i>"di connessioni protette dal protocollo SSLv3"</i>. • Aggiornati i riferimenti alle norme di legge.
4	4.4.2	<ul style="list-style-type: none"> • Aggiornati i riferimenti alle norme di legge. • Inserito punto 7: <i>"la generazione del certificato è registrata nel giornale di controllo."</i> • Cambiato il periodo di validità del certificato. • Inserito <i>"La presenza di uno degli OID indicati nel paragrafo 4.4.3 e l'indirizzo del sito di distribuzione del Manuale Operativo nel campo Certificate Policies indica che il certificato emesso è un certificato qualificato ai sensi dell'articolo 28, comma 1, lettera a) del [DLGS 82]. Per certificati già emessi conformemente all'art. 4, comma 5, lettera f) della [Delibera 4], l'indicazione che il certificato è qualificato è rappresentata dal valore id-etsi-qcs-QcCompliance presente nell'estensione qcStatement."</i>
4	4.4.3	<ul style="list-style-type: none"> • Inserito intero paragrafo <i>"Policy supportate"</i>
4	4.4.4	<ul style="list-style-type: none"> • Aggiornati i riferimenti alle norme di legge. • Inserito punto 2: <i>"il certificato e la relativa marca temporale vengono inviati all'utente tramite posta elettronica, all'indirizzo fornito in fase di registrazione:"</i> • Eliminato <i>"art. 28 del [DPCM]"</i>. • Eliminato <i>"e la relativa marca temporale"</i>. • Eliminato <i>"A seguito di un accordo di certificazione ai sensi dell'art. 21 del [DPCM], è previsto il rilascio di un certificato a favore di un altro certificatore. In questo caso, la richiesta e l'emissione del certificato avvengono in modo analogo a quanto già descritto nelle sezioni precedenti, con le seguenti differenze:</i> <ul style="list-style-type: none"> ▪ <i>la richiesta di certificazione deve essere consegnata di persona all'operatore di registrazione, memorizzata su supporto magnetico;</i> ▪ <i>il codice riservato per l'autenticazione delle richieste di sospensione/revoca viene fornito al richiedente in busta chiusa."</i>

4	4.5	<ul style="list-style-type: none"> • Inserito riferimento all'articolo 38/3/m. • Sostituito <i>"secondo le modalità e procedure seguenti"</i> con <i>"secondo le modalità e le procedure descritte nei paragrafi successivi. La revoca di un certificato causa la cessazione anticipata e definitiva della sua validità, la sospensione interrompe la validità di un certificato e ne prevede il ripristino o la revoca definitiva, secondo la policy concordata dal certificatore con il Cliente, dopo un periodo di tempo predefinito. Il codice identificativo del certificato revocato è inserito in una delle liste dei certificati revocati e sospesi. L'efficacia della revoca o della sospensione decorre dal momento della pubblicazione in una delle liste dei certificati revocati e sospesi."</i>
4	4.5.1	<ul style="list-style-type: none"> • Sostituito <i>"La sospensione o revoca del certificato avviene, nel rispetto degli artt. da 29 a 36 del [DPCM], secondo le modalità e procedure seguenti"</i> con <i>"La revoca può avvenire in seguito alle seguenti circostanze"</i>. • Inserito punto 2: <i>"smarrimento, furto o guasto del dispositivo sicuro per la firma;"</i>. • Inserito punto 5: <i>"compromissione della chiave privata;"</i>. • Inserito punto 6: <i>"compromissione del codice di attivazione del dispositivo sicuro per la firma;"</i>. • Inserito punto 7: <i>"variazione dei dati presenti nel certificato;"</i>. • Inserito punto 8: <i>"mancato rispetto del manuale operativo;"</i>. • Punto 9: sostituito <i>"del certificatore"</i> con <i>"dell'autorità"</i>. • Sostituito <i>"Il certificatore procede alla sospensione del certificato (in luogo della revoca) nel caso in cui non abbia la possibilità di accertare in tempo utile l'autenticità della richiesta di revoca."</i> con <i>"La sospensione può avvenire in seguito alle seguenti circostanze:</i> <ul style="list-style-type: none"> ▪ <i>richiesta di revoca di cui non è possibile accertare in tempo utile l'autenticità;</i> ▪ <i>interruzione della validità del certificato per inutilizzo temporaneo.</i> <p><i>Il certificatore revoca o sospende il certificato di sua iniziativa, per richiesta del Titolare o del Terzo Interessato, per esecuzione di un provvedimento dell'autorità."</i></p>
4	4.5.2	<ul style="list-style-type: none"> • Sostituito <i>"della procedura"</i> con <i>"delle procedure utilizzabili"</i>.
4	4.5.2.1	<ul style="list-style-type: none"> • Punto 2: <i>eliminato "(cfr. il paragrafo "Pubblicazione del certificato</i> • <i>")."</i> • Inserito punto 6: <i>"la data e ora di decorrenza della sospensione o revoca;"</i>.
4	4.5.3	<ul style="list-style-type: none"> • Aggiornati i riferimenti alle norme di legge. • Inserito punto 3: <i>"codice fiscale o partita IVA del richiedente;"</i>. • Inserito punto 10: <i>"la data e ora di decorrenza della so-</i>

		<p><i>suspensione o revoca".</i></p> <ul style="list-style-type: none"> • Inserito <i>"La lettera è accompagnata dalla documentazione giustificativa che dimostri la legittimità del ruolo di "terzo interessato" nei confronti dello specifico titolare."</i> • Inserito nel punto 11 <i>"o la sospensione"</i>.
4	4.5.4	<ul style="list-style-type: none"> • Aggiornati i riferimenti alle norme di legge.
4	4.5.5	<ul style="list-style-type: none"> • Inserito <i>"segretezza della"</i> e <i>"privata"</i>.
4	4.6	<ul style="list-style-type: none"> • Inserito riferimento all'articolo 38/3/n.
4	4.6.1	<ul style="list-style-type: none"> • Aggiornati i riferimenti alle norme di legge. • Inserita la frase <i>"Anche per il rinnovo, l'interazione con l'utente avviene tramite il canale di comunicazione sicura."</i>
4	4.6.2	<ul style="list-style-type: none"> • Aggiornati i riferimenti alle norme di legge.
4	4.6.3	<ul style="list-style-type: none"> • Aggiornati i riferimenti alle norme di legge.
4	4.7	<ul style="list-style-type: none"> • Inserito riferimento all'articolo 38/3/o.
4	4.7.1	<ul style="list-style-type: none"> • Inserita la frase <i>"Nel resto di questa sezione, i termini "registro dei certificati" e "directory (server)" sono usati in modo equivalente."</i>
4	4.7.2	<ul style="list-style-type: none"> • Sostituito <i>"Ai sensi dell'art. 44, comma 3, del [DPCM], lo svolgimento delle operazioni che modificano il contenuto del registro dei certificati è possibile solo per il personale espressamente autorizzato. In ogni caso, tutte le operazioni che modificano il contenuto del registro dei certificati vengono tracciate nel giornale di controllo (art. 44, comma 3, del [DPCM]). Il registro dei certificati è sottoposto ad un monitoraggio che permette di rilevare e segnalare gli eventi di cui all'art. 44, commi 2 e 5, del [DPCM]."</i> con <i>"Lo svolgimento delle operazioni che modificano il contenuto del registro dei certificati è possibile solo per il personale espressamente autorizzato. In ogni caso, tutte le operazioni che modificano il contenuto del registro dei certificati vengono tracciate nel giornale di controllo. Ad ogni evento registrato nel giornale di controllo è apposta un riferimento temporale contenente la data e l'ora - rif. art. 39, comma 2, del [DPCM]. Il registro dei certificati è sottoposto ad un monitoraggio che permette di rilevare e segnalare qualsiasi evento che comprometta i requisiti di sicurezza."</i>
4	4.7.3	<ul style="list-style-type: none"> • Aggiornati i riferimenti alle norme di legge. • Punto 1: inserito <i>"che ne hanno autorizzato la pubblicazione"</i>. • Inserita la frase <i>"Le liste dei certificati revocati e sospesi ed i certificati qualificati resi accessibili alla consultazione del pubblico sono utilizzabili secondo le finalità di cui all'art. 29, comma 3 del [DPCM]. Un riferimento temporale (data/ora) attesta la pubblicazione di una CRL."</i> • Punto 7: sostituito <i>"almeno una volta al giorno"</i> con <i>"secondo una frequenza dipendente dalla tipologia di policy"</i>.
4	4.7.4	<ul style="list-style-type: none"> • Eliminato <i>"Nel rispetto dell'art. 43, comma 3, del [DPCM]"</i>.
4	4.8	<ul style="list-style-type: none"> • Inserito riferimento all'articolo 38/3/p.
4	4.8.1	<ul style="list-style-type: none"> • Aggiornati i riferimenti alle norme di legge.

		<ul style="list-style-type: none"> • Inserita la frase <i>"Il certificatore si riserva la facoltà di rendere disponibili anche ulteriori modalità di accesso."</i>.
4	4.8.2	<ul style="list-style-type: none"> • Inserito nuovo paragrafo <i>"Controllo degli accessi: Il registro dei certificati è accessibile in lettura a chiunque mentre l'accesso in scrittura o modifica è consentito solo alle persone autorizzate."</i>.
4	4.9	<ul style="list-style-type: none"> • Aggiunto riferimento all'articolo 38/3/q.
4	4.9.1	<ul style="list-style-type: none"> • Eliminato <i>"ai sensi dell'art. 28 del [DPCM]"</i>. • Sostituito <i>"Dati personali - comunque di natura non riservata - sono contenuti anche nei certificati, i quali tuttavia devono essere resi pubblici nel rispetto da quanto stabilito dalla legge [L675]; di conseguenza, gli archivi contenenti certificati (per es. il registro dei certificati) non sono considerati nell'ambito delle misure di protezione della riservatezza descritte di seguito."</i> con <i>"Il database di registrazione, infatti, contiene dati personali raccolti direttamente dalla persona cui si riferiscono o previo suo esplicito consenso. I dati obbligatori sono indispensabili per il rilascio del certificato qualificato. Al richiedente, nell'ambito del contratto di servizio, è fornita l'informativa di cui all'art. 13 del [DLGS 196]. I dati personali presenti nel certificato sono utilizzabili unicamente per l'identificazione del titolare della firma, per legittimare la sottoscrizione di un documento informatico e per indicare eventualmente le funzioni del titolare. Dati personali - comunque di natura non riservata - contenuti nei certificati, sono resi pubblici su richiesta del titolare e comunicati a terzi nei casi consentiti dal titolare e nel rispetto del [DLGS 196]. Una parte delle informazioni di registrazione viene inizialmente raccolta su supporti cartacei e successivamente trasferita su supporto informatico; i supporti cartacei, in ogni caso, sono archiviati e gestiti come descritto nel paragrafo successivo."</i> • Sostituito <i>"Ai sensi dell'art. 23, comma 3, del [DPCM], le informazioni memorizzate nel database di registrazione vengono conservate almeno per 10 anni."</i> con <i>"Le informazioni memorizzate nel database di registrazione vengono conservate almeno per 20 anni."</i>
4	4.9.2	<ul style="list-style-type: none"> • Riscritto l'intero paragrafo in base alle nuove norme di legge.
4	4.10	<ul style="list-style-type: none"> • Sostituito il vecchio paragrafo con <i>"Modalità per l'apposizione e la definizione del riferimento temporale"</i>.
4	4.11	<ul style="list-style-type: none"> • Eliminato il vecchio paragrafo 4.11.
4	4.12	<ul style="list-style-type: none"> • Inserito intero paragrafo <i>"Modalità operative per l'utilizzo del sistema di verifica delle firme art. 38/3/s)"</i>.
4	4.13	<ul style="list-style-type: none"> • Inserito intero paragrafo <i>"modalità operative per la generazione della firma digitale (art. 38/3/t)"</i>.
5	5	<ul style="list-style-type: none"> • Aggiornati i riferimenti alle norme di legge. • Sostituito <i>"Titolo III"</i> con <i>"Titolo IV"</i>.
5	5.2	<ul style="list-style-type: none"> • Sostituito <i>"BMPS"</i> con <i>"Actalis"</i>. • Eliminato <i>"([DPCM] 8/2/99)"</i>.

Legenda di copertina

Stato del documento

Le firme sulla copertina del presente documento fanno riferimento allo standard interno di Banca Monte dei Paschi di Siena S.p.A. per la gestione della documentazione di servizio: hanno lo scopo di permetterne il controllo di configurazione e di indicarne lo stato di lavorazione.

Si segnala che la firma di approvazione autorizza la circolazione del documento limitatamente alla lista di distribuzione e non implica in alcun modo che il documento sia stato revisionato e/o accettato da eventuali Enti esterni.

In particolare, il documento è da intendersi **REDATTO** se provvisto della/e firma/e di chi lo ha redatto; **VERIFICATO** se ha superato con esito positivo la verifica interna e quindi provvisto della/e firma/e di verifica che ne autorizza il rilascio alla GESTIONE DELLA CONFIGURAZIONE. Nel caso in cui la revisione abbia esito negativo il documento viene modificato e verificato, con un nuovo numero di versione e una nuova data di emissione. Il documento è da intendersi **APPROVATO** se provvisto della firma di approvazione che si aggiunge alle altre.

Un documento sprovvisto di firme è in uno stato indefinito, e non può essere messo in circolazione.

Distribuzione

La distribuzione di un documento può essere:

- **PUBBLICA**, se il documento può circolare senza restrizioni;
- **INTERNA**, se il documento può circolare solo all'interno di banca monte dei paschi di siena s.p.a.;
- **RISTRETTA**, se il documento è distribuibile ad un numero limitato di destinatari;
- **CONTROLLATA**, se il documento è distribuibile ad un numero limitato di destinatari e ogni copia è controllata.

INDICE DELLE FIGURE

<i>Figura 1: identificazione e registrazione degli utenti</i>	29
<i>Figura 2: richiesta, generazione e rilascio del certificato</i>	35
<i>Figura 3: sospensione o revoca del certificato su richiesta del titolare</i>	38

SOMMARIO

• 1. GENERALITÀ	17
1.1 Scopo del documento	17
1.2 Riferimenti alle norme di legge	17
1.3 Convenzioni di lettura	18
1.4 Riferimenti agli standard	19
1.5 Definizioni ed acronimi	19
• 2. INTRODUZIONE	21
2.1 Dati identificativi del certificatore (art. 38/3/a)	21
2.2 Dati identificativi del documento	21
2.3 Versione del manuale operativo (art. 38/3/b)	21
2.4 Responsabile del manuale operativo (art. 38/3/c)	22
• 3. REGOLE GENERALI	23
3.1 Obblighi del certificatore, del titolare e di quanti accedono per la verifica delle firme (art. 38/3/d)	23
3.1.1 Obblighi e responsabilità del certificatore.....	23
3.1.2 Obblighi e responsabilità del titolare.....	24
3.1.3 Obblighi di quanti accedono per la verifica delle firme	25
3.1.4 Obblighi del terzo interessato.....	26
3.2 Definizione delle responsabilità e delle eventuali limitazioni agli indennizzi (art. 38/3/e)	26
3.2.1 Limitazioni di responsabilità	26
3.2.2 Limitazioni agli indennizzi	26
3.3 Tariffe del servizio (art. 38/3/f)	27
3.4 Orari di Disponibilità del Servizio	27
• 4. ASPETTI OPERATIVI	28
4.1 Note sull'organizzazione del personale	28
4.2 Modalità di identificazione e registrazione degli utenti (art. 38/3/g)	28
4.2.1 Identificazione dei richiedenti.....	29
4.2.2 Verifiche svolte dal certificatore in fase di registrazione	32
4.2.3 Dispositivo di firma	33
4.3 Modalità di generazione delle chiavi (art. 38/3/h)	33
4.3.1 Modalità di generazione delle chiavi di certificazione.....	33
4.3.2 Modalità di generazione delle chiavi di marcatura temporale.....	34
4.3.3 Modalità di generazione delle chiavi di sottoscrizione degli utenti	34
4.4 Modalità di emissione dei certificati qualificati (art. 38/3/i/l)	34
4.4.1 Richiesta del certificato.....	35
4.4.2 Generazione del certificato	36
4.4.3 Policy supportate	37
4.4.4 Pubblicazione del certificato.....	37
4.5 Modalità di sospensione e revoca dei certificati (art. 38/3/m)	37
4.5.1 Circostanze per la sospensione o revoca del certificato	37
4.5.2 Richiesta di sospensione o revoca da parte del titolare	38
4.5.3 Richiesta di sospensione o revoca da parte del terzo interessato	39
4.5.4 Sospensione o revoca del certificato su iniziativa del certificatore	40
4.5.5 Completamento della sospensione o revoca del certificato	40

4.6	Modalità di sostituzione delle chiavi (art. 38/3/n)	41
4.6.1	Sostituzione delle chiavi di sottoscrizione degli utenti	41
4.6.2	Sostituzione delle chiavi di certificazione	41
4.6.3	Sostituzione delle chiavi di marcatura temporale	41
4.7	Modalità di gestione del registro dei certificati (art. 38/3/o)	42
4.7.1	Realizzazione del registro dei certificati	42
4.7.2	Sicurezza del registro dei certificati	42
4.7.3	Pubblicazione dei certificati e delle CRL	42
4.7.4	Repliche su più siti del registro dei certificati	43
4.8	Modalità di accesso al registro dei certificati (art. 38/3/p)	43
4.8.1	Protocolli supportati	43
4.8.2	Controllo degli accessi	43
4.9	Modalità di protezione della riservatezza (art. 38/3/q)	43
4.9.1	Archivi contenenti dati personali	43
4.9.2	Misure di tutela della riservatezza	44
4.10	Modalità per l'apposizione e la definizione del riferimento temporale (art. 38/3/r)	44
4.11	Modalità operative per l'utilizzo del sistema di verifica delle firme (art. 38/3/s)	44
4.12	Modalità operative per la generazione della firma digitale (art. 38/3/t)	45
• 5.	SERVIZIO DI MARCATURA TEMPORALE	47
5.1	Standard di riferimento	47
5.2	Precisione del riferimento temporale	47

1. GENERALITÀ

1.1 Scopo del documento

Questo documento è la nuova versione del **Manuale Operativo** relativo al servizio di certificazione chiavi pubbliche erogato da Banca Monte dei Paschi S.p.A. ai sensi del [DPR445], del [DLGS 82] e successive modifiche ed integrazioni e del [DPCM] richiesto ai fini dell'iscrizione di Banca Monte dei Paschi di Siena S.p.A. nell'elenco dei certificatori tenuto dal CNIPA ai sensi del [DM].

Questo documento è altresì richiesto dal Circuito IdenTrust per descrivere la modalità di erogazione del servizio di certificazione di firma digitale erogati all'interno del circuito cui Banca Monte dei Paschi di Siena partecipa, così come descritto nel presente documento.

La struttura di questo documento è basata sullo standard "the Internet X.509 Public Key Infrastructure Certificate policy and Certification Practices Framework [RFC2527], così come richiesto dal circuito IdenTrust, cui Banca Monte dei Paschi di Siena prende parte.

IdenTrust LLC è la società di diritto statunitense, partecipata da banche, che in qualità di "Root Certification Authority" è organo di coordinamento per la definizione delle regole per il network degli Istituti Finanziari ad essa aderenti con il ruolo di Certification Authority.

1.2 Riferimenti alle norme di legge

- **[DPR445]** Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445, "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa", pubblicato sul S. O. alla G. U. n. 42 del 20 febbraio 2001, successivamente modificato dal DL 23 gennaio 2002 n. 10, "attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche", pubblicato nella GU n. 39 del 15 febbraio 2002 e successivamente modificato dal Decreto del Presidente della Repubblica 7 aprile 2003 n. 137 "regolamento recante disposizioni di coordinamento in materia di firma elettronica a norma dell'art. 13 del DLGS 23 gennaio 2002. b.10 pubblica nella GU n 138 del 17/6/2003.
- **[DPCM]** Decreto del Presidente del Consiglio dei Ministri (DPCM) 13/01/2004, "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ", pubblicato sulla Gazzetta Ufficiale 27 aprile 2004, n. 98.
- **[DIR]** Direttiva del Parlamento europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche (Gazzetta Ufficiale delle Comunità europee L. 13 del 13 dicembre 1999).
- **[DLGS196]** Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", pubblicato nel Supplemento Ordinario n. 123 della Gazzetta Ufficiale n. 174, 29 luglio 2003, in vigore a partire dal 1 gennaio 2004.
- **[DM]** Decreto 2 luglio 2004, "Competenza in materia di certificatori di firma elettronica" pubblicato nella Gazzetta Ufficiale n. 199, 25 agosto 2004.
- **[DLGS 82]** Decreto Legislativo 7 marzo 2005, n. 82: "Codice dell'amministrazione digitale", pubblicato nella Gazzetta Ufficiale. n. 112 del 16 maggio 2005.
- **[Delibera 4]** Deliberazione 17 febbraio 2005, "Regole per il riconoscimento e la verifica del documento informatico" (Deliberazione n. 4/2005), Pubblicato nella Gazzetta Ufficiale n. 51 del 3 marzo 2005.

- **[L. 273]** Legge 11 agosto 1991, "Istituzione del Sistema Nazionale di Taratura", Pubblicato nella Gazzetta Ufficiale 6 maggio 2002, n. 104.
- **[DM 591]** Decreto Ministeriale 30 novembre 1993, N. 591, "Regolamento concernente la determinazione dei campioni nazionali di talune unità di misura del Sistema Internazionale (SI) in attuazione dell'art. 3 della Legge 11 agosto 1991, n. 273", Pubblicato in Gazzetta Ufficiale 15 febbraio 1994, n. 37.
- **[DLGS 21/01/04]** Disposizioni ulteriori di riordino del Consiglio Nazionale delle Ricerche (CNR) e Istituzione dell'Istituto Nazionale di Ricerca Metrologica (INRIM)".
- **[DLGS 159]** Decreto legislativo 4 aprile 2006, n. 159 "Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale", Pubblicato in Gazzetta Ufficiale 29 aprile 2006, n. 99.
- **[DLGS 20/03/06]** Decreto legislativo recante "modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, a norma dell'articolo 10 della legge delega 29 luglio 2003, n. 229".

1.3 Convenzioni di lettura

L'azienda Banca Monte dei Paschi di Siena S.p.A., erogatrice del servizio di certificazione, è indicata con la sola sigla "BMPS".

In alcuni dei titoli e sottotitoli di questo documento è stato riportato tra parentesi l'articolo, comma e lettera di riferimento del [DPCM]; specifici riferimenti allo standard RFC 2527 sono altresì indicati.

Col termine "Manuale Operativo" si intende sempre fare riferimento alla *versione corrente* del Manuale Operativo (vedere la sezione 2.3).

Il termine Certificate Practice Statement ha lo stesso significato di Manuale operativo.

1.4 Riferimenti agli standard

- **[LDAP2]** W. Yeong, T. Howes, S. Kille, "Lightweight Directory Access Protocol", Internet RFC 1777, March 1995.
- **[PKCS1]** B. Kaliski, "PKCS#1: RSA Encryption - Version 1.5", Internet RFC 2313, March 1998.
- **[PKCS10]** B. Kaliski, "PKCS#10: Certification Request Syntax - Version 1.5", Internet RFC 2314, March 1998.
- **[SHA1]** ISO/IEC 10118-3:1998, "Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions", May 1998.
- **[X500]** ITU-T Recommendation X.500 (1997 E), "Information Technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services", August 1997.
- **[X509]** ITU-T Recommendation X.509 (1997 E), "Information Technology – Open Systems Interconnection – The Directory: Authentication Framework", August 1997.
- **[RFC2527]** Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- **[RFC 3161]** RFC 3161 (2001): "Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)"
- **[RFC 3280]** RFC 3280 (2002): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile"
- **[ETSI 280]** ETSI TS 102 280 v 1.1.1 – "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons" , March 2004.
- **[ETSI 862]** ETSI TS 101 862 v.1.3.2 – "Qualified Certificate profile", June 2004.

1.5 Definizioni ed acronimi

Il seguente elenco riporta il significato di acronimi ed abbreviazioni usate in questo documento:

AIPA	Autorità per l'Informatica nella Pubblica Amministrazione
CMS	Certificate Management System
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
CRL	Certificate Revocation List
CPS	Certificate Practice Statement
CRP	Codice Riservato Personale
DBMS	DataBase Management System
DN	Distinguished Name
DNS	Domain Name System
DPCM	Decreto del Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
ETSI	European Telecommunications Standards Institute
GPS	Global Positioning System

HTTP	HyperText Transfer Protocol
IEN	Istituto Elettrotecnico Nazionale
INRIM	Istituto Nazionale di ricerca Metrologica
IETF	Internet Engineering Task Force
ITSEC	Information Technology Security Evaluation Criteria
LDAP	Lightweight Directory Access Protocol
OID	Object Identifier
PDF	Portable Document Format
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman
SHA-1	Secure Hash Function 1
SSL	Secure Sockets Layer
TCP	Transport Control Protocol
TSS	Time Stamping Server
TST	Time Stamping Token
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

2. INTRODUZIONE

2.1 Dati identificativi del certificatore (art. 38/3/a)

Il servizio di certificazione è erogato dall'organizzazione identificata come segue:

Denominazione sociale:	Banca Monte dei Paschi di Siena S.p.A.
Indirizzo della sede legale:	Piazza Salimbeni, 3 – 53100 Siena
Legale rappresentante:	Avv. Giuseppe Mussari
N° di iscrizione al Registro delle Imprese di Milano:	R.E.A. n. 00884060526
N° di Partita IVA:	00884060526
N° di telefono (centralino):	0577/294111
ISO Object Identifier (OID):	18774
Sito web generale (informativo):	http://ca.mps.it
Sito web del servizio di certificazione:	http://ca.mps.it
E-mail (informativo):	info@banca.mps.it
Directory Server (registro dei certificati)	Ldap://ldap.mps.it

2.2 Dati identificativi del documento

Il presente documento, denominato Manuale Operativo, è individuato dal codice di documento 1030 18774.1.1.1.1 – 2006 – 01 - 01 e dall'OID seguente: 18774.

2.3 Versione del manuale operativo (art. 38/3/b)

Il presente documento è il Manuale Operativo relativo al servizio di certificazione chiavi pubbliche erogato da BMPS ai sensi del [DLGS 82] e successive correzioni ed integrazioni e del [DPCM]. Il codice interno di questo documento è riportato su frontespizio e nel paragrafo precedente.

Questo documento è pubblicato sul sito Web del certificatore ed è quindi consultabile telematicamente ai sensi dell'art. 38, comma 2, del [DPCM].

→ Come *versione corrente* del Manuale Operativo si intenderà esclusivamente la versione in formato elettronico disponibile sul sito Web del certificatore oppure quella pubblicata sul sito Web della CNIPA. In ogni caso, farà fede la versione pubblicata sul sito web CNIPA.

Il documento è pubblicato in formato PDF protetto in modo tale da assicurarne l'integrità; inoltre è possibile accedere al documento col protocollo HTTPS (http su SSLv3), in modo tale che il consultatore sia garantito, grazie al meccanismo di "server authentication" insito nel protocollo SSL, circa la provenienza del documento stesso.

2.4 Responsabile del manuale operativo (art. 38/3/c)

Il responsabile di questo manuale operativo è:

Enrico Fatucchi (Enrico.Fatucchi@banca.mps.it)
Area Facility Management
Consorzio Operativo Gruppo MPS
Banca Monte dei Paschi di Siena S.p.A.

3. REGOLE GENERALI

3.1 Obblighi del certificatore, del titolare e di quanti accedono per la verifica delle firme (art. 38/3/d)

3.1.1 Obblighi e responsabilità del certificatore

Il certificatore ha l'obbligo di attenersi a quanto disposto nell'art. 32 del [DLGS 82]; è tenuto pertanto a:

- adottare tutte le misure organizzative e tecniche idonee ad evitare danno a terzi;
- identificare con certezza la persona che richiede il certificato anche nel caso in cui tale attività sia delegata a terzi;
- rilasciare e rendere pubblico il certificato elettronico nei modi e nei casi stabiliti dal [DPCM] e nel rispetto del [DLGS 196];
- specificare, nel certificato qualificato, su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della sussistenza degli stessi sulla base della documentazione presentata dal richiedente;
- attenersi alle regole tecniche stabilite dal [DPCM];
- informare i richiedenti in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
- trattare i dati personali nel rispetto del [DLGS 196] e successive modificazioni, predisponendo tutele rispondenti almeno alle misure minime stabilite nello stesso decreto legislativo. Limitatamente al servizio erogato sulla base del Manuale Operativo, il certificatore non tratta "dati particolari" ovvero dati sensibili ai sensi dell'art. 4 comma 1 lettera d) o giudiziari ai sensi dello stesso articolo comma 1 lettera e);
- non rendersi depositario di dati per la creazione della firma del titolare;
- procedere alla pubblicazione della revoca e della sospensione del certificato nei casi di cui all'art. 32, comma 3, lettera g), del [DLGS];
- garantire il funzionamento efficiente, puntuale e sicuro del registro dei certificati ed un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo;
- assicurare la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
- non copiare, né conservare le chiavi private di firma del proprietario del certificato;
- fornire, prima dell'accordo, ai richiedenti il servizio, le informazioni relative ai termini ed alla condizioni sull'utilizzo del certificato;
- garantire che solo il personale autorizzato possa effettuare inserimenti e modifiche del registro dei certificati e che l'autenticità delle informazioni sia verificabile;

- conservare le informazioni relative al certificato qualificato per venti anni;
- raccogliere i dati personali nel rispetto del [DLGS 196].

Il certificatore che rilascia certificati qualificati ha l'obbligo di operare secondo quanto previsto dal Titolo II ("Regole tecniche di base") del [DPCM]; in particolare, il certificatore accreditato ha l'obbligo di attenersi anche alle disposizioni di cui al Titolo III ("Ulteriori regole per i certificatori accreditati") e IV ("Regole per la validazione temporale per la protezione dei documenti informatici") del [DPCM].

Infine il certificatore accreditato, nel caso in cui intenda lasciare l'attività, ha l'obbligo di attenersi a quanto previsto nell'art. 37 del [DLGS 82].

La responsabilità del certificatore nei confronti dei titolari di certificato e dei terzi che vi fanno affidamento sono descritte nell'art. 30 del [DLGS 82]. In particolare il certificatore garantisce:

- l'esattezza e completezza, alla data del rilascio, delle informazioni necessarie alla verifica della firma contenute nel certificato e rispetto ai requisiti fissati per i certificati qualificati.
- Il possesso da parte del firmatario, al momento del rilascio del certificato, dei dati per la creazione della firma corrispondente ai dati per la verifica della firma riportati o identificati nel certificato.

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 (§ 4.2.1.4).

BMPS si obbliga anche ad attenersi alle regole tecniche stabilite dal circuito IdenTrust.

3.1.2 Obblighi e responsabilità del titolare

Il titolare ha l'obbligo di assicurare la custodia del dispositivo di firma e di utilizzarlo personalmente. L'utilizzo del dispositivo di firma è riconducibile al titolare a meno che non fornisca prova contraria.

Il titolare di un certificato ha inoltre l'obbligo di attenersi a tutte le disposizioni del [DPCM] che lo riguardano; in particolare, egli ha l'obbligo di:

- richiedere il certificato con le modalità previste nel manuale operativo; in particolare:
 - inoltrare al certificatore la richiesta di certificato con le modalità indicate nel Manuale Operativo,
- custodire le proprie chiavi secondo quanto previsto dall'art. 7 del [DPCM]; in particolare:
 - conservare con la massima diligenza le proprie chiavi private ed i dispositivi di firma che le contengono al fine di preservarne l'integrità e la riservatezza;
 - conservare le informazioni di abilitazione all'uso della chiave privata separatamente dal dispositivo che la contiene;
 - richiedere immediatamente la revoca delle certificazioni relative alle chiavi contenute in dispositivi di firma di cui abbia perduto il possesso o difettosi;
- nel caso in cui intenda richiedere la revoca del proprio certificato, seguire le modalità previste nell'art. 19 del [DPCM];
- nel caso in cui intenda richiedere la sospensione del proprio certificato, seguire le modalità previste nell'art. 23 del [DPCM].

Il titolare di un certificato ha anche l'obbligo di:

- prendere visione di questo Manuale Operativo prima di richiedere al certificatore di essere registrato;
- fornire al certificatore informazioni esatte e veritiere in fase di registrazione;
- custodire con la massima diligenza i codici riservati ricevuti dal certificatore, al fine di preservarne la riservatezza;
- successivamente alla registrazione e fino alla scadenza o revoca del certificato, avvisare prontamente il certificatore di ogni variazione alle informazioni fornite al certificatore in fase di registrazione (dati anagrafici, indirizzi, numeri di telefono, ruoli ricoperti, etc.);
- in caso di furto o smarrimento del proprio dispositivo di firma, informarne tempestivamente il certificatore e farne denuncia alla Autorità di Pubblica Sicurezza; una copia della denuncia deve essere inviata al certificatore;
- utilizzare il certificato con le sole modalità e finalità descritte nel Manuale Operativo.

3.1.3 Obblighi di quanti accedono per la verifica delle firme

Coloro che verificano firme digitali generate con chiavi certificate da BMPS, sono tenuti a svolgere le seguenti azioni, a prescindere dal fatto che essi accedano o meno al registro dei certificati:

- prima di usare la chiave pubblica contenuta nel certificato del sottoscrittore, assicurarsi della validità del certificato stesso; in particolare:
 - verificare che la firma apposta al certificato dal certificatore sia valida, verificando se necessario anche i certificati relativi ad accordi di certificazione;
 - verificare il periodo di validità del certificato (rif. art. 28, comma 1, lettera f, del [DLGS 82]);
 - verificare che il certificato non sia sospeso o revocato;
 - verificare la tipologia delle chiavi (rif. art. 15, comma 1, lettera b, del [DPCM]).
- Nel caso degli utenti del circuito IdenTrust, le operazioni di verifica firma sono effettuate dalle banche stesse partecipanti al circuito, cui BMPS prende parte secondo le modalità tecniche ed organizzative definite dal circuito IdenTrust stesso.
- conoscere, se presenti nel certificato, le seguenti informazioni: qualifiche specifiche del titolare, limiti d'uso del certificato, limiti di valore degli atti unilaterali e dei contratti per i quali il certificato può essere utilizzato;
- conoscere il Manuale Operativo/Certificate Practice Statement; in particolare, conoscere le limitazioni di responsabilità e di indennizzo del certificatore e del titolare.

In caso di contenzioso col certificatore o col titolare, coloro che verificano firme digitali non potranno avanzare alcuna pretesa se non adempiono agli obblighi sopra esposti.

3.1.4 Obblighi del terzo interessato

Il terzo interessato è la persona fisica o giuridica che acconsente all'inserimento nel certificato di un ruolo - rif. art. 32, comma 2 lettera c) del [DLGS 82]. Il Terzo Interessato è tenuto a:

- conoscere ed attenersi al Manuale Operativo;
- inoltrare tempestivamente le richieste di revoca o sospensione nei casi (§ 4.5.1) e con le modalità (§ 4.5.3) previste nel Manuale Operativo.

3.2 Definizione delle responsabilità e delle eventuali limitazioni agli indennizzi (art. 38/3/e)

3.2.1 Limitazioni di responsabilità

Si applicano le seguenti limitazioni, dove con "Contraente" si intende la controparte del contratto di servizio stipulato con BMPS.

- fatti salvi i limiti inderogabili di legge, la responsabilità di BMPS, a qualsiasi titolo derivanti dal contratto di servizio, sussisterà solo nei casi di dolo o colpa grave;
- BMPS non sarà responsabile della mancata esecuzione delle obbligazioni assunte con il contratto di servizio, qualora tale mancata esecuzione sia dovuta a cause non imputabili a BMPS, quali - a scopo esemplificativo e senza intento limitativo - caso fortuito, disfunzioni di ordine tecnico assolutamente imprevedibili e poste al di fuori di ogni controllo, interventi dell'autorità, cause di forza maggiore, calamità naturali, scioperi anche aziendali - ivi compresi quelli presso soggetti di cui le parti si avvalgono nell'esecuzione delle attività connesse al contratto - ed altre cause imputabili a terzi;
- BMPS, in particolare, non sarà responsabile di eventuali disservizi derivanti dal mancato rispetto, da parte del Contraente o di soggetti terzi, delle norme e specifiche tecnico-operative contenute nel contratto o da esso richiamate;
- nel caso in cui i certificati rilasciati da BMPS prevedano limitazioni all'utilizzo - tra cui limitazioni nel valore delle transazioni per le quali il certificato è valido, ovvero limitazioni negli scopi per i quali il certificato può essere utilizzato - BMPS non sarà responsabile per i danni conseguenti ad un utilizzo non conforme.

3.2.2 Limitazioni agli indennizzi

Ai sensi dell'art. 11, comma 1, lettera m, del [DPCM], la BMPS ha stipulato un'apposita assicurazione a copertura dei rischi dell'attività e degli eventuali danni derivanti dall'erogazione del servizio di certificazione.

Le limitazioni agli indennizzi, in ogni caso dipendenti dal tipo di certificato e dalle modalità operativa con cui esso è utilizzato, sono indicate nei contratti di servizio e pubblicate sul sito web del certificatore insieme alle condizioni commerciali di erogazione del servizio.

Nel caso in cui i certificati rilasciati da BMPS prevedano limitazioni all'utilizzo - tra cui limitazioni nel valore delle transazioni per le quali il certificato è valido, ovvero limitazioni negli scopi per i quali il certificato può essere utilizzato - BMPS non sarà responsabile per i danni conseguenti ad un utilizzo non conforme.

In ogni caso, il risarcimento di danni non potrà superare l'importo massimo di € 500.000,00 (cinquecentomila/00 euro) per singolo sinistro e di € 1.500.000,00 (un milione e cinquecentomila/00 euro) per annualità. Le limitazioni agli indennizzi sono indicate nel contratto di servizio.

Tali regole e limitazioni sono conformi sia alla normativa italiana sia alle regole del circuito IdenTrust.

3.3 Tariffe del servizio (art. 38/3/f)

La tariffa massima in Euro (€) per il rilascio di ogni nuovo certificato è pari ad € 65,00.

→ Le tariffe *effettivamente* applicate dipenderanno dagli specifici accordi in essere con il cliente.

3.4 Orari di Disponibilità del Servizio

Le tabelle sottostanti vanno discusse con ciascuna banca sulla base di Step 1 o Step 2.

Finestre temporali di erogazione

Servizio	Orario disponibilità richiesto	Giorni disponibilità
Servizio gestione certificati	8.00 – 18.00	Lun. – Ven.
Revoca/sospensione (terzo interessato)	8.00 – 18.00	Lun. – Ven.
Sospensione (utente)	24h	7 giorni su 7
Accesso directory (certificati, CRL, CSL)	24h	7 giorni su 7
Accesso servizio TS	24h	7 giorni su 7
Help Desk	8.00 – 18.00	Lun. – Ven.

Livelli di servizio

Parametro	Indice richiesto
Tempo max tra registrazione e pubblicazione	30' nel 95% dei casi
Tempo max emissione marca temporale	60" nel 95% dei casi
Tempo max accesso CRL/CSL	60" nel 95% dei casi
Tempo max blocco certificato da segnalazione	5' nel 95% dei casi
Disponibilità infrastrutture CA/RA	99,5% (su base mensile)
Disponibilità infrastrutture TS	99,5% (su base giornaliera)
Tempo di ripristino di disservizio entro 8 ore	99,5%

4. ASPETTI OPERATIVI

4.1 Note sull'organizzazione del personale

Il personale preposto all'erogazione e controllo del servizio di certificazione è organizzato nel rispetto dell'art. 33 del [DPCM]. In particolare, sono definite le seguenti figure organizzative:

- responsabile della sicurezza;
- responsabile della generazione e della custodia delle chiavi;
- responsabile della personalizzazione dei dispositivi di firma;
- responsabile della generazione dei certificati;
- responsabile della gestione del registro dei certificati;
- responsabile della registrazione degli utenti;
- responsabile della crittografia o di altro sistema utilizzato;
- responsabile dell'auditing (verifiche ed ispezioni);
- responsabile della sicurezza dei dati;
- responsabile dei servizi tecnici;
- responsabile del sistema di riferimento temporale.

Talune figure professionali possono svolgere più funzioni tra loro compatibili.

Le figure sopra elencate possono avvalersi, per lo svolgimento delle funzioni di loro competenza, di addetti ed operatori.

Gli operatori di registrazione possono eventualmente operare anche presso sedi remote, rispetto al centro di elaborazione dati presso BMPS, e scambiare informazioni col sito principale mediante canali di comunicazione sicuri.

In tal caso, gli addetti alla registrazione operano secondo le procedure stabilite da BMPS, e sono responsabili nei confronti di BMPS della corretta identificazione del richiedente. BMPS rimane pienamente responsabile delle operazioni di registrazione svolte presso le società terze.

4.2 Modalità di identificazione e registrazione degli utenti (art. 38/3/g)

Viene di seguito descritto il processo di identificazione di un utente che si pone per la prima volta in rapporto con BMPS.

La seguente figura illustra, in modo semplificato, la procedura di identificazione e registrazione degli utenti; la procedura si articola nelle seguenti fasi:

- sottomissione della richiesta, corredata della necessaria documentazione da parte di un terzo interessato o dal richiedente stesso, nel caso in cui il certificato venga rilasciato in nome e per conto di un'organizzazione di appartenenza o nel caso in cui il richiedente coincida con l'intestatario del certificato stesso;

- verifica delle informazioni fornite ed accettazione o rifiuto della richiesta.

In questa procedura, il richiedente, o il terzo interessato, interagisce con un operatore di registrazione, il quale opera per conto del responsabile di registrazione.

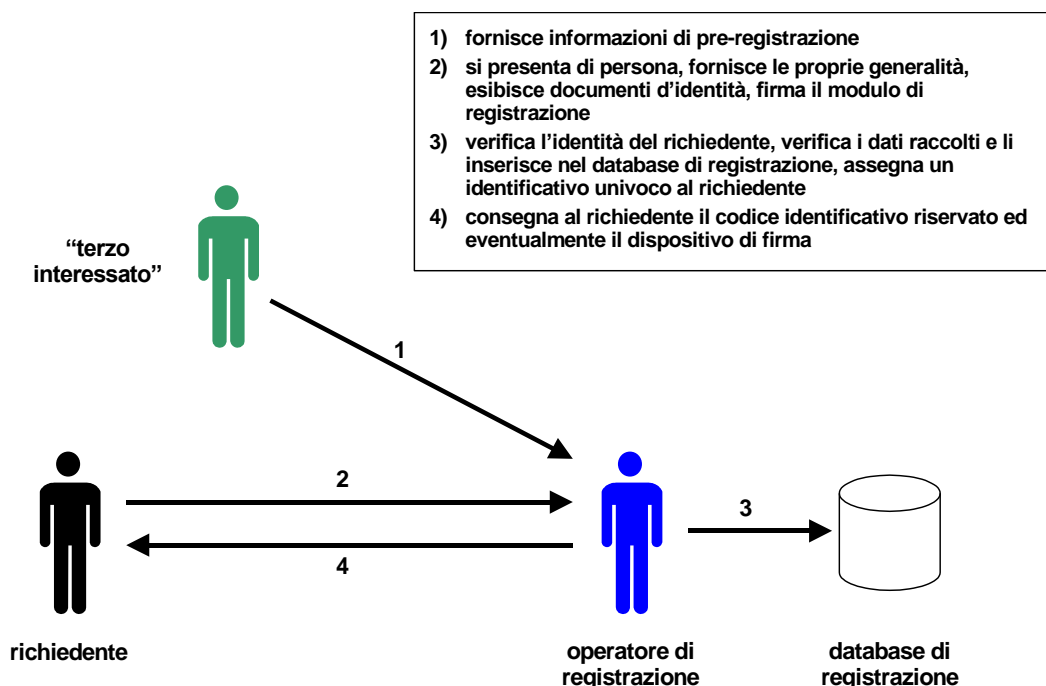


Figura 1: identificazione e registrazione degli utenti

Nel seguito di questa sezione si descrivono i dettagli della procedura.

4.2.1 Identificazione dei richiedenti

Il richiedente deve **recarsi di persona** davanti all'operatore di registrazione e dimostrare la propria identità fornendo:

- un documento di identità o un documento di riconoscimento equipollente ai sensi dell'art. 35 del [DPR 445].

Contestualmente, il richiedente deve consegnare all'operatore di registrazione un apposito **modulo di registrazione** in forma cartacea con relative condizioni contrattuali, debitamente compilato. Il modulo di registrazione deve essere **firmato dal richiedente** in presenza dell'operatore di registrazione.

Nel modulo, il richiedente fornisce le seguenti informazioni, le quali sono raccolte e memorizzate in un apposito database ("database di registrazione"):

- nome e cognome;
- data di nascita;
- comune, provincia e stato estero di nascita;
- codice fiscale;
- indirizzo di residenza (facoltativo);
- numero di telefono fisso (facoltativo);

- numero di telefono mobile (facoltativo);
- numero di fax (facoltativo);
- indirizzo di posta elettronica;
- tipo e numero del documento d'identità o del documento di riconoscimento equipollente esibito dal richiedente;
- autorità che ha rilasciato il documento d'identità e luogo del rilascio;
- eventuali abilitazioni professionali (vedere "Abilitazioni professionali");
- eventuali poteri di rappresentanza (vedere "Poteri di rappresentanza");
- eventuale pseudonimo che il certificatore può riportare nel certificato in luogo del nome di battesimo e cognome del titolare ai sensi dell'art. 33 del [DLGS 82] e della lettera e), comma 3 dell'art. 4 della [Delibera 4];
- nel caso il richiedente intenda usare la propria chiave per firma apposta con "procedura automatica" ai sensi degli artt. 4 e 10 del [DPCM]:
 - dati identificativi della procedura automatica che usa la chiave di firma (es. indirizzo DNS del server, nel caso il server sia accessibile attraverso Internet);
 - dati identificativi del sistema software utilizzato dall'organizzazione.

Tutte le informazioni sopra elencate ed applicabili sono da considerarsi obbligatorie ai fini della registrazione dell'utente e del rilascio del certificato. Il certificatore si riserva comunque di accettare richieste mancanti di alcune informazioni, valutando caso per caso se le informazioni fornite dal richiedente siano comunque sufficienti.

È responsabilità del richiedente fornire un indirizzo valido di posta elettronica, poiché il certificatore (che non verifica la validità dell'indirizzo) userà in seguito tale indirizzo per trasmissioni con valore giuridico secondo quanto disposto dall'art. 45 comma 2 del [DLGS 82].

Firmando il modulo di registrazione, il richiedente:

- fornisce tutti i dati personali necessari per la registrazione;
- si assume esplicitamente gli obblighi di cui all'art. 32, comma 1, del [DLGS 82];
- si assume esplicitamente gli obblighi di cui all'art. 7, comma 3, del [DPCM];
- dichiara di aver preso visione di questo Manuale Operativo e di averlo compreso ed accettato;
- acconsente al trattamento dei propri dati personali nel rispetto del [DLGS 196] e dell'informativa fornita.

4.2.1.1 Abilitazioni professionali

Con riferimento alla lettera a), comma 3 dell'art. 28 del [DLGS 82] e successive correzioni ed integrazioni, nel caso in cui sia richiesta, dal titolare o dal terzo interessato, l'indicazione nel certificato di abilitazioni professionali (es. l'appartenenza ad un ordine professionale, l'iscrizione ad un albo o la qualifica di pubblico ufficiale), il richiedente deve produrre un certificato rilasciato dall'Ordine di appartenenza o un'autocertificazione ai sensi dell'art. 46 del [DPR 445]. Una fotocopia di tale documentazione viene trattenuta dal certificatore.

L'inserimento nel certificato di tali informazioni è subordinabile a preventivi accordi del certificatore con i singoli enti cui compete la gestione e la tenuta degli albi, elenchi e registri professionali.

4.2.1.2 Poteri di rappresentanza

Con riferimento alla lettera a), comma 3 dell'art. 28 del [DLGS 82]: nel caso in cui sia richiesta, dal titolare o dal terzo interessato, l'indicazione nel certificato di poteri di rappresentanza (es. l'appartenenza ad un'organizzazione e la carica ivi ricoperta, l'abilitazione ad operare in nome e per conto di un terzo, etc.), il richiedente deve produrre idonea documentazione a dimostrazione della effettiva sussistenza di tali poteri di rappresentanza. Una fotocopia di tale documentazione viene trattata dal certificatore.

4.2.1.3 Appartenenza ad organizzazioni

Nel caso di appartenenza ad un'organizzazione (ente di diritto privato o di diritto pubblico, etc.), salvo diversa pattuizione tra il certificatore e l'organizzazione, deve essere presentata una comunicazione su carta intestata, recante data e numero di protocollo, nella quale l'organizzazione segnala al certificatore i dati di tutte le persone per le quali si chiede la emissione di un certificato, indicando per ciascuna:

- nome e cognome;
- il codice fiscale;
- il numero di telefono presso l'organizzazione;
- l'indirizzo di posta elettronica (mailbox) presso l'organizzazione;
- unità organizzativa di appartenenza del titolare (se applicabile);
- l'eventuale carica ricoperta all'interno dell'organizzazione.

La comunicazione deve contenere una **dichiarazione** che impegna l'organizzazione a comunicare tempestivamente al certificatore ogni variazione alle informazioni sopra elencate (fatta eccezione per nome e cognome, che non sono comunque modificabili), per ogni singolo nominativo indicato.

La comunicazione deve essere **firmata dal rappresentante Legale** dell'organizzazione o da altra persona munita di apposita procura autenticata da pubblico ufficiale.

La comunicazione deve riportare chiaramente almeno le seguenti informazioni – salvo varianti dipendenti dal particolare tipo di organizzazione – le quali vengono raccolte e memorizzate in un apposito database ("database di registrazione"):

- denominazione dell'organizzazione (es. ragione sociale dell'ente di diritto privato o denominazione dell'ente di diritto pubblico);
- indirizzo della sede legale dell'organizzazione;
- N° di Codice Fiscale;
- N° di Partita IVA (se applicabile);
- N° di iscrizione al Registro delle Imprese (se applicabile);
- nome, numero di telefono e numero di fax del rappresentante legale;
- dominio Internet registrato dall'organizzazione (se disponibile).

La data di redazione della lettera deve essere **non anteriore di 90 giorni** alla data prevista per la registrazione del primo utente appartenente all'organizzazione in discorso.

La lettera deve pervenire al certificatore **almeno una settimana prima** della data in cui si richiede la registrazione del primo utente appartenente all'organizzazione in discorso.

Alla lettera di segnalazione dei nominativi dei soggetti da certificare, per le organizzazioni di diritto privato, deve essere allegato un **certificato di iscrizione al Registro delle Imprese** rilasciato non più di 90 giorni prima della data prevista per la registrazione del primo utente appartenente all'organizzazione in discorso.

4.2.1.4 Limiti d'uso e limiti di valore

Un certificato qualificato può contenere, previo accordo tra il certificatore ed il Cliente, limiti di utilizzo compresi quelli derivanti dalla titolarità delle qualifiche e dai poteri di rappresentanza o limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere utilizzato. Gli eventuali limiti di uso e di valore sono presenti nell'attributo explicitText del campo UserNotice del certificato.

4.2.2 Verifiche svolte dal certificatore in fase di registrazione

A fronte della richiesta di registrazione, l'operatore di registrazione svolge le seguenti verifiche:

- verifica l'identità del richiedente (mediante ispezione dei validi documenti d'identità forniti);
- verifica che il modulo di registrazione, comprensivo delle condizioni contrattuali che disciplinano l'erogazione del servizio, sia correttamente compilato, datato e firmato dal richiedente;
- esamina la documentazione fornita dal richiedente a dimostrazione delle proprie abilitazioni professionali e/o poteri di rappresentanza, verificando che sia idonea allo scopo;
- confronta le informazioni fornite dal richiedente con quelle eventualmente fornite dai terzi interessati (es. dall'organizzazione di appartenenza del richiedente);
- se necessario, svolge ulteriori verifiche circa i *fatti, stati e qualità* del richiedente con le modalità consentite dalla legge.

Se le verifiche descritte determinano il personale convincimento dell'operatore di registrazione di aver correttamente identificato il richiedente, l'operatore completa la procedura secondo i seguenti passi:

- attiva il processo di consegna del **codice riservato personale (CRP)**, col quale il richiedente potrà farsi riconoscere dal certificatore in fase di colloquio remoto;
- controfirma il modulo di registrazione ed archivia l'originale. Ai sensi dell'art. 32 comma 3, lettera j) del [DLGS 82] e successive correzioni ed integrazioni, il modulo è conservato per almeno 20 anni;
- consegna al richiedente copia del modulo compilato con le relative condizioni contrattuali;
- riporta nel database di registrazione le informazioni raccolte e l'esito positivo delle verifiche svolte;
- Autorizza nel database di registrazione, l'emissione di un certificato per il richiedente.

Ai sensi dell'art. 15 comma 1, lettera a) del [DPCM], sarà assegnato al richiedente e memorizzato nel database di registrazione un **identificativo univoco**, non riservato. Nel caso il richiedente ricopra più ruoli, per ciascuno dei ruoli sarà assegnato un diverso identificativo univoco e sarà rilasciato un diverso certificato.

4.2.3 Dispositivo di firma

4.2.3.1 Fornitura e caratteristiche del dispositivo di firma

Il certificatore può fornire al richiedente un dispositivo sicuro per la generazione delle firme conforme alle caratteristiche ed ai requisiti di sicurezza di cui all'art. 35 del [DLGS 82] ed all'art. 9 comma 1, 2 e 3 del [DPCM] .

Il dispositivo di firma può essere fornito al richiedente anche da una terza parte, purché il dispositivo sia conforme alle caratteristiche ed ai requisiti di sicurezza di cui all'art. 35 del [DLGS 82] ed all'art. 9 comma 1, 2 e 3 del [DPCM] e sia espressamente indicato dal certificatore.

4.2.3.2 Accordi di certificazione

Prima di essere utilizzato per generare firme digitali, il dispositivo di firma deve essere "personalizzato" ai sensi dell'art. 9, comma 4 del [DPCM], con modalità stabilite dal certificatore.

In generale, la personalizzazione del dispositivo di firma è svolta sotto il controllo dell'utente e si basa su interazioni sicure con il certificatore (generalmente connessioni tramite la rete Internet protette da protocolli che garantiscano un alto livello di sicurezza come quello definito SSLv3) in questa fase, il richiedente è riconosciuto dal certificatore tramite un codice personale riservato o una password.

La personalizzazione del dispositivo di firma può essere anche fatta dal certificatore o da una terza parte che operi su delega del certificatore (tale delega è disciplinata da un accordo scritto).

4.3 Modalità di generazione delle chiavi (art. 38/3/h)

Le chiavi appartenenti ad una delle tipologie elencate nell'art. 4, comma 4, del [DPCM] sono generate (art. 6, comma 3), conservate (art. 7) ed utilizzate (art. 9, comma 1) all'interno di uno stesso dispositivo elettronico avente le caratteristiche di sicurezza di cui all'art. 9, comma 3 del [DPCM].

Le chiavi hanno le caratteristiche previste dagli artt. 4 e 53, comma 1 del [DPCM].

La generazione delle chiavi avviene all'interno del dispositivo sicuro per la generazione delle firme. Nel caso in cui la generazione avvenga al di fuori di tale dispositivo, il sistema di generazione è conforme alle disposizioni di cui all'art. 8 del [DPCM].

4.3.1 Modalità di generazione delle chiavi di certificazione

Questa avviene nel rispetto dell'art. 13 del [DPCM]; in particolare:

- la generazione chiavi avviene in modo conforme agli artt. 5 e 6 del [DPCM];
- per ciascuna coppia di chiavi di certificazione viene generato un certificato, firmato con la chiave privata della coppia.

Queste chiavi, ai sensi dell'art. 6, comma 1 del [DPCM], sono generate dal responsabile di certificazione.

Prima autorizzazione del CNIPA, le chiavi di certificazione possono essere utilizzate per finalità diverse da quelle indicate all'art. 4, comma 4, lettera b).

4.3.2 Modalità di generazione delle chiavi di marcatura temporale

Questa avviene nel rispetto dell'art. 46 del [DPCM]; in particolare:

- la coppia di chiavi viene univocamente associata ad un singolo sistema di validazione temporale;
- le chiavi vengono sostituite dopo non più di un mese di utilizzazione;
- per la firma dei certificati relativi alle chiavi di marcatura temporale viene utilizzata una chiave di certificazione diversa da quella utilizzata per i certificati degli utenti.

Queste chiavi, ai sensi dell'art. 6 del [DPCM], sono generate dal responsabile di certificazione.

4.3.3 Modalità di generazione delle chiavi di sottoscrizione degli utenti

Le chiavi di sottoscrizione degli utenti sono generate dagli utenti stessi o dal certificatore, rif. art. 6, comma 2, del [DPCM], attivando con il software approvato dal certificatore il dispositivo sicuro per la generazione della firma fornito o indicato dallo stesso certificatore.

La generazione delle chiavi di sottoscrizione sul dispositivo sicuro per la generazione della firma richiede da parte dell'utente la digitazione del PIN del dispositivo.

4.4 Modalità di emissione dei certificati qualificati (art. 38/3/i/I)

La seguente figura illustra, in modo semplificato, la procedura di richiesta ed emissione del certificato; la procedura si articola nelle seguenti fasi:

- generazione della coppia di chiavi ed invio della richiesta contenente la chiave pubblica al certificatore;
- verifica, da parte del certificatore, dell'autenticità e correttezza della richiesta;
- generazione e pubblicazione del certificato;
- invio del certificato al titolare ed installazione del medesimo sul dispositivo sicuro per la generazione della firma.

In questa procedura, il richiedente interagisce col certificatore con modalità telematiche (via web). Procedure analoghe, sempre aderenti alla normativa vigente, possono essere adottate in accordo con il cliente per particolari tipologie di servizi.

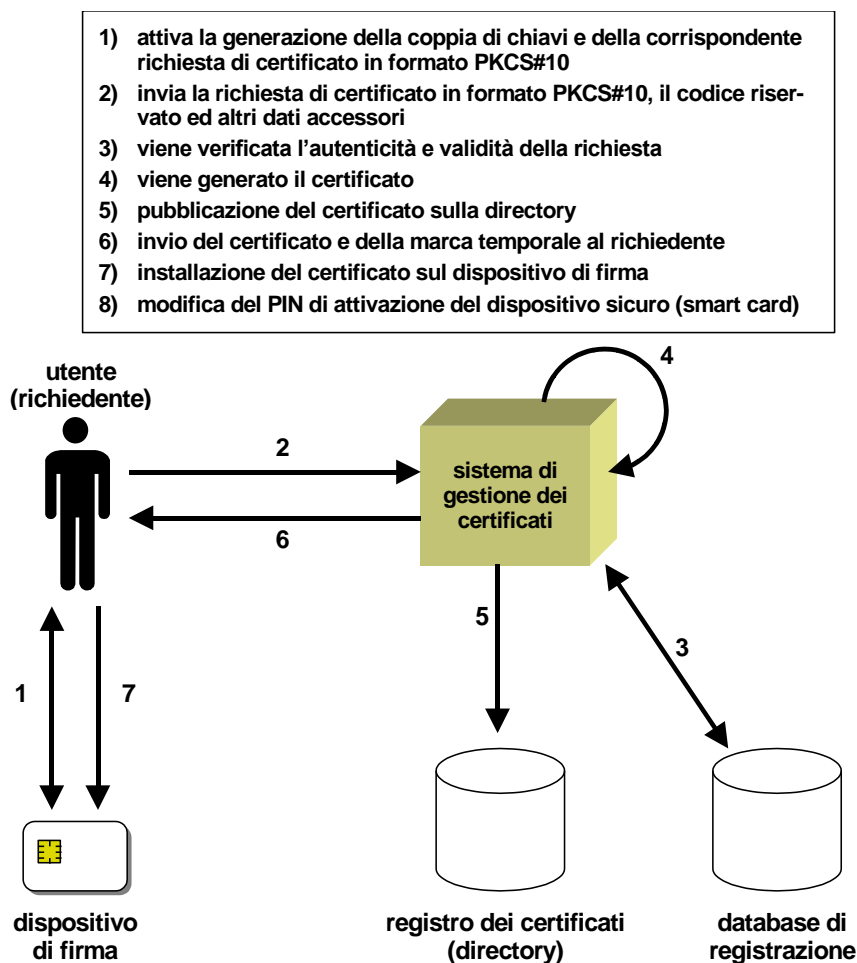


Figura 2: richiesta, generazione e rilascio del certificato

Nel seguito di questa sezione si descrivono i dettagli della procedura.

4.4.1 Richiesta del certificato

Il richiedente accede al sito web del certificatore, autenticandosi tramite il Codice Riservato Personale ottenuto in fase di registrazione.

Nel caso in cui il codice sia andato smarrito, potrà essere richiesto il rilascio di un nuovo CRP all'operatore di registrazione, previa firma di una lettera di manleva.

Il richiedente deve approntare la richiesta di certificazione della propria chiave pubblica, trasmettendo al certificatore un file di richiesta (in formato PKCS#10) contenente la chiave pubblica da certificare e firmato con la corrispondente chiave privata. In tal modo, il richiedente dimostra il possesso della coppia di chiavi.

La richiesta di certificazione deve quindi essere inviata al certificatore attraverso il "canale telematico sicuro" stabilito con il sito web del certificatore.

Il "canale telematico sicuro" è di norma ottenuto con l'uso di connessioni protette dal protocollo SSLv3 fornito nel collegamento al sito indicato dal certificatore.

La richiesta di certificazione deve essere generata mediante strumenti approvati dal certificatore.

Ai sensi dell'art. 32 comma 3, lettera j) del [DLGS 82] e successive correzioni ed integrazioni, la richiesta di certificazione viene conservata dal certificatore per almeno 20 anni.

La richiesta del certificato può essere fatta anche presso la struttura che esegue la registrazione.

4.4.2 Generazione del certificato

La generazione del certificato avviene, nel rispetto dell'art. 14 del [DPCM], secondo la seguente procedura:

- si verifica l'autenticità della richiesta di certificazione (art. 14, comma 1, lettera a) mediante interrogazione della base dati di registrazione (in particolare, si verifica il codice riservato personale del richiedente);
- si verifica il possesso della chiave privata da parte del richiedente ed il corretto funzionamento della coppia di chiavi (art. 14, comma 1, lettera b) del [DPCM] mediante validazione della firma del richiedente contenuta nella struttura dati PKCS#10;
- si verifica che la chiave pubblica non sia già stata certificata a nome di qualche altro utente; questa verifica viene svolta:
 - in primo luogo mediante ricerca nella base dati del certificatore BMPS;
 - ove possibile, anche mediante ricerca nelle basi dati degli altri certificatori iscritti nell'elenco CNIPA;
- nel caso si rilevi che la chiave è già stata certificata a nome di un titolare diverso dal richiedente:
 - la richiesta di certificazione viene rigettata;
 - il rigetto viene notificato al richiedente e al titolare del certificato preesistente;
 - l'evento viene registrato nel giornale di controllo;
 - se il richiedente ha fornito la prova del possesso della chiave privata viene inoltre avviata la procedura di revoca del certificato pre-esistente;
- se le verifiche di cui ai punti precedenti vengono superate, l'operatore di certificazione (sotto la supervisione del responsabile di certificazione) abilita la generazione del certificato, con un sistema conforme all'art. 28 del [DPCM];
- il certificato viene quindi generato col formato di cui all'art. 35 del [DPCM]; il certificato contiene le informazioni previste nell'art. 15 del [DPCM] e nell'art. 28 del [DLGS 82] e successive correzioni ed integrazioni;
- la generazione del certificato è registrata nel giornale di controllo.

Il **periodo di validità del certificato** può variare da 1 a 3 anni.

La presenza di uno degli OID indicati nel paragrafo 4.4.3 e l'indirizzo del sito di distribuzione del Manuale Operativo nel campo Certificate Policies indica che il certificato emesso è un certificato qualificato ai sensi dell'articolo 28, comma 1, lettera a) del [DLGS 82].

Per certificati già emessi conformemente all'art. 4, comma 5, lettera f) della [Delibera 4], l'indicazione che il certificato è qualificato è rappresentata dal valore id-etsi-qcs-QcCompliance presente nell'estensione qcStatement.

4.4.3 Policy supportate

Il profilo del certificato dipende dalla specifica policy utilizzata, concordata con la controparte del contratto del servizio di erogazione certificati.

BMPS supporta le seguenti policy, descritte in altrettanti documenti pubblicati sul sito web del servizio di certificazione <http://ca.mps.it>.

Policy OID	Descrizione
1.3.6.1.4.1.18774.1.1.1	Certificati qualificati per firma digitale.
1.3.6.1.4.1.18774.1.1.2	Certificati qualificati per firma digitale con limitazioni d'uso e/o di valore.

Le policy sono parte integrante del Manuale Operativo e delle condizioni contrattuali del servizio.

4.4.4 Pubblicazione del certificato

La pubblicazione del certificato avviene, nel rispetto delle regole del circuito IdenTrust e nel rispetto della normativa vigente, secondo la seguente procedura:

- sotto il controllo del responsabile della registrazione, il certificato viene pubblicato nel registro dei certificati; il momento (data/ora) della pubblicazione viene attestato con la richiesta di una marca temporale; questa è ottenuta mediante interazione col sistema di marcatura temporale predisposto dal certificatore nel rispetto degli artt. 44÷51 del [DPCM];
- il certificato viene inviato all'utente tramite posta elettronica, all'indirizzo fornito in fase di registrazione;
- la pubblicazione del certificato e la relativa marcatura temporale sono registrate nel giornale di controllo.

Il canale sicuro è ottenuto, di norma, con l'uso del protocollo SSL (Secure Sockets Layer); l'uso di altri meccanismi di sicurezza dovrà essere preventivamente concordato col certificatore.

4.5 Modalità di sospensione e revoca dei certificati (art. 38/3/m)

La sospensione o revoca del certificato avviene, nel rispetto degli artt. da 18 a 24 del [DPCM] e secondo le modalità e le procedure descritte nei paragrafi successivi. La revoca di un certificato causa la cessazione anticipata e definitiva della sua validità, la sospensione interrompe la validità di un certificato e ne prevede il ripristino o la revoca definitiva, secondo la policy concordata dal certificatore con il Cliente, dopo un periodo di tempo predefinito.

Il codice identificativo del certificato revocato è inserito in una delle liste dei certificati revocati e sospesi. L'efficacia della revoca o della sospensione decorre dal momento della pubblicazione in una delle liste dei certificati revocati e sospesi.

4.5.1 Circostanze per la sospensione o revoca del certificato

La revoca può avvenire in seguito alle seguenti circostanze:

- richiesta da parte del titolare;
- smarrimento, furto o guasto del dispositivo sicuro per la firma;
- richiesta da parte del terzo dal quale derivino i poteri del titolare;

- perdita del possesso della chiave dichiarata dal titolare o dal terzo dal quale derivino i poteri del titolare;
- compromissione della chiave privata;
- compromissione del codice di attivazione del dispositivo sicuro per la firma;
- variazione dei dati presenti nel certificato;
- mancato rispetto del manuale operativo;
- provvedimento dell'autorità;
- acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni.

La sospensione può avvenire in seguito alle seguenti circostanze:

- richiesta di revoca di cui non è possibile accertare in tempo utile l'autenticità;
- interruzione della validità del certificato per inutilizzo temporaneo.

Il certificatore revoca o sospende il certificato di sua iniziativa, per richiesta del Titolare o del Terzo Interessato, per esecuzione di un provvedimento dell'autorità.

4.5.2 Richiesta di sospensione o revoca da parte del titolare

La seguente figura illustra, in modo semplificato, la procedura di richiesta ed effettuazione della sospensione o revoca del certificato su richiesta del titolare; la procedura si articola nelle seguenti fasi:

- inoltro della richiesta da parte del titolare;
- verifica, da parte del certificatore, dell'autenticità e correttezza della richiesta;
- effettuazione della revoca, ossia generazione e pubblicazione della CRL.

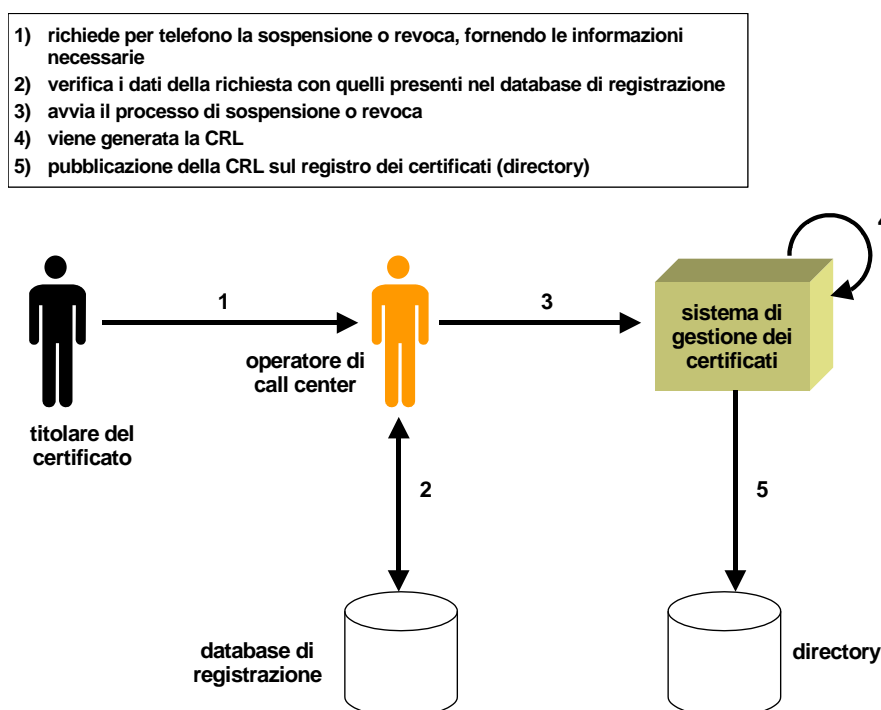


Figura 3: sospensione o revoca del certificato su richiesta del titolare

Nel seguito di questa sezione si descrivono i dettagli delle procedure utilizzabili.

4.5.2.1 Procedura di sospensione o revoca dei certificati

Per il servizio di revoca certificati, il titolare ha a disposizione uno o più numeri verdi opportunamente comunicati all'atto della consegna della carta, ai quali dovrà fornire le seguenti informazioni:

- tipo di intervento richiesto (sospensione o revoca);
- il proprio nome e cognome;
- ulteriori dati identificativi (es. il codice fiscale) nel caso in cui si debbano risolvere omonimie;
- la motivazione per la richiesta di sospensione o revoca;
- la data e ora di decorrenza della sospensione o revoca;
- nel caso di richiesta di sospensione, la durata della sospensione;

Il numero verde sopra indicato è presidiato 24 ore su 24, 7 giorni su 7, da un gruppo di operatori che svolge l'attività di sospensione/revoca certificati su delega del responsabile della registrazione (cfr. la sezione "Note sull'organizzazione del personale").

A fronte della richiesta, l'operatore BMPS svolge le seguenti azioni:

- recupera i dati del titolare nel database di registrazione, per verificare l'autenticità e correttezza della richiesta;
- se necessario, richiede altri dati di identificazione personale (es. codice fiscale);
- nel caso di richiesta non valida (es. il richiedente non risulta titolare di un certificato emesso da BMPS), respinge la richiesta;
- memorizza l'avvenuta richiesta e le informazioni correlate nel database di registrazione;
- avvia la procedura di sospensione o revoca del certificato.

4.5.3 Richiesta di sospensione o revoca da parte del terzo interessato

Avviene nel rispetto degli artt. 20 e 24 del [DPCM].

La richiesta di sospensione o revoca da parte del terzo interessato deve essere inoltrata al certificatore **per iscritto** e corredata della **documentazione giustificativa**.

Non è previsto l'impiego di uno specifico modulo di richiesta. Il terzo interessato deve inviare una **lettera datata e firmata**, nella quale fornisce almeno le seguenti informazioni:

- organizzazione di appartenenza del richiedente (se applicabile);
- nome e cognome del richiedente;
- codice fiscale o partita IVA del richiedente;
- numero di telefono e numero di fax del richiedente;
- dati identificativi del titolare del certificato (es. nome, cognome e codice fiscale) di cui si chiede la sospensione o revoca;
- dati identificativi (es. il numero di serie o altri elementi) del certificato di cui chiede la sospensione o revoca;

- tipo di intervento richiesto (sospensione o revoca);
- nel caso di richiesta di sospensione, intervallo temporale di sospensione;
- la motivazione per la richiesta di sospensione o revoca;
- la data e ora di decorrenza della sospensione o revoca.

La lettera è accompagnata dalla documentazione giustificativa che dimostri la legittimità del ruolo di "terzo interessato" nei confronti dello specifico titolare.

Il certificatore può rigettare la richiesta nel caso la giudichi incompleta o non autentica; l'eventuale rigetto viene notificato al terzo interessato.

A fronte della richiesta, il certificatore:

- notifica la richiesta o la sospensione al titolare del certificato tramite posta elettronica;
- provvede alla sospensione o revoca nei tempi richiesti (cfr. la sezione "Completamento della sospensione o revoca del certificato").

4.5.4 Sospensione o revoca del certificato su iniziativa del certificatore

Avviene nel rispetto degli artt. 18 e 22 del [DPCM].

Salvo i casi di motivata urgenza, qualora il certificatore intenda sospendere o revocare un certificato ne darà preventiva comunicazione al titolare, specificando i motivi della sospensione o revoca, la data di decorrenza della stessa e la durata (nel caso di sospensione).

In ogni caso il certificatore darà successiva comunicazione di quanto sopra elencato.

4.5.5 Completamento della sospensione o revoca del certificato

Al completamento della procedura di revoca o sospensione dei certificati viene prodotta una nuova CRL, la quale viene pubblicata sul registro dei certificati (directory); la data/ora di pubblicazione viene attestata mediante generazione di una corrispondente marca temporale.

Il tempo massimo intercorrente tra l'accettazione della richiesta di sospensione o revoca da parte del titolare e la pubblicazione della CRL aggiornata è di sessanta minuti. In ogni caso, il certificatore si impegna a svolgere l'operazione nel più breve tempo possibile quando la sospensione o revoca è motivata da sospetta o accertata compromissione della segretezza della chiave privata.

Inoltre:

- nel caso di sospensione o revoca su iniziativa del certificatore, il responsabile di registrazione comunica al titolare del certificato l'avvenuta sospensione o revoca;
- l'avvenuta sospensione o revoca viene registrata nel giornale di controllo.

4.6 Modalità di sostituzione delle chiavi (art. 38/3/n)

4.6.1 Sostituzione delle chiavi di sottoscrizione degli utenti

Ai sensi dell'art. 15, comma 4, del [DPCM], il certificatore determina il termine di scadenza del certificato ed il periodo di validità delle chiavi in funzione della lunghezza delle chiavi e dei servizi cui esse sono destinate. Il periodo di validità delle chiavi degli utenti si considera coincidere col periodo di validità del corrispondente certificato, che può essere al massimo di 3 anni.

In prossimità della data di scadenza del periodo di validità del proprio certificato, il titolare o il cliente possono richiedere l'emissione di un nuovo certificato; questa comporta la generazione di una nuova coppia di chiavi (da parte del certificatore stesso) con periodo di validità spostato in avanti di al massimo 3 anni. L'emissione del nuovo certificato richiede la preventiva autorizzazione da parte del responsabile di registrazione.

La procedura seguita per l'emissione di un nuovo certificato è identica a quella seguita per il rilascio del primo certificato e prevede la consegna/invio di un nuovo Codice Riservato Personale e di un nuovo dispositivo sicuro. Essendo tuttavia il titolare già registrato, non è richiesta una nuova registrazione dei dati a meno che non siano intervenute variazioni ai dati del titolare (variazioni che il titolare è comunque tenuto a segnalare tempestivamente al certificatore).

Anche per il rinnovo, l'interazione con l'utente avviene tramite il canale di comunicazione sicura.

4.6.2 Sostituzione delle chiavi di certificazione

Avviene nel rispetto dell'art. 25 del [DPCM].

È svolta a cura del responsabile della certificazione.

4.6.3 Sostituzione delle chiavi di marcatura temporale

Avviene nel rispetto dell'art. 46 del [DPCM].

È svolta mensilmente dal responsabile di certificazione.

4.7 Modalità di gestione del registro dei certificati (art. 38/3/o)

4.7.1 Realizzazione del registro dei certificati

Il registro dei certificati è realizzato con software di tipo "directory server", interrogabile con protocollo LDAP attraverso Internet ed interrogabile via protocollo OCSP così come richiesto dal circuito IdenTrust. Nel resto di questa sezione, i termini "registro dei certificati" e "directory (server)" sono usati in modo equivalente.

4.7.2 Sicurezza del registro dei certificati

La copia di riferimento è resa inaccessibile dall'esterno e risiede su un sistema sicuro installato in locali tecnici protetti. La copia operativa è invece liberamente accessibile attraverso la rete Internet, limitatamente alla sola operazione di lettura.

Lo svolgimento delle operazioni che modificano il contenuto del registro dei certificati è possibile solo per il personale espressamente autorizzato. In ogni caso, tutte le operazioni che modificano il contenuto del registro dei certificati vengono tracciate nel giornale di controllo. Ad ogni evento registrato nel giornale di controllo è apposta un riferimento temporale contenente la data e l'ora - rif. art. 39, comma 2, del [DPCM].

Il registro dei certificati è sottoposto ad un monitoraggio che permette di rilevare e segnalare qualsiasi evento che comprometta i requisiti di sicurezza.

4.7.3 Pubblicazione dei certificati e delle CRL

La pubblicazione dei certificati avviene secondo le modalità previste dalla normativa italiana e le regole che il circuito IdenTrust prevede.

Per quanto riguarda alla normativa italiana nel directory vengono pubblicati i seguenti oggetti:

- certificati per le chiavi degli utenti che ne hanno autorizzato la pubblicazione (rif. art. 29, comma 2, del [DPCM]);
- certificati per le chiavi del certificatore;
- certificati relativi ad accordi di certificazione;
- certificati per le chiavi di firma di CNIPA;
- la lista dei certificati sospesi o revocati.

Con riferimento all'art. 17, comma 1, del [DPCM], il certificatore *non mantiene liste distinte* per i certificati sospesi e per quelli revocati: viene mantenuta e pubblicata un'unica CRL integrale.

Le liste dei certificati revocati e sospesi ed i certificati qualificati resi accessibili alla consultazione del pubblico sono utilizzabili secondo le finalità di cui all'art. 29, comma 3 del [DPCM]. Un riferimento temporale (data/ora) attesta la pubblicazione di una CRL.

La frequenza delle pubblicazioni varia secondo il tipo di oggetto considerato:

- i certificati sono pubblicati nel directory in occasione del loro rilascio al titolare;

- le CRL sono generate e pubblicate nel directory in occasione della sospensione o revoca di uno o più certificati e comunque, anche in assenza di sospensioni o revoche, secondo una frequenza dipendente dalla tipologia di policy.

4.7.4 Repliche su più siti del registro dei certificati

Il certificatore replica il registro dei certificati su più siti, garantendo la consistenza e l'integrità delle copie.

4.8 Modalità di accesso al registro dei certificati (art. 38/3/p)

4.8.1 Protocolli supportati

L'accesso al registro dei certificati è consentito attraverso la rete pubblica Internet; l'indirizzo DNS del directory server è pubblicato sul sito Web del certificatore.

Il certificatore consente l'accesso al registro dei certificati col protocollo LDAP definito nella specifica pubblica RFC 1777. Il registro dei certificati è utilizzabile secondo le finalità di cui all'art. 29 comma 3 del [DPCM].

Per gli utenti operanti nel circuito IdenTrust il certificatore rende disponibile la modalità di verifica tramite protocollo OCSP, gestendo direttamente le richieste di validazione secondo il protocollo di validazione che il circuito IdenTrust prevede.

Il certificatore si riserva la facoltà di rendere disponibili anche ulteriori modalità di accesso.

4.8.2 Controllo degli accessi

Il registro dei certificati è accessibile in lettura a chiunque mentre l'accesso in scrittura o modifica è consentito solo alle persone autorizzate.

4.9 Modalità di protezione della riservatezza (art. 38/3/q)

4.9.1 Archivi contenenti dati personali

Ai fini della tutela della riservatezza, è rilevante solo il "database di registrazione", ossia l'archivio logico contenente:

- le informazioni relative ai titolari dei certificati, prevalentemente raccolte in fase di registrazione;
- le informazioni associate, generate dal certificatore stesso (es. i codici segreti utilizzati per rendere sicure determinate comunicazioni tra certificatore ed utente).

Il database di registrazione, infatti, contiene dati personali raccolti direttamente dalla persona cui si riferiscono o previo suo esplicito consenso. I dati obbligatori sono indispensabili per il rilascio del certificato qualificato. Al richiedente, nell'ambito del contratto di servizio, è fornita l'informativa di cui all'art. 13 del [DLGS 196]. I dati personali presenti nel certificato sono utilizzabili unicamente per l'identificazione del titolare della firma, per legittimare la sottoscrizione di un documento informatico e per indicare eventualmente le funzioni del titolare.

Dati personali - comunque di natura non riservata - contenuti nei certificati, sono resi pubblici su richiesta del titolare e comunicati a terzi nei casi consentiti dal titolare e nel rispetto del [DLGS 196]. Una parte delle informazioni di registrazione viene inizialmente raccolta su supporti cartacei e successivamente trasferita su supporto informatico; i supporti cartacei, in ogni caso, sono archiviati e gestiti come descritto nel paragrafo successivo.

Per quanto riguarda la componente informatica del database di registrazione, basata su un database relazionale, si applica quanto di seguito elencato:

- il database di registrazione e la relativa applicazione di gestione risiedono su un elaboratore dedicato, ubicato in una sala tecnica ad accesso controllato;
- per accedere all'applicazione, gli operatori devono identificarsi mediante una parola chiave personale;
- l'applicazione mantiene accuratamente traccia, in un apposito giornale di controllo, di ogni operazione effettuata;
- viene prodotta periodicamente una copia di sicurezza (backup) della base dati e di altre informazioni essenziali per il ripristino del sistema in caso di guasto all'elaboratore o di perdita accidentale di dati.

Le informazioni memorizzate nel database di registrazione vengono conservate almeno per 20 anni.

4.9.2 Misure di tutela della riservatezza

Ai sensi dell'art. 32 del [DLGS 82] e successive modificazioni, il certificatore tratta tali dati personali nel rispetto del [DLGS 196] e successive modificazioni, predisponendo tutele rispondenti almeno alle misure minime stabilite nello stesso decreto legislativo.

Limitatamente al servizio erogato sulla base del Manuale Operativo, il certificatore non tratta "dati particolari" ovvero dati sensibili ai sensi dell'articolo 4 comma 1 lettera d) o giudiziari ai sensi dello stesso articolo comma 1 lettera e).

4.10 Modalità per l'apposizione e la definizione del riferimento temporale (art. 38/3/r)

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

Le chiavi di certificazione e marcatura temporale sono generate per mezzo di apparati che utilizzano l'algoritmo RSA, in conformità al comma 1 dell'art.53 del [DPCM].

Per la generazione delle chiavi di certificazione e di marcatura temporale sono utilizzati apparati dedicati esclusivamente a tale attività e situati in locali adeguatamente protetti.

4.11 Modalità operative per l'utilizzo del sistema di verifica delle firme (art. 38/3/s)

BMPS possiede applicazioni che consentono di verificare file firmati presenti in "buste" crittografiche conformi al formato PKCS#7.

Tali applicazioni consentono di verificare:

- l'integrità del documento firmato e i dati del firmatario;

- l'autenticità e l'affidabilità del certificato del firmatario;
- la presenza del certificato del firmatario nelle liste dei certificati sospesi o revocati.

Pertanto il processo di validazione di una firma richiede:

- il certificato del firmatario già presenta nella "busta" crittografica;
- il certificato della chiave di certificazione emittente per verificare la credibilità del certificato del firmatario. Tale certificato, se non già disponibile, può essere importata dall'utente tramite un'apposita funzione;
- l'accesso alle liste dei certificati revocati e sospesi (CRL/CSL) per verificare che il certificato del firmatario non sia stato revocato o sospeso.

Ai fini della verifica si tenga inoltre conto dell'eventuale presenza di codici eseguibili o di macroistruzioni cui si fa riferimento nel par. 4.13.

Le CRL/CSL sono accessibili automaticamente via Internet al momento della verifica della firma. Un'apposita funzione consente l'aggiornamento delle CRL/CSL.

I prodotti di verifica delle firme forniti da Actalis sono conformi a quanto indicato all'art. 40, comma 2 del [DPCM].

Le sequenze operative, descritte dettagliatamente nei relativi manuale utente, prevedono dei percorsi guidati con degli appositi menu "a tendina" e/o con delle icone autoesplicative. Nei manuali utente sono inoltre indicati i prerequisiti hw/sw e le modalità di installazione delle applicazioni.

4.12 Modalità operative per la generazione della firma digitale (art. 38/3/t)

Le stesse applicazioni utilizzate per la verifica delle firme consentono di:

- apporre una firma digitale producendo come risultato una busta crittografica in formato standard PKCS#7;
- apporre firme multiple;

La generazione della firma avviene tramite una chiave privata la cui corrispondente chiave pubblica è stata certificata secondo una delle policy indicate al paragrafo 4.4.3. La suddetta chiave privata è custodita all'interno dei dispositivi sicuri forniti o indicati da Actalis. Alla firma digitale è allegato il certificato qualificato del firmatario corrispondente alla chiave pubblica da utilizzare per la verifica.

Operativamente l'utente:

- accede all'applicazione di firma;
- seleziona la funzione di firma dal menu principale;
- seleziona il file da firmare;
- seleziona il dispositivo di firma;
- digita il PIN per l'accesso al dispositivo;
- seleziona la coppia di chiavi che intende utilizzare per firmare con il relativo certificato qualificato. Prima di firmare, può visualizzare il certificato selezionato;

- attiva la funzione di firma;
- il file firmato può essere salvato in una directory a piacere. Il formato DER (binario) è il formato di default con cui è salvata la busta. In alternativa, è possibile salvarla nel formato PEM (Base64) che utilizza solo caratteri stampabili.

In rapporto al sistema operativo ed alle applicazioni disponibili all'utenza, prima di apporre la firma, un'apposita funzione consente di visualizzare il contenuto dell'oggetto da firmare e richiede contestualmente conferma della volontà di apporre la firma.

Le sequenze operative, descritte dettagliatamente nei relativi manuale utente, prevedono dei percorsi guidati con degli appositi menu "a tendina" e/o con delle icone autoesplicative.

Nei manuali utente sono inoltre indicati i prerequisiti hw/sw e le modalità di installazione delle applicazioni.

Le applicazioni di firma fornite da Actalis consentono di firmare file di qualsiasi dimensione e formato. La firma di file in formato "statico" (es. formato txt per il testo e tiff per le immagini) ovvero non contenenti codici eseguibili o macroistruzioni che possano alterare gli atti, i dati o i fatti rappresentati, produce gli effetti di cui all'art. 21, comma 2 del [DLGS 82].

Nel caso in cui il titolare intenda firmare file che possono contenere codici eseguibili o macroistruzioni, ne verifica preventivamente la presenza tramite le funzionalità tipiche di ciascun prodotto.

Codici eseguibili sono, ad esempio, i codici di campo dell'applicazione Microsoft Word™ (es. Date, NumPages, ecc.).

Se si utilizza tale applicazione, procedere come segue: selezionare il menu "Strumenti" e la voce "Opzioni"; nella scheda "Visualizza", selezionare l'opzione "Codici di campo" ed il valore "Sempre" del menu "Ombreggiatura di campo". Scorrendo il documento, i codici di campo sono individuabili in quanto racchiusi tra parentesi graffe __ ed evidenziati in grigio.

Per verificare la presenza di macro, sempre a titolo esemplificativo, con l'applicazione Microsoft Word™, selezionare dal menu "Strumenti" la voce "Macro" e quindi l'opzione "Macro...". Nella finestra che comparirà sono elencate tutte le macro.

L'apposizione ad un documento informatico di una firma digitale basata su un certificato revocato, sospeso o scaduto non è valida – rif. art. 21, comma 3 del [DLGS 82].

5. SERVIZIO DI MARCATURA TEMPORALE

Il certificatore dispone di un servizio di marcatura temporale ai sensi del Titolo IV del [DPCM] avvalendosi dei servizi erogati dal certificatore Actalis. Per la descrizione delle procedure per l'inoltro della richiesta di validazione temporale, previste dall'art. 51 del [DPCM], si rimanda al manuale operativo di detto certificatore.

5.1 Standard di riferimento

Per quanto il formato delle marche temporali ed il protocollo di colloquio tra client e server, il sistema di marcatura temporale di BMPS si basa sulle specifiche "Time Stamp Protocol" sviluppate dal gruppo di lavoro PKIX dell'IETF. Ulteriori dettagli sono precisati nel contratto di servizio.

5.2 Precisione del riferimento temporale

Il server di marcatura temporale ricava il tempo da un ricevitore radio sintonizzato col segnale emesso dall'Istituto Elettrotecnico Nazionale (IEN) "Galileo Ferraris". Il ricevitore usato da Actalis è stato preventivamente tarato e certificato dallo IEN stesso. Il segnale orario così ottenuto ricade ampiamente entro i margini di precisione richiesti dalla normativa vigente.

FINE DEL DOCUMENTO