



Certificati Qualificati

Manuale Operativo

Redatto da:	Adriano Santoni Responsabile Sicurezza	_____	_____
			Data
Verificato da:	Giorgio Girelli Direttore Generale	_____	_____
			Data
Approvato da:	Omero Narducci Amministratore Delegato	_____	_____
			Data

Il documento è :

- **REDATTO** se provvisto della/e firma/e di redazione,
- **VERIFICATO** se provvisto anche della firma di verifica,
- **APPROVATO** se provvisto di tutte le firme

Codice documento: CAACT - 00 - 00 - 10

Codice Progetto Cod Sottoprogram. N. Doc Versione

Distribuzione: PUBBLICA

STORIA DELLE MODIFICHE APPORTATE

Di seguito sono riportate le modifiche apportate al documento con la versione 2.

Capitolo	Descrizione
3.3	Revisione delle le tariffe massime per il rilascio di ogni nuovo certificato
4.1	Modificato l'ultimo paragrafo della sezione in modo da chiarire meglio il caso in cui la registrazione viene fatta da enti (RA) diversi da Actalis
3.2	Revisione all'ultimo punto della sezione 3.2.1 (limitazioni di responsabilità)
4.4	Introdotta la sezione 4.4.2.1 con precisazioni sul supporto di diverse policy di certificato
1.2	Aggiunto riferimento alla Direttiva Europea 1999/93/CE e al D.Lgs. 23/1/2002, n. 10
	Ovunque è stato sostituito <i>"canale telematico sicuro"</i> con <i>"canale di comunicazione sicura"</i>
4.2.1	Specificato che solo alcune delle informazioni fornite dal richiedente vengono memorizzate in un apposito database
4.2.1	Aggiunta la possibilità di inserire un secondo numero di telefono fisso
4.2.1.	Eliminata la possibilità da parte dell'utente di richiedere o meno l'inserimento del proprio indirizzo di posta elettronica nel certificato
4.2.3.1	Eliminata la frase <i>"La fornitura, se prevista, è disciplinata da un contratto separato"</i>
4.2.3.2	Generalizzato il riferimento a interazioni sicure con il sito web del certificatore
4.3.2	Eliminato il riferimento ad un singolo sistema di validazione temporale
4.4.1	Eliminata la frase <i>"oppure memorizzata su un supporto magnetico e consegnata di persona ad un operatore di registrazione"</i>
4.4.1	Inserita la possibilità di eseguire la richiesta del certificato anche presso la struttura di registrazione
4.4.2	Esteso a tre anni il periodo possibile di validità dei certificati
4.4.2.1	Inserita la specificazione che Actalis supporta alternativamente i due tipi di policy
4.4.3	Eliminato il riferimento al codice riservato di revoca
4.5.2.1	Eliminato il numero verde e specificato che è disponibile sul sito web
4.5.2.1	Eliminato il riferimento al paragrafo <i>"Pubblicazione del certificato"</i>
4.5.2.1	Inserite due modalità alternative per inoltrare la richiesta di revoca
4.5.3	Inserita la possibilità di utilizzare uno specifico modulo per la richiesta di sospensione o revoca da parte del terzo interessato
4.6.1	Generalizzato il riferimento a interazioni tramite il sito web del certificatore
4.7.4	Indicato che la frequenza dell'aggiornamento delle CRL dipende dalla tipologia di policy
4.10.2	Generalizzate le modalità di conservazione dei supporti di backup e i riferimenti al responsabile della registrazione.
4.11.3	Eliminato riferimento a <i>"contenitori diversi"</i>
5.2	Inserita la modalità di accesso solo tramite badge

Di seguito sono riportate le modifiche apportate al documento con la versione 3.

Capitolo	Descrizione
1.1	Aggiornati i riferimenti normativi.
1.2	Aggiornati i riferimenti normativi
1.3	Aggiornato riferimento normativo. Eliminato riferimento generico al "DPCM".
1.4	Inseriti riferimenti all'RFC 3161 e RFC 3280
1.5	Inseriti i seguenti acronimi: CNIPA, ETSI, HTTPS, IEN, IETF, TCP, UTC. Eliminati i seguenti acronimi: AIPA, DBMS, CMS.
2.1	Aggiornato riferimento normativo. Modifica dell'indirizzo del sito web del servizio di certificazione. Aggiunto indirizzo LDAP. Eliminati Nomi X.500.
2.2	Aggiornato riferimento normativo. Specificato indirizzo web del servizio di certificazione e la versione ufficiale del manuale operativo.
2.3	Modificato responsabile del manuale operativo.
3.1	Aggiornato riferimento normativo.
3.1.1	Aggiornati i riferimenti normativi. Allineati obblighi del Certificatore alla normativa vigente.
3.1.2	Aggiornati i riferimenti normativi. Inserito riferimento ai Carabinieri per le denunce di furto o smarrimento del dispositivo di firma.
3.1.3	Aggiornati i riferimenti normativi.

3.2	Aggiornato riferimento normativo.
3.2.1	Aggiornato riferimento normativo. Eliminato riferimento esplicito agli scioperi da ritenersi "causa imputabile a terzi" già presente nel testo.
3.2.2	Aggiornati i riferimenti normativi. Aggiornato importo massimo di risarcimento danni per sinistro. Inserito importo massimo di risarcimento danni per annualità.
3.3	Aggiornato riferimento normativo. Eliminate tariffe ed inserito riferimento al sito web del servizio di certificazione per la loro pubblicazione.
4.1	Aggiornato riferimento normativo. Prevista possibilità di raggruppamento di più funzioni compatibili.
4.2	Aggiornato riferimento normativo.
4.2.1	Aggiornati i riferimenti normativi. Prevista data di scadenza del documento presentato dal richiedente. Previsto documento di riconoscimento equipollente. Eliminata l'esibizione del tesserino del codice fiscale.
4.2.1.1	Aggiornati i riferimenti normativi. Prevista l'esibizione del certificato dell'Ordine di appartenenza.
4.2.1.2	Aggiornato riferimento normativo.
4.2.1.3	Revisione del testo relativo alla comunicazione da inviare al Certificatore. Eliminati limitazioni di comunicazione dei dati variati.
4.2.2	Aggiornati i riferimenti normativi. Inserito riferimento ad una password.
4.2.4	Eliminato paragrafo.
4.2.3.1	Aggiornati i riferimenti normativi.
4.2.3.2	Aggiornato riferimento normativo. Inserito riferimento ad una password.
4.2.4	Aggiornati riferimenti normativi. Previsto contratto tra le parti.
4.3	Aggiornati i riferimenti normativi. Inserito riferimento alla generazione delle chiavi al di fuori del dispositivo di firma.
4.3.1	Aggiornati i riferimenti normativi. Previsto utilizzo di chiavi di certificazione per più finalità.
4.3.2	Aggiornato riferimento normativo.
4.3.3	Specificato che il dispositivo di firma è fornito o indicato da Actalis.
4.4	Aggiornato riferimento normativo. Specificato che è inviata una richiesta contenente la chiave pubblica. Specificato che procedure diverse di emissione dei certificati possono essere adottate.
4.4.1	Aggiornati i riferimenti normativi.
4.4.2	Aggiornati i riferimenti normativi. Specificata l'indicazione che il certificato emesso è qualificato. Eliminata verifica che la chiave pubblica non sia stata certificata da altro Certificatore.
4.4.3	Specificato l'indirizzo del sito web del servizio di certificazione.
4.4.4	Eliminato paragrafo sugli accordi di certificazione e rassegnato il n.ro paragrafo alla "Pubblicazione del certificato".
4.5	Aggiornati i riferimenti normativi. Specificati gli effetti della revoca e della sospensione e la loro efficacia.
4.5.1	Specificate le circostanze della revoca e della sospensione ed i richiedenti.
4.5.2	Generalizzata la descrizione in Figura 3.
4.5.2.1	Dettagliata la richiesta cartacea. Specificati orari del servizio di assistenza telefonica. Specificata la disponibilità h24 dell'applicazione web.
4.5.3	Aggiornati riferimenti normativi. Specificato che occorre fotocopia della denuncia di smarrimento o furto del dispositivo di firma. Inserito codice fiscale o partita IVA nella richiesta tramite lettera. Eliminato riferimento al sito web. Eliminato riferimento alla posta elettronica per la notifica al titolare. Inserita definizione del Terzo Interessato.
4.5.4	Aggiornati riferimenti normativi.
4.5.5	Specificata tempestività dell'aggiornamento della CRL in caso di sospensione o revoca per sospetta o accertata compromissione della chiave privata.
4.6.1	Aggiornato riferimento normativo. Eliminati riferimenti a modalità operative specifiche.
4.6.2	Aggiornato riferimento normativo.
4.6.3	Aggiornato riferimento normativo.
4.7.1	Eliminato riferimento articolo DPCM 8/2/1999.
4.7.2	Eliminati riferimenti alle diverse copie del registro dei certificati e rinumerato il paragrafo "Sicurezza del registro dei certificati". Inserita modalità di riferimento temporale per il giornale di controllo.
4.7.3	Aggiornati i riferimenti normativi.
4.7.4	Eliminato riferimento articolo DPCM 8/2/1999 ed al paragrafo "Compromissione del sito principale".
4.8	Aggiornato riferimento normativo.
4.8.1	Eliminato riferimento al sito web.
4.8.2	Eliminati riferimenti a copie distinte del registro dei certificati.
4.9	Aggiornato riferimento normativo.

4.9.1	Aggiornati i riferimenti normativi. Inserito riferimento all'informativa ai sensi del "Codice in materia di protezione dei dati personali".
4.9.2	Aggiornati i riferimenti normativi. Inserito riferimento alle misure minime previste dal "Codice in materia di protezione dei dati personali".
4.10	Sostituito paragrafo relativo alle procedure di gestione delle copie di sicurezza con le "Modalità per l'apposizione e la definizione del riferimento temporale".
4.11	Sostituito paragrafo relativo alle procedure di gestione degli eventi catastrofici con "Modalità operative per l'utilizzo del sistema di verifica delle firme".
4.12	Nuovo paragrafo "Modalità operative per la generazione della firma digitale".
5	Eliminato capitolo "Servizio di marcatura temporale".

Di seguito sono riportate le modifiche apportate al documento con la versione 4.

Capitolo	Descrizione
1.1	Aggiornati i riferimenti normativi.
1.1.1	Nuovo paragrafo sui certificati qualificati di firma a bordo della CNS.
1.2	Inseriti riferimento al [DLGS82], alla [DELIB. 4/05], alla [L.273], al [DM 591], al [DLGS 21/01/04].
1.3	Inserita delucidazione sui riferimenti.
1.4	Inseriti nuovi riferimenti a standard (ETSI TS 102 280 v 1.1.1 e ETSI TS 101 862 v.1.3.2).
1.5	Inseriti nuovi acronimi (ATS, CNS, INRIM, OID, TSS, TST).
2.1	Aggiornato indirizzo LDAP del directory server
2.2	Inserito riferimento al [DLGS82].
3.1.1	Allineati obblighi e responsabilità al [DLGS82] e successive correzioni ed integrazioni ed inseriti riferimenti ai Titoli II, III, IV del [DPCM].
3.1.2	Allineati obblighi e responsabilità al [DLGS82] e successive correzioni ed integrazioni ed inserito riferimento a modalità e finalità di utilizzo del certificato.
3.1.3	Allineati obblighi e responsabilità al [DLGS82] ed inserito riferimento specifico ad alcune eventuali informazioni presenti nel certificato.
3.1.4	Nuovo paragrafo "Obblighi del Terzo Interessato".
3.2.1	Aggiornamento riferimento normativo.
4.2.1	Aggiornati riferimenti normativi. Precisazioni sull'obbligatorietà delle informazioni.
4.2.1.1	Aggiornamento riferimento normativo al [DLGS82] e successive correzioni ed integrazioni.
4.2.1.2	Aggiornamento riferimento normativo.
4.2.1.3	Inseriti riferimenti agli enti di diritto pubblico.
4.2.1.4	Nuovo paragrafo "Limiti d'uso e di valore".
4.2.3.1	Aggiornamento riferimento normativo.
4.4.2	Aggiornamento riferimento normativo al [DLGS82] e successive correzioni ed integrazioni. Inserito riferimento all'estensione qcStatement.
4.5.5	Sostituita marca temporale con riferimento temporale.
4.6.1	Inserita precisazione sui termini temporali di avvio della procedura di rinnovo.
4.7.2	Sostituita marca temporale con riferimento temporale.
4.7.3	Specificato riferimento temporale per pubblicazione CRL.
4.10	Riorganizzato tutto il paragrafo con nuovo sottoparagrafo 4.10.1.
4.9.2	Aggiornamento riferimento normativo.
4.10.2.1, 4.10.2.2, 4.10.2.3	Aggiornate le descrizioni delle modalità operative del servizio di marcatura temporale. Inserito riferimento all'INRIM ed al relativo decreto di istituzione.
4.12	Aggiornamento riferimento normativo.

Di seguito sono riportate le modifiche apportate al documento con la versione 5.

Capitolo	Descrizione
frontesp.	Allineato nominativi ciclo di approvazione alla nuova struttura organizzativa.
2.1	Sostituito nominativo del Rappresentante legale.
4.4.4	Sostituita marca temporale con riferimento temporale.

Di seguito sono riportate le modifiche apportate al documento con la versione 6.

Capitolo	Descrizione
(tutti)	Inserimento di precisazioni, disposizioni e chiarimenti relativi al caso della CNS.
1.2	Inseriti i riferimenti alla normativa della CNS.
1.5	Inseriti nuovi acronimi (CCIAA, PA, RI, TSG)
2.2	Precisazione sul formato del manuale e inserimento dell'indirizzo del sito web del CNIPA.
3	Inserimento di precisazioni relative al caso della CNS.
4.1.1	Nuovo paragrafo che precisa il concetto di Registration Authority (RA), le relazioni tra il certificatore e le RA, l'applicazione del concetto anche al caso della CNS.
4.2.1.2	Nuovo paragrafo comprensivo sia della gestione dei ruoli che dei limiti di valore e di utilizzo (integrazione dei § 4.2.1.2, 4.2.1.3, 4.2.1.4 della release 05).
4.3.1	Inserita precisazione sul profilo dei certificati di certificazione.
4.3.2	Inserita precisazione sul profilo dei certificati di marcatura temporale.
4.4.2	Inserita precisazione sul riferimento temporale all'atto dell'emissione del certificato e precisazione sulle estensioni OcStatements.
4.4.3	Inserita precisazione sul profilo dei certificati qualificati e sugli OID che li identificano.
4.5.2.1	Inserita precisazioni sull'assistenza telefonica.
4.9.1	Nuovo paragrafo contenente l'informativa sulla privacy ai sensi del D.Lgs. 196/03.
4.10.2.1	Inserito dettaglio sulla sequenza operativa del servizio di time-stamping.
4.11	Inserito riferimento all'obbligo di fornire o indicare un prodotto o sistema di verifica delle firme digitali da parte del Certificatore.

Di seguito sono riportate le modifiche apportate al documento con la versione 7.

Capitolo	Descrizione
1.2	Inserito riferimento alla L.48/2008.
1.5	Inserito acronimi CP, DER, PEM.
3.1.2	Inserito obbligo di dichiarazioni ed attestazioni veritieri.
3.1.1	Inserito riferimento al reato di frode informatica di cui all'art. 640-quinquies del CP.
4.2.1	Inserita precisazione sulla validità del documento di riconoscimento esibito.
4.2.1.2	Inserito riferimento al reato di falsa dichiarazione o attestazione di cui all'art. 495-bis del CP.
4.2.3.1	Rinominato paragrafo da "Fornitura e caratteristiche del dispositivo di firma" in "Requisiti di sicurezza e caratteristiche del dispositivo di firma".
4.2.3.3	Nuovo paragrafo "Conservazione e distribuzione del dispositivo di firma".
4.11	Revisionato intero paragrafo con precisazioni sulla sequenza operativa.
4.12	Revisionato intero paragrafo con precisazioni sulla sequenza operativa e sul formato dei file.

Di seguito sono riportate le modifiche apportate al documento con la versione 8.

Capitolo	Descrizione
4.5.2.1	Corretto l'orario di inizio del servizio assistenza
4.2.1, 4.4.4, 4.8.1, 4.9.1	Correzioni alla descrizione dei criteri per la pubblicazione dei certificati
4.10.1	Correzioni alla descrizione del riferimento temporale

Di seguito sono riportate le modifiche apportate al documento con la versione 9.

Capitolo	Descrizione
-	Modificato il frontespizio del documento
1.2	Aggiornati i riferimenti normativi
1.4	Aggiornati i riferimenti agli standard tecnici
1.5	Eliminati alcuni acronimi non più utilizzati
2.2	Modificato il nome del presidente e l'indirizzo della società
2.3	Modificato il nome di riferimento per il Manuale Operativo
4.2.1.2	Precisazioni sulla lunghezza massima delle eventuali limitazioni d'uso
4.3.2	Modificata la durata delle chiavi di marcatura temporale come da norme
4.5.2.1	Precisazioni sulla sospensione (durata massima e azioni intraprese al termine)
4.10	Precisazioni sul servizio di marcatura temporale
4.12	Precisazioni sugli standard di firma (busta crittografica)
4.12.1	Nuovo paragrafo per dare maggiore evidenza al tema dell'Art. 3 comma 3 del DPCM

Di seguito sono riportate le modifiche apportate al documento con la versione 10.

Capitolo	Descrizione
-	Modificato il frontespizio del documento
2.2	Modificato il nome del responsabile legale
(tutti)	Modificato CNIPA in DigitPA; aggiornati o corretti i riferimenti normativi
Diversi	Aggiunte precisazioni relative al caso della firma automatica e/o remota
4.2.1.4	Introdotta la possibilità d'identificazione del richiedente mediante autentica firma da parte di un pubblico ufficiale (nuovo par. 4.2.1.3)

INDICE DELLE FIGURE

<i>Figura 1: identificazione e registrazione degli utenti</i>	19
<i>Figura 2: richiesta, generazione e rilascio del certificato</i>	27
<i>Figura 3: sospensione o revoca del certificato su richiesta del titolare</i>	31

SOMMARIO

1. GENERALITÀ	10
1.1 Scopo del documento	10
1.1.1 Carta Nazionale dei Servizi	10
1.2 Riferimenti alle norme di legge	10
1.3 Convenzioni di lettura	11
1.4 Riferimenti agli standard	11
1.5 Definizioni ed acronimi	12
2. INTRODUZIONE	13
2.1 Dati identificativi del certificatore (art. 36/3/a)	13
2.2 Versione del manuale operativo (art. 36/3/b)	13
2.3 Responsabile del manuale operativo (art. 36/3/c)	13
3. DISPOSIZIONI GENERALI	14
3.1 Obblighi del certificatore, del titolare e dei richiedenti la verifica delle firme (art. 36/3/d)	14
3.1.1 Obblighi e responsabilità del certificatore.....	14
3.1.2 Obblighi e responsabilità del titolare.....	15
3.1.3 Obblighi dei richiedenti la verifica delle firme.....	16
3.1.4 Obblighi del Terzo Interessato	16
3.2 Responsabilità e limitazioni agli indennizzi (art. 36/3/e)	17
3.2.1 Limitazioni di responsabilità	17
3.2.2 Limitazioni agli indennizzi	17
3.3 Tariffe del servizio (art. 36/3/f)	17
4. ASPETTI OPERATIVI	18
4.1 Note sull'organizzazione del personale (art. 34)	18
4.1.1 Registration Authority	18
4.2 Identificazione e registrazione degli utenti (art. 36/3/g)	19
4.2.1 Identificazione dei richiedenti	20
4.2.1.1 Abilitazioni professionali	21
4.2.1.2 Inserimento di ruoli, limiti di valore e di uso	22
4.2.1.3 Identificazione da parte di un pubblico ufficiale	23
4.2.2 Verifiche svolte dal certificatore in fase di registrazione.....	23
4.2.3 Dispositivo di firma	24
4.2.3.1 Requisiti di sicurezza e caratteristiche del dispositivo di firma	24
4.2.3.2 Personalizzazione del dispositivo di firma	24
4.2.3.3 Conservazione e distribuzione del dispositivo di firma.....	25
4.3 Generazione delle chiavi (art. 36/3/h)	25
4.3.1 Modalità di generazione delle chiavi di certificazione	25
4.3.2 Modalità di generazione delle chiavi di marcatura temporale.....	26
4.3.3 Modalità di generazione delle chiavi di sottoscrizione degli utenti	26
4.4 Emissione dei certificati qualificati (art. 36/3/i)	26
4.4.1 Richiesta del certificato	27
4.4.2 Generazione del certificato	28

4.4.3	Policy supportate.....	29
4.4.4	Pubblicazione del certificato.....	29
4.5	Sospensione e revoca dei certificati (art. 36/3/l).....	29
4.5.1	Circostanze per la sospensione o revoca del certificato.....	30
4.5.2	Richiesta di sospensione o revoca da parte del titolare.....	30
4.5.2.1	Procedura di sospensione o revoca dei certificati	31
4.5.3	Richiesta di sospensione o revoca da parte del terzo interessato.....	32
4.5.4	Sospensione o revoca del certificato su iniziativa del certificatore.....	33
4.5.5	Completamento della sospensione o revoca del certificato.....	33
4.6	Sostituzione delle chiavi (art. 36/3/m)	33
4.6.1	Sostituzione delle chiavi di sottoscrizione degli utenti.....	33
4.6.2	Sostituzione delle chiavi di certificazione.....	34
4.6.3	Sostituzione delle chiavi di marcatura temporale	34
4.7	Gestione del registro dei certificati (art. 36/3/n).....	34
4.7.1	Realizzazione del registro dei certificati.....	34
4.7.2	Sicurezza del registro dei certificati	34
4.7.3	Pubblicazione dei certificati e delle CRL.....	34
4.7.4	Repliche su più siti del registro dei certificati.....	35
4.8	Accesso al registro dei certificati (art. 36/3/o)	35
4.8.1	Protocolli supportati.....	35
4.8.2	Controllo degli accessi.....	35
4.9	Protezione dei dati personali (art. 36/3/q)	35
4.9.1	Informativa ai sensi del D.Lgs. 196/03.....	36
4.9.2	Archivi contenenti dati personali	36
4.9.3	Misure di tutela della riservatezza	37
4.10	Apposizione e definizione del riferimento temporale (art. 36/3/p)	37
4.10.1	Riferimento temporale	37
4.10.2	La marca temporale.....	38
4.10.2.1	Modalità di erogazione del servizio	38
4.10.2.2	Accesso al servizio	38
4.10.2.3	Modalità di utilizzo del servizio	38
4.10.2.4	Sicurezza fisica	39
4.10.2.5	Sicurezza logica	39
4.11	Utilizzo del sistema di verifica delle firme (art. 36/3/r).....	39
4.12	Generazione della firma digitale (art.38/3/s)	40
4.12.1	Firma con dispositivo di firma personale	40
4.12.2	Firma con procedura automatica e/o remota.....	41
4.12.3	Raccomandazioni per evitare la perdita di efficacia della firma digitale.....	42

1. GENERALITÀ

1.1 Scopo del documento

Questo documento è il **Manuale Operativo** del servizio di certificazione di chiavi pubbliche erogato da Actalis S.p.A. ai sensi del [DPR 445], del [DLGS82] (e s.m.i.) e del [DPCM].

1.1.1 Carta Nazionale dei Servizi

La disciplina e le indicazioni contenute nel presente documento si applicano anche ai certificati qualificati di firma digitale emessi da Actalis per essere installati sulle CNS (Carta Nazionale dei Servizi) su richiesta delle Pubbliche Amministrazioni emittenti (Enti Emittenti). Nel caso della CNS, l'Amministrazione emittente è la sola responsabile dell'identificazione e registrazione del titolare, come discende dalla normativa di riferimento [RTCNS].

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 Supplemento Ordinario alla Gazzetta Ufficiale n. 42 del 20 febbraio 2001.
- [DPCM] Decreto del Presidente del Consiglio dei Ministri (DPCM) 30 marzo 2009, "Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici", pubblicato sulla Gazzetta Ufficiale n.129 del 6 giugno 2009.
- [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 G.U. n. 174, 29 luglio 2003.
- [DM] Decreto 2 luglio 2004, "Competenza in materia di certificatori di firma elettronica" pubblicato nella Gazzetta Ufficiale n.199, 25 agosto 2004.
- [DLGS82] Decreto Legislativo 7 marzo 2005, n. 82: "Codice dell'amministrazione digitale", pubblicato nella Gazzetta Ufficiale. n. 112 del 16 maggio 2005.
- [DLB45/09] Deliberazione CNIPA n.45 del 21 maggio 2009, "Regole per il riconoscimento e la verifica del documento informatico", Pubblicato nella G.U. n. 282 (serie generale) del 3 dicembre 2009, e successive modifiche e integrazioni.
- [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.
- [DLGS159] 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 G.U. 29 aprile 2006, n.99.
- [DPR117] Decreto del Presidente della Repubblica 2 marzo 2004, n. 117, "Regolamento concernente la diffusione della Carta Nazionale dei Servizi, a norma dell'articolo 27, comma 8, lettera b), della legge 16 gennaio 2003, n. 3." (G.U. n. 105 del 6 maggio 2004).
- [RTCNS] Decreto del Ministero dell'Interno, del Ministro per l'innovazione e le tecnologie e del Ministro dell'economia e delle finanze 9 dicembre 2004, recante "Regole tecniche e di sicurezza

relative alle tecnologie e ai materiali utilizzati per la produzione della Carta Nazionale dei Servizi” pubblicato nella Gazzetta Ufficiale n.296, 18 dicembre 2004.

[LGCNS] “Linee guida per l’emissione e l’utilizzo della Carta Nazionale dei Servizi”, Ufficio standard e metodologie d’identificazione, CNIPA, Versione 3.0, 15 maggio 2006.

[L. 48] Legge 18 marzo 2008, n.48, “Ratifica ed esecuzione della Convenzione del Consiglio d’Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell’ordinamento interno” pubblicato nella Gazzetta Ufficiale n.80 del 4 aprile 2008

1.3 Convenzioni di lettura

Nel resto del documento, l’azienda Actalis S.p.A., erogatrice del servizio di certificazione qui descritto e disciplinato, è indicata semplicemente con “Actalis”.

Col termine “Manuale Operativo” si intende sempre fare riferimento alla *versione corrente* del Manuale Operativo (vedere la sezione 2.2).

I riferimenti alla normativa e agli standard sono riportati tra parentesi quadre. In particolare, in alcuni dei titoli e sottotitoli di questo documento è riportato tra parentesi l’articolo, il comma e la lettera di riferimento del [DPCM].

1.4 Riferimenti agli standard

[LDAP3] Wahl, M., Kille, S. and T. Howes, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

[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 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

[RFC 3161] Adams, C., Cain, P., Pinkas, D. and Zuccherato, R., "Time-Stamp Protocol (TSP)", RFC 3161, August 2001.

[RFC 5816] Santesson, S., Pope, N., “ESSCertIDv2 Update for RFC 3161”, RFC 5186, March 2010.

[RFC 5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, RFC 5280, May 2008.

[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 usati in questo documento:

CCIAA	Camera di Commercio, Industria, Artigianato ed Agricoltura
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
CNS	Carta Nazionale dei Servizi
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DigitPA	Ex CNIPA
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
HTTPS	HyperText Transfer Protocol Secure
IEN	Istituto Elettrotecnico Nazionale
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
OID	Object Identifier
PA	Pubblica Amministrazione
PDF	Portable Document Format
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Function 1
SSL	Secure Sockets Layer
TST	Time Stamping Token
URL	Uniform Resource Locator

2. INTRODUZIONE

2.1 Dati identificativi del certificatore (art. 36/3/a)

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

Denominazione sociale:	Actalis S.p.A.
Indirizzo della sede legale:	Via dell'Aprica, 18 – 20158 Milano
Legale rappresentante:	Omero Narducci (Amministratore Delegato)
N° di iscrizione al Registro delle Imprese di Milano:	R.E.A. n. 1669411
N° di Partita IVA:	03358520967
N° di telefono (centralino):	+39 02 68825.1
DUNS number:	440-489-735
ISO Object Identifier (OID):	1.3.159
Sito web generale (informativo):	http://www.actalis.it/
Sito web del servizio di certificazione:	https://portal.actalis.it
E-mail (informativo):	info@actalis.it
Directory server (registro dei certificati):	ldap://ldap.actalis.it ldap://fe.csp.multicertify.com

2.2 Versione del manuale operativo (art. 36/3/b)

Il presente documento è il Manuale Operativo relativo al servizio di certificazione di chiavi pubbliche erogato dalla Actalis ai sensi del [DLGS82] e successive correzioni ed integrazioni e del [DPCM]. Il codice interno di questo documento è riportato sul frontespizio.

Questo documento è pubblicato sul sito web del servizio di certificazione <https://portal.actalis.it> 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 servizio di certificazione <https://portal.actalis.it> oppure quella pubblicata sul sito web del DigitPA (www.digitpa.gov.it). In ogni caso, farà fede la versione pubblicata sul sito web del DigitPA.

Il documento è pubblicato in formato PDF firmato, in modo tale da assicurarne l'origine e l'integrità.

2.3 Responsabile del manuale operativo (art. 36/3/c)

Le comunicazioni riguardanti il presente documento possono essere inviate all'attenzione di:

Adriano Santoni <adriano.santoni@actalis.it>
Via dell'Aprica 18
20158 Milano
Actalis S.p.A.

3. DISPOSIZIONI GENERALI

3.1 Obblighi del certificatore, del titolare e dei richiedenti la verifica delle firme (art. 36/3/d)

3.1.1 *Obblighi e responsabilità del certificatore*

Il certificatore ha l'obbligo di attenersi a quanto disposto nell'art. 32 del [DLGS82], quindi 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 (nel caso di emissione di certificato per la Carta Nazionale dei Servizi: la responsabilità dell'identificazione del titolare è in capo alla PA emittente secondo quanto specificato espressamente dal [DPR117] e dal [RTCNS]);
- rilasciare e rendere pubblico il certificato nei modi e nei casi stabiliti dal [DPCM] e nel rispetto del [DLGS196];
- specificare nel certificato, 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 nel [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;
- non rendersi depositario di dati per la creazione della firma del titolare;
- procedere alla tempestiva pubblicazione della revoca e della sospensione del certificato elettronico nei casi di cui all'art. 32, comma 3, lettera g), del [DLGS82];
- 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 titolare del certificato;
- fornire, prima dell'accordo, ai richiedenti il servizio, le informazioni relative ai termini ed alle condizioni relative all'utilizzo del certificato;
- garantire che solo 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 [DLGS196].

Il certificatore che rilascia certificati qualificati ha l'obbligo di operare secondo quanto previsto dal Titolo II ("Regole tecniche di base") del [DPCM] nonché dal Titolo III ("Certificatori accreditati") e dal Titolo IV ("Regole per la validazione temporale mediante marca temporale") del [DPCM].

Infine il Certificatore accreditato, nel caso in cui intenda cessare l'attività, ha l'obbligo di attenersi a quanto previsto nell'art. 37 del [DLGS82].

Le responsabilità del Certificatore nei confronti dei titolari di certificato e dei terzi che vi fanno affidamento sono descritte nell'art. 30 del [DLGS82]. 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" (ossia: della chiave privata corrispondente alla chiave pubblica contenuta nel certificato).

Il certificatore non è responsabile dei danni derivanti dall'uso di un certificato per negozi di valore superiore al valore limite specificato nel certificato stesso ovvero eccedenti il limite d'uso specificato.

Il Certificatore che, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri un danno viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato è punito con reclusione fino a 3 (tre) anni o con la multa fino a € 1.032,00 (milletrentadue/00 euro), secondo quanto stabilito dall'art. 640-quinquies del Codice Penale, così come modificato dalla [L. 48].

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 si presume riconducibile al titolare a meno che quest'ultimo non fornisca prova contraria.

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

- richiedere il certificato con le modalità previste dal Manuale Operativo tranne il caso in cui il certificato sia abbinato ad una CNS (considerato che la richiesta proviene dalla PA emittente);
- 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 dei certificati relativi alle chiavi contenute in dispositivi di firma di cui abbia perduto il possesso o difettosi,
 - mantenere in modo esclusivo la conoscenza o la disponibilità di almeno uno dei dati per la creazione della firma (nel caso della firma con procedura automatica o remota, si tratta dei dati di autenticazione necessari per l'uso della chiave di firma);
- 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 del Manuale Operativo prima di richiedere al certificatore di essere registrato tranne in caso in cui il certificato sia abbinato ad una CNS ove tale obbligo deve essere assolto a cura del Titolare prima dell'attivazione del certificato;

- fornire al certificatore (o alla PA emittente, ove richieste da quest'ultima, nel caso di certificato abbinato alla CNS) 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, qualità personali, ruoli ricoperti, etc.);
- in caso di furto o smarrimento del proprio dispositivo di firma, farne denuncia alla Polizia o ai Carabinieri ed informarne tempestivamente il certificatore;
- utilizzare il certificato con le sole modalità e finalità descritte nel Manuale operativo;
- dichiarare o attestare al Certificatore, all'atto della richiesta del servizio, identità o qualità personali proprie o di altri veritiere (rif. art. 495-bis del Codice Penale).

3.1.3 Obblighi dei richiedenti la verifica delle firme

Coloro che verificano firme digitali generate con chiavi certificate da Actalis 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, verificare la 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 eventuali "accordi di certificazione";
 - verificare il periodo di validità del certificato - rif. art. 28, comma 1, lettera f, del [DLGS82];
 - verificare che il certificato non sia sospeso o revocato;
 - verificare la tipologia delle chiavi - rif. art. 15, comma 1, lettera b, del [DPCM];
- tenere nella debita considerazione le seguenti informazioni, se presenti nel certificato: 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; 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 gli obblighi sopra esposti.

3.1.4 Obblighi del Terzo Interessato

Il terzo interessato è la persona fisica o giuridica che acconsente all'inserimento di un ruolo nel certificato (come previsto dall'art. 32, comma 2 lettera c) del [DLGS82]) oppure l'organizzazione che richiede o autorizza il rilascio del certificato del titolare (cfr. art. 12 comma 3 lettera c) della [DLB45/09]).

Il Terzo Interessato è tenuto a:

- conoscere il Manuale Operativo ed attenersi ad esso;
- 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 Responsabilità e limitazioni agli indennizzi (art. 36/3/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 Actalis:

- fatti salvi i limiti inderogabili di legge, la responsabilità di Actalis, a qualsiasi titolo derivante dal contratto di servizio, sussisterà solo nei casi di dolo o colpa grave;
- Actalis non sarà responsabile della mancata esecuzione delle obbligazioni assunte con il contratto di servizio, qualora tale mancata esecuzione sia dovuta a cause non imputabili ad Actalis, 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 ed altre cause imputabili a terzi;
- Actalis, 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;
- Actalis rilascia anche certificati qualificati contenenti limiti d'uso ai sensi dell'art. 30 comma 3 del [DLGS82] e dell'art. 43 del [DPCM], quali limitazioni per il valore dei negozi per i quali il certificato può essere usato, ovvero limitazioni negli scopi per i quali il certificato può essere usato. Actalis non sarà responsabile per gli eventuali danni derivanti dall'uso di un certificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite.

Il presente Manuale operativo, che può essere integrato o meno da condizioni generali o particolari di contratto sottoscritte specificamente dal Titolare, costituisce la disciplina che regola l'utilizzo del certificato da parte del Titolare e regola inoltre i rapporti tra Titolare e Certificatore. La richiesta – ovvero l'attivazione, nel caso di CNS – del certificato implica l'accettazione integrale e incondizionata del Manuale Operativo e della disciplina in esso contenuta da parte del Titolare.

3.2.2 Limitazioni agli indennizzi

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

Nel caso in cui i certificati rilasciati da Actalis 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 - Actalis non sarà responsabile per i danni conseguenti ad un utilizzo non conforme.

In ogni caso, il risarcimento di danni a terzi non potrà superare l'importo massimo annuo di € 1.250.000 (un milione e duecentocinquantamila Euro) incluse le spese di reclamo.

3.3 Tariffe del servizio (art. 36/3/f)

Le tariffe massime del servizio sono pubblicate sul sito web <https://portal.actalis.it>.

4. ASPETTI OPERATIVI

4.1 Note sull'organizzazione del personale (art. 34)

Il personale preposto all'erogazione e controllo del servizio di certificazione è organizzato nel rispetto dell'art. 34 del [DPCM]. In particolare, sono definite le seguenti figure organizzative:

- responsabile della sicurezza;
- responsabile del servizio di certificazione e validazione temporale;
- responsabile della conduzione tecnica dei sistemi;
- responsabile dei servizi tecnici e logistici;
- responsabile delle verifiche e delle ispezioni (auditing).

Inoltre, in Actalis è definita la figura del “responsabile della registrazione” il quale è responsabile specificamente del corretto, sicuro ed efficiente svolgimento delle attività di identificazione e registrazione dei titolari, svolte da operatori interni od esterni secondo i casi (cfr. la sezione successiva).

Le figure sopra elencate possono avvalersi, per lo svolgimento delle attività di loro competenza, di addetti e collaboratori.

Gli operatori di registrazione possono eventualmente operare anche presso sedi remote, rispetto alla sede principale di Actalis, e scambiare informazioni col sito principale mediante canali di comunicazione sicuri.

4.1.1 *Registration Authority*

Al fine di ampliare le possibilità operative, le funzioni di registrazione possono essere svolte anche da terze parti, con sedi distribuite sul territorio, sulla base di appositi accordi stipulati con Actalis. In tal caso, tali terze parti (“Registration Authority”, abbreviato RA) operano secondo procedure concordate con Actalis. Le procedure adottate dalle RA possono in parte differire da quelle descritte nei successivi paragrafi del presente documento, ma devono assicurare il medesimo livello di accuratezza ed affidabilità e soddisfare i requisiti tecnici di Actalis per quanto concerne le modalità di codifica e trasmissione al certificatore dei dati di registrazione dei richiedenti.

Le RA sono responsabili nei confronti di Actalis della corretta e sicura identificazione dei richiedenti, nonché del trattamento dei loro dati nel pieno rispetto della normativa sulla privacy e della normativa sulla firma digitale. Actalis rimane a sua volta pienamente responsabile, nei confronti di chiunque si affidi ai certificati, delle operazioni di identificazione e registrazione dei richiedenti, siano esse svolte in proprio da Actalis oppure dalle RA.

Prima di essere attivati, gli accordi di delega che Actalis stipula con le RA devono essere firmati dal legale rappresentante - o altra persona dotata dei poteri di firma - della controparte. Il responsabile della registrazione di Actalis accerta che tale requisito sia soddisfatto e verifica inoltre, coi mezzi consentiti dalla legge (per es. mediante visura camerale), che l'azienda od ente che svolge il ruolo di RA esista effettivamente.

Il certificatore rende disponibili alle RA strumenti e procedure per effettuare telematicamente le operazioni di registrazione degli utenti, nonché di sospensione o revoca dei certificati. A tali strumenti

possono accedere solo gli operatori espressamente autorizzati dalle RA, previa verifica da parte del responsabile Actalis della registrazione.

Si noti che le RA possono in molti casi rivestire anche il ruolo di “terzo interessato” e dunque avere i relativi obblighi (cfr. il paragrafo 3.1.4).

Nell’ambito dell’emissione di un certificato abbinato ad una CNS, il ruolo di RA è sempre svolto da una Pubblica Amministrazione in qualità di Ente Emittitore a cui compete l’identificazione del titolare, direttamente o tramite struttura delegata, come previsto dalle [RTCNS].

4.2 Identificazione e registrazione degli utenti (art. 36/3/g)

La seguente Figura 1 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;
- verifica delle informazioni fornite ed accettazione o rifiuto della richiesta.

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

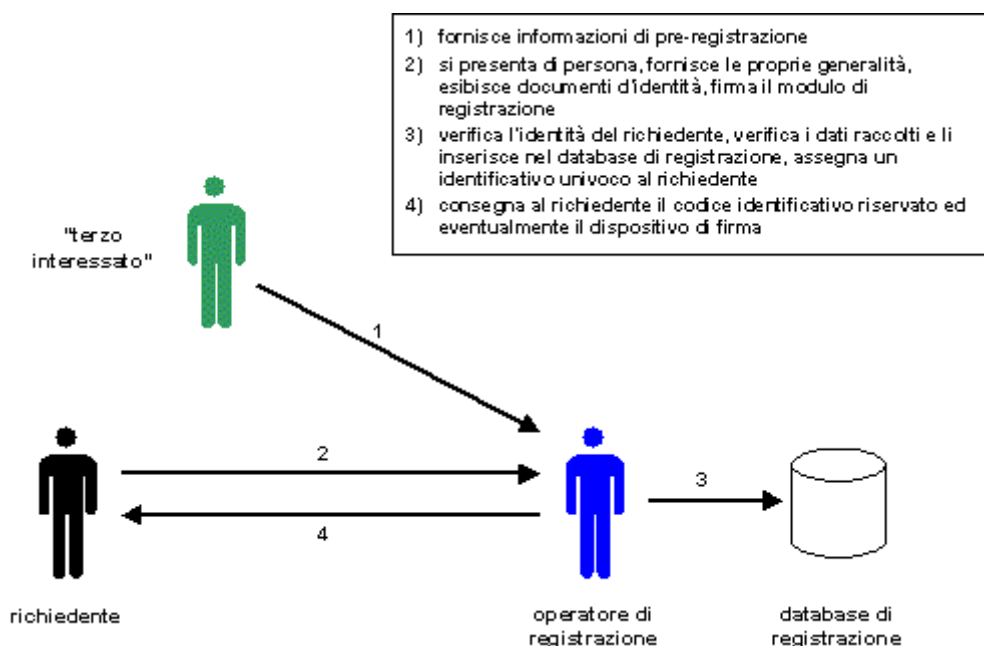


Figura 1: identificazione e registrazione degli utenti

Lo schema generale della Figura 1 vale anche nel caso di emissione di certificato abbinato ad una CNS, laddove con “operatore di registrazione” si intenda un operatore dell’Amministrazione emittente. Tuttavia, nel caso della CNS, alcune operazioni possono essere svolte in modo diverso e/o in tempi diversi – in ogni caso nel rispetto delle [RTCNS] - rispetto alla descrizione di dettaglio che si riporta più avanti. Dove necessario, nel resto del documento vengono indicate le differenze.

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

4.2.1 Identificazione dei richiedenti

Ove la richiesta di emissione di un certificato non provenga da una PA che attesta autonomamente l'identità del titolare in forza della propria autorità, 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] in corso di validità;

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, alcune delle 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, eventualmente all'estero,
- indirizzo di posta elettronica, (*)
- tipo e numero del documento d'identità o del documento di riconoscimento equipollente esibito,
- eventuali abilitazioni professionali (vedere "Abilitazioni professionali"), (*)
- eventuali poteri di rappresentanza (vedere "Inserimento di ruoli, limiti di valore e di uso"), (*)
- eventuali limiti di valore e d'uso (vedere "Inserimento di ruoli, limiti di valore e di uso"), (*)
- eventuale pseudonimo da inserire nel certificato in luogo del nome di battesimo e cognome del titolare ai sensi dell'art. 33 del [DLGS82] e dell'art.12, comma 3, lettera e) della [DLB45/09]. (*)

(*) Tutti i dati contrassegnati con l'asterisco sono inseriti nel certificato, tranne nel caso di utilizzo dello pseudonimo (in tal caso solo lo pseudonimo ed il paese di residenza sono inseriti nel certificato).

Tutte le informazioni sopra elencate sono obbligatorie ai fini della registrazione dell'utente e del rilascio del certificato. Altre informazioni elencate nel modulo (indirizzo dell'Organizzazione o di residenza del richiedente, telefono, ecc.) sono facoltative. 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 ne verifica la validità, userà in seguito tale indirizzo per trasmissioni con valore giuridico secondo quanto disposto dall'art. 45 comma 2 del [DLGS82]. Con indirizzo "valido" si intende un indirizzo corrispondente ad una casella (mailbox) di posta elettronica (e-mail) effettivamente esistente e che l'utente consulta con regolarità. L'utente si assume ogni responsabilità nel caso in cui l'indirizzo di posta elettronica fornito al certificatore in sede di registrazione risulti inesatto o attribuito a persona diversa.

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 [DLGS82];
- si assume esplicitamente gli obblighi di cui all'art. 7, comma 3 del [DPCM];
- dichiara di aver preso visione del Manuale Operativo e di averlo compreso ed accettato;
- acconsente al trattamento dei propri dati personali nel rispetto del [DLGS196] e dell'informativa fornita.

Nel modulo di registrazione, inoltre, il richiedente fornisce la propria autorizzazione alla eventuale pubblicazione del certificato, la quale avviene solo nei casi previsti (secondo lo specifico cliente).

Nell'ambito dell'emissione della CNS contenente anche il certificato qualificato per la firma digitale, l'emissione di tale certificato si intende richiesta dalla PA emittente; in tal caso Actalis non richiede la compilazione e sottoscrizione di un modulo di registrazione specifico. In tale ambito, Actalis emette i certificati qualificati sulla base dei dati anagrafici trasmessi ad Actalis in modalità sicura dalla PA emittente.

Nell'ambito dell'emissione di un certificato abbinato ad una CNS la PA effettua l'identificazione e registrazione dei titolari di CNS secondo procedure proprie che devono comunque rispettare le [RTCNS] e al contempo il [DPCM]; pertanto i seguenti requisiti devono essere soddisfatti:

- il titolare di CNS deve esibire all'operatore di registrazione un documento di identità o un documento di riconoscimento equipollente ai sensi dell'art.35 del [DPR 445] e delle [RTCNS] al momento della consegna del PIN di firma e/o all'attivazione del certificato (nel caso in cui questo venga emesso pre-sospeso);
- la PA deve conservare evidenza dell'identificazione di ciascun titolare ai fini della consegna del PIN di firma e attivazione del certificato (per es. mediante fotocopia del documento d'identità esibito dal titolare); tali evidenze devono essere conservate per 20 anni, ai sensi dell'Art. 30, comma 3, lettera j) del [DLGS82] e successive correzioni e integrazioni, pertanto, la PA emittente deve essa stessa provvedere a tale conservazione oppure consegnare ad Actalis le suddette evidenze (in quest'ultimo caso sarà Actalis a provvedere alla conservazione).

4.2.1.1 Abilitazioni professionali

Con riferimento alla lettera a), comma 3 dell'art. 28 del [DLGS82] 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.

Nel caso di certificato abbinato ad una CNS, le eventuali abilitazioni professionali da indicare nel certificato sono verificate dalla PA emittente con procedure proprie. L'evidenza di tale verifica deve peraltro essere conservata per 20 anni, ai sensi dell'Art. 30, comma 3, lettera j) del [DLGS82] e successive correzioni e integrazioni, pertanto, la PA emittente deve provvedere essa stessa a tale conservazione oppure consegnare ad Actalis le suddette evidenze (in quest'ultimo caso sarà Actalis a provvedere alla conservazione).

4.2.1.2 Inserimento di ruoli, limiti di valore e di uso

Con riferimento al comma 3 dell'art. 28 del [DLGS82], il titolare o il terzo interessato possono richiedere l'indicazione nel certificato delle seguenti informazioni aggiuntive:

- ruolo o qualifica del titolare (es. poteri di rappresentanza, cariche sociali, appartenenza ad un ente od organizzazione, abilitazioni professionali);
- limiti di utilizzo, compresi quelli derivanti dalla titolarità delle qualifiche e dai poteri di rappresentanza;
- limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere utilizzato.

I limiti di utilizzo sono espressi in linguaggio naturale con un massimo di 200 caratteri.

Nel caso in cui l'inserimento di tali informazioni sia richiesto direttamente dal titolare, quest'ultimo produce idonea documentazione (ad es. certificato della CCIAA competente, attestante i poteri di rappresentanza, non anteriore a 30 gg. dalla data della richiesta). Il titolare si impegna a comunicare tempestivamente al certificatore ogni variazione alle informazioni aggiuntive fornite. Il certificatore si riserva la facoltà di verificare la pertinenza dell'informazione con lo scopo per il quale il certificato è richiesto.

Nel caso in cui l'inserimento di tali informazioni sia richiesto dal Terzo Interessato, quest'ultimo comunica preventivamente al Certificatore il consenso.

La falsa dichiarazione o attestazione al Certificatore di identità, stati o altre qualità personali riferite alla propria o altrui persona è sanzionata con la pena della reclusione fino ad un anno, secondo quanto disposto dall'art. 495-bis del Codice Penale, così come modificato dalla [L. 48].

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

La data di redazione della comunicazione deve essere non anteriore a 30 giorni alla data prevista per la registrazione del primo utente appartenente all'organizzazione in discorso.

La comunicazione 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 comunicazione 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 30 giorni prima della data prevista per la registrazione del primo utente appartenente all'organizzazione in discorso.

La comunicazione deve contenere una dichiarazione che impegna l'organizzazione a comunicare tempestivamente al certificatore ogni variazione alle informazioni fornite per singolo nominativo indicato.

Il certificatore, sia nel caso in cui le informazioni aggiuntive siano richieste dal titolare che dal Terzo Interessato, si riserva la facoltà di verificare la pertinenza dell'informazione con lo scopo per il quale il certificato è richiesto.

Nel caso di certificato abbinato ad una CNS, l'eventuale ruolo del titolare o i limiti di valore e di uso da indicare nel certificato sono verificati dalla PA emittente con procedure proprie. L'evidenza di tale verifica deve peraltro essere conservata per 20 anni, ai sensi dell'Art. 30, comma 3, lettera j) del [DLGS82] e successive correzioni e integrazioni, pertanto, la PA emittente deve essa stessa provvedere a tale conservazione oppure consegnare ad Actalis le suddette evidenze (in quest'ultimo caso sarà Actalis a provvedere alla conservazione).

4.2.1.3 Identificazione da parte di un pubblico ufficiale

L'identificazione degli utenti può anche essere svolta "a distanza" da un pubblico ufficiale ai sensi dell'Art. 21 del "Testo Unico delle disposizioni legislative e regolamentari in materia di Documentazione Amministrativa" [DPR445]. In breve, l'utente deve:

- recarsi presso un pubblico ufficiale (vedere più sotto);
- compilare in sua presenza il modulo di registrazione e le eventuali dichiarazioni accompagnatorie se previste secondo il tipo di certificato (come descritto nei par. precedenti);
- richiedere al pubblico ufficiale l'autentica della propria firma ai sensi del [DPR445], esibendo a tale scopo un documento valido d'identificazione;
- inviare ad Actalis gli originali dei documenti firmati e l'originale dell'autentica rilasciata dal pubblico ufficiale (datata, firmata e timbrata).

Per farsi identificare con tale modalità l'utente può rivolgersi a:

- un notaio (anche presso un consolato italiano all'estero),
- un cancelliere, ufficiale d'anagrafe, segretario comunale o altro incaricato dal Sindaco.

La possibilità di identificazione dell'utente da parte dell'ufficio notarile di un consolato consente il rilascio di certificati anche a coloro che risiedono all'estero.

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 personalmente l'identità del richiedente (mediante esame del documento d'identità di fronte al richiedente) tranne nel caso in cui tale verifica sia stata fatta a distanza con le modalità descritte nel par. 4.2.1.3 (in tal caso l'operatore di registrazione verifica la documentazione di identificazione inviata dal richiedente);
- 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 l'eventuale 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, egli completa la procedura secondo i seguenti passi:

- rilascia o invia in busta chiusa al richiedente un codice riservato, col quale il richiedente può farsi riconoscere dal certificatore;

- controfirma il modulo di registrazione e archivia l'originale e la documentazione annessa; ai sensi dell'art. 32 comma 3, lettera j) del [DLGS82] e successive correzioni ed integrazioni, il modulo è conservato per almeno 20 anni;
- fornisce al richiedente copia del modulo compilato con le relative condizioni contrattuali;
- inserisce nel database di registrazione (in tempo reale o un modo differito, con modalità tecniche che possono variare caso per caso) tutte le informazioni raccolte.

Ai sensi degli 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.

Nell'ambito dell'emissione di un certificato abbinato ad una Carta Nazionale dei Servizi (CNS), si rimanda a quanto riportato nel paragrafo **4.2.1**.

4.2.3 Dispositivo di firma

4.2.3.1 Requisiti di sicurezza e caratteristiche del dispositivo di firma

Il certificatore può fornire al richiedente un dispositivo sicuro per la generazione delle firme conformi alle caratteristiche e ai requisiti di sicurezza di cui all'art. 35 del [DLGS82] ed all'art. 9 del [DPCM].

Il dispositivo di firma può essere fornito al richiedente anche da una terza parte, purché il dispositivo sia conforme alle caratteristiche e ai requisiti di sicurezza di cui ai succitati articoli e sia espressamente approvato dal Certificatore.

Nel caso della firma digitale con procedura automatica o remota, il dispositivo sicuro per la generazione delle firme è un HSM (Hardware Security Module) che può essere ubicato presso il Certificatore (Actalis) oppure presso il Cliente. Per altre informazioni sui requisiti di sicurezza si veda il §4.12.2.

Nel caso di certificato di firma su CNS, il dispositivo di firma - che deve rispondere anche ai requisiti dettati dalle [RTCNS] - viene fornito direttamente dalla PA emittente.

4.2.3.2 Personalizzazione del dispositivo di firma

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, o comunque in sua presenza, e si basa su interazioni telematiche sicure con il certificatore (generalmente connessioni via Internet protette da protocolli che garantiscano un adeguato livello di sicurezza). 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).

Nel caso della firma digitale con procedura automatica o remota, il Certificatore tiene traccia di quali HSM (modello e numero di serie) sono utilizzati per gestire le chiavi di firma degli utenti.

Nel caso di certificato abbinato a una CNS, la personalizzazione del dispositivo di firma può avvenire centralmente, presso il certificatore, oppure presso il produttore delle CNS, secondo gli specifici accordi in essere con la PA emittente, comunque nel rispetto delle [RTCNS].

4.2.3.3 Conservazione e distribuzione del dispositivo di firma

I dispositivi di firma sono conservati, in attesa di essere forniti ai clienti, in un magazzino accessibile solo da personale autorizzato. La gestione del magazzino (descrizione delle attività svolte, definizione di ruoli e responsabilità di Actalis e dell'outsourcer del servizio di magazzino che fornisce gli spazi e i servizi a supporto) sono descritti in un'apposita procedura del Sistema Qualità aziendale di Actalis.

I dispositivi di firma possono essere distribuiti ai clienti con o senza certificato qualificato di firma. Nel caso in cui il dispositivo sia predisposto da Actalis e la sua consegna al titolare non avvenga in modo diretto, i dati per l'attivazione del dispositivo sono spediti separatamente ed Actalis non conserva copia della chiave privata di firma del titolare.

Viene mantenuto un inventario dei dispositivi di firma da parte del Responsabile della registrazione o da un suo delegato ai sensi dell'art. 33 del [DPCM].

4.3 Generazione delle chiavi (art. 36/3/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].

Nel caso di certificato abbinato ad una CNS, la generazione delle chiavi di firma può avvenire centralmente ed anche al di fuori della CNS stessa; inoltre essa può essere svolta presso il certificatore oppure presso il produttore delle CNS, secondo gli specifici accordi in essere con la PA emittente, comunque nel rispetto delle [RTCNS] e dell'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 del servizio di certificazione o sotto la sua supervisione.

Con il consenso del DigitPA, le chiavi di certificazione possono essere utilizzate per finalità diverse da quelle indicate all'art. 4, comma 4, lettera b).

Il profilo dei certificati di certificazione è conforme alla specifica RFC 5280 e contiene le estensioni di cui all'art. 12, comma 5, della [DLB45/09].

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 associata ad un singolo sistema di validazione temporale;
- le chiavi vengono sostituite dopo non più di tre mesi 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 della certificazione o sotto la sua supervisione.

Il profilo dei certificati di marcatura temporale è conforme alla specifica RFC 5280 e contiene le estensioni di cui all'art. 15 della [DLB45/09].

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 l'autenticazione dell'utente mediante digitazione del PIN del dispositivo.

Nel caso della firma con procedura automatica o remota, la generazione delle chiavi di sottoscrizione sul dispositivo sicuro:

- richiede l'autenticazione dell'utente con le modalità previste dallo specifico sistema di firma automatica o remota utilizzato;
- secondo le caratteristiche dallo specifico sistema di firma automatica o remota utilizzato, può essere attivata anche dall'operatore di registrazione con modalità che garantiscono la riservatezza del PIN che deve restare noto solamente all'utente titolare.

Nel caso di certificato abbinato a una CNS, la generazione delle chiavi di firma può avvenire centralmente ed anche al di fuori della CNS stessa; inoltre essa può essere svolta presso il certificatore oppure presso il produttore delle CNS, secondo gli specifici accordi in essere con la PA emittente, comunque nel rispetto delle [RTCNS] e dell'art. 8 del [DPCM].

4.4 Emissione dei certificati qualificati (art. 36/3/i)

La seguente figura illustra, in modo semplificato, una procedura di richiesta ed emissione del certificato su iniziativa dell'utente titolare; tale procedura si articola nelle seguenti fasi:

- generazione della coppia di chiavi ed invio al certificatore della chiave pubblica;
- verifica, da parte del certificatore, dell'autenticità e correttezza della richiesta;
- generazione e (se prevista) pubblicazione del certificato sul directory server;
- installazione del certificato sul dispositivo sicuro per la generazione della firma.

In questa procedura, il richiedente interagisce col certificatore con modalità telematiche.

Procedure analoghe, sempre aderenti alla normativa vigente, possono essere adottate in accordo con il cliente per particolari tipologie di servizi.

- 1) attiva la generazione della coppia di chiavi e della corrispondente richiesta di certificato in formato PKCS#10
- 2) invia la richiesta di certificato in formato PKCS#10, il codice riservato ed altri dati accessori
- 3) viene verificata l'autenticità e validità della richiesta
- 4) viene generato il certificato
- 5) pubblicazione del certificato sulla directory
- 6) invio del certificato al richiedente
- 7) installazione del certificato sul dispositivo di firma

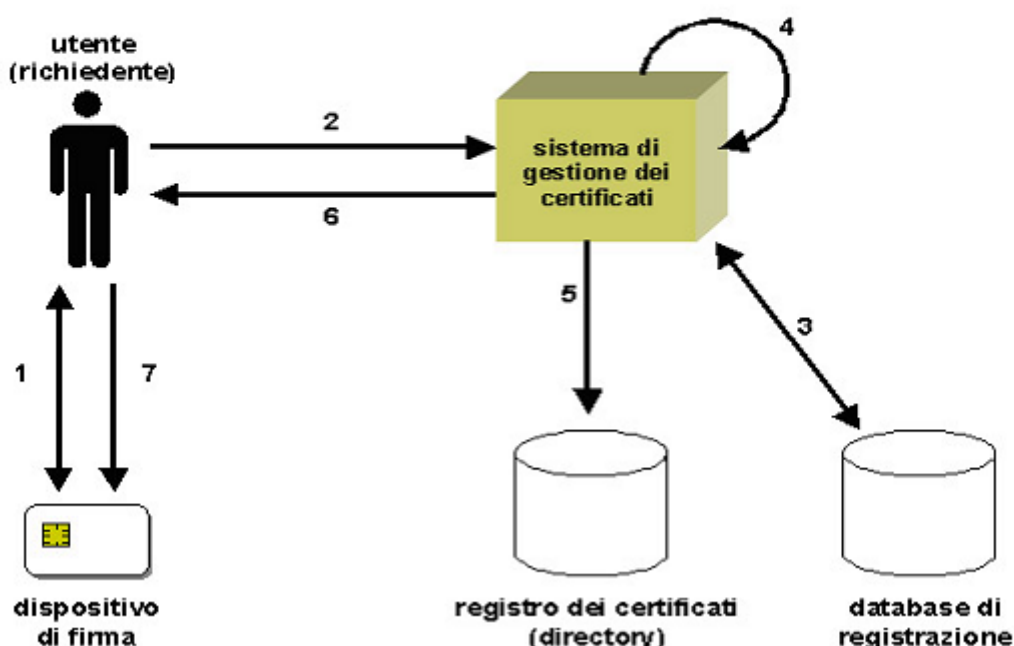


Figura 2: richiesta, generazione e rilascio del certificato

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

Nel caso di certificato abbinato ad una CNS, tuttavia, la procedura può essere diversa. In particolare:

- la generazione delle chiavi può avvenire in modo diverso, come già detto al paragrafo 4.3;
- la generazione del certificato e la sua installazione sulla CNS (come parte dell'operazione di personalizzazione del dispositivo di firma) può avvenire in modo diverso, come già detto al paragrafo 4.2.3.2.

4.4.1 Richiesta del certificato

Il richiedente deve approntare una richiesta di certificazione, ossia un insieme di dati che include almeno quanto segue:

- la chiave pubblica di cui chiede la certificazione;
- un dato che dimostri il possesso, da parte del richiedente, della corrispondente chiave privata;
- un codice segreto personale, ottenuto in fase di registrazione, a dimostrazione della propria identità.

Le prime due informazioni (chiave pubblica e prova del possesso della chiave privata) devono essere fornite al certificatore nel formato descritto nella specifica pubblica PKCS#10. L'adozione di altri formati dovrà essere preventivamente concordata tra richiedente e certificatore.

La richiesta di certificazione deve quindi essere inviata al certificatore attraverso un "canale telematico di comunicazione sicuro". Esso è di norma ottenuto con l'uso del protocollo SSLv3/TLS.

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

Ai sensi dell'art. 32 comma 3, lettera j) del [DLGS82] 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 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;
- se le verifiche di cui ai punti precedenti vengono superate, l'operatore di certificazione (sotto la supervisione del responsabile della certificazione) abilita la generazione del certificato, con un sistema conforme all'art. 28 del [DPCM];
- il certificato viene quindi generato col formato previsto dalla [DLB45/09]; il certificato contiene le informazioni previste nell'art. 15 del [DPCM] e nell'art. 28 del [DLGS82] e successive modifiche ed integrazioni;
- la generazione del certificato è attestata da un riferimento temporale;
- la generazione del certificato è registrata nel giornale di controllo.

L'indicazione che il certificato è qualificato e che la chiave privata, corrispondente alla chiave pubblica presente nel certificato qualificato, è memorizzata su un *dispositivo sicuro per la creazione della firma* (SSCD) è rappresentata, rispettivamente, dai valori id-etsi-qcs-QcCompliance ed id-etsi-qcs-QcSSCD inseriti nell'estensione qcStatements del certificato.

Il periodo di validità del certificato varia secondo le esigenze dei clienti e l'uso previsto dei certificati.

Nel caso di certificati da installare su carte CNS, la data di scadenza del certificato di firma generalmente coincide con la data di scadenza della carta o con la data di scadenza del contratto tra l'Amministrazione emittente ed il certificatore, secondo gli accordi in essere.

4.4.3 Policy supportate

Il profilo del certificato è conforme alla [DLB45/09]. Attributi ed estensioni facoltativi possono variare in rapporto alle specifiche policy utilizzate, previamente concordate con il cliente.

Le policy Actalis, descritte in altrettanti documenti pubblicati sul sito web del servizio di certificazione <https://portal.actalis.it>, sono identificate dagli OID presenti nell'estensione CertificatePolicies ed indicati nella tabella riportata di seguito:

Policy OID	Descrizione
1.3.159.1.1.1	Certificati qualificati normali.
1.3.159.1.5.1	Certificati qualificati con limitazioni d'uso (per es. per procedura automatica).
1.3.159.1.15.1	Certificati qualificati per firma con procedura remota.

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, nei casi previsti, secondo la seguente procedura:

- il certificato è pubblicato nel registro dei certificati; il momento (data/ora) della pubblicazione è attestato da un riferimento temporale;
- la pubblicazione del certificato ed il relativo riferimento temporale sono registrati nel giornale di controllo.

La pubblicazione del certificato non è una componente standard del servizio; il consenso del titolare non comporta automaticamente la pubblicazione del certificato, a meno che questa non sia prevista nell'ambito del servizio specifico erogato al cliente.

4.5 Sospensione e revoca dei certificati (art. 36/3/l)

La sospensione o revoca del certificato avviene, nel rispetto degli artt. da 18 a 24 del [DPCM], 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.

Nel caso di certificato abbinato ad una CNS:

- la PA emittente è responsabile di definire un servizio di "contact center" per l'assistenza, nonché per la revoca o sospensione della CNS (come disposto dalle [RTCNS]);

- la sospensione o revoca del certificato può avvenire anche su richiesta della PA emittente, sulla base degli accordi in essere col certificatore, e può basarsi su procedure in parte diverse da quelle descritte di seguito.

4.5.1 *Circostanze per la sospensione o revoca del certificato*

La revoca può avvenire in seguito alle seguenti circostanze:

- smarrimento, furto o guasto del dispositivo sicuro per la firma;
- 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 di conoscenza di cause limitative delle capacità del titolare

La sospensione può avvenire in seguito alle seguenti circostanze:

- richiesta di revoca di cui non é 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.

- 1) richiede la sospensione o revoca, fornendo le informazioni necessarie
- 2) verifica i dati della richiesta con quelli presenti nel database di registrazione
- 3) avvia il processo di sospensione o revoca
- 4) viene generata la CRL
- 5) pubblicazione della CRL sul registro dei certificati (directory)

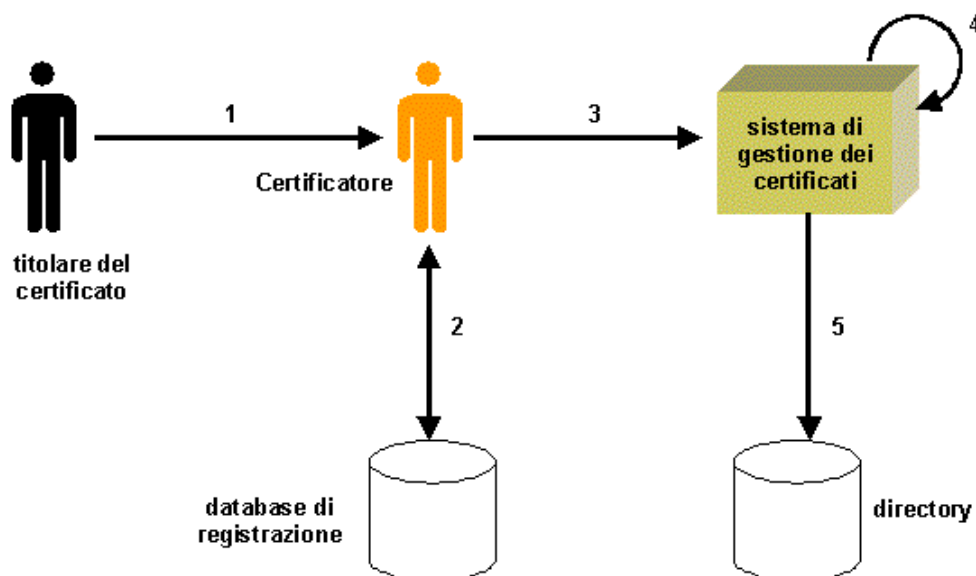


Figura 3: sospensione o revoca del certificato su richiesta del titolare

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

4.5.2.1 Procedura di sospensione o revoca dei certificati

Il titolare inoltra la richiesta al Certificatore utilizzando un'applicazione web disponibile sul sito del servizio di certificazione <https://portal.actalis.it>. La richiesta può essere inoltrata 24 ore su 24.

In alternativa il titolare può:

- compilare un modulo cartaceo sottoscritto con firma autografa. Il modulo firmato può essere consegnato a mano, esibendo contestualmente un documento di riconoscimento presso lo sportello dove è stata sottoscritta la richiesta del servizio di certificazione, oppure può essere spedito direttamente dal titolare al Certificatore, per mezzo di una raccomandata con ricevuta di ritorno. L'indirizzo a cui deve essere inviata la richiesta cartacea è prestampato sul modulo. In caso di smarrimento o furto del dispositivo di firma, oltre alla copia fotostatica di un documento di riconoscimento, va allegata una fotocopia della denuncia dell'evento alla Polizia o ai Carabinieri.
- telefonare al numero del servizio di assistenza reperibile sul sito del servizio di certificazione <https://portal.actalis.it> e sul sito web www.actalis.it, fornendo le seguenti informazioni:
 - tipo di intervento richiesto (sospensione o revoca);
 - il codice di revoca del certificato;
 - 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;

Nel caso in cui sia richiesta una revoca e non sia possibile accertare in tempo utile l'autenticità della richiesta, Actalis procede alla sospensione del certificato.

La sospensione ha una durata massima di 15 giorni solari. Al termine del periodo di sospensione, in assenza di diverse indicazioni da parte del soggetto che ha richiesto la sospensione, il certificato viene automaticamente riattivato.

La richiesta telefonica di revoca deve essere confermata inviando, via fax, la documentazione prevista per la richiesta di revoca sottoscritta con firma autografa. Con le stesse modalità deve essere confermata la richiesta di sospensione telefonica. Il certificatore può rigettare la richiesta nel caso la giudichi incompleta o non leggibile.

Il numero del servizio di assistenza è presidiato dal lunedì al venerdì dalle ore 9.00 alle 13.00 e dalle 14.30 alle 17.30 escluso i giorni festivi; dalle 9.00 alle 14.00 nei giorni semifestivi (24 e 31 dicembre) da un gruppo di operatori che svolge anche attività di sospensione o revoca dei certificati su delega di Actalis (cfr. la sezione "Note sull'organizzazione del personale"). Sul sito del servizio di certificazione <https://portal.actalis.it> è inoltre disponibile un modulo on-line per la richiesta di informazioni di diversa natura (commerciali, legali, ecc.).

4.5.3 Richiesta di sospensione o revoca da parte del terzo interessato

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

Il Terzo Interessato inoltra al Certificatore una richiesta di revoca o sospensione sottoscritta.

Il certificatore rende disponibili alle RA strumenti e procedure per effettuare richieste di sospensione o revoca per via telematica.

Nel caso in cui si utilizzi il modulo di richiesta cartaceo predisposto da Actalis, quest'ultimo va inviato al certificatore, unitamente alla documentazione giustificativa, per mezzo di una raccomandata con ricevuta di ritorno. L'indirizzo a cui deve essere inviata la richiesta cartacea è prestampato sul modulo stesso.

In alternativa, il terzo interessato può inviare al certificatore una lettera datata e firmata nella quale fornisce almeno le seguenti informazioni:

- organizzazione di appartenenza del richiedente;
- 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) 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:

- provvede alla sospensione o revoca nei tempi richiesti (cfr. la sezione “Completamento della revoca o sospensione del certificato”);
- notifica la revoca o la sospensione al titolare.

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).

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 un corrispondente riferimento temporale.

Il certificatore svolge l’operazione tempestivamente 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 Sostituzione delle chiavi (art. 36/3/m)

4.6.1 Sostituzione delle chiavi di sottoscrizione degli utenti

Ai sensi dell’art. 15 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 e in ogni caso varia da un minimo di 1 anno ad un massimo di 6 anni.

Il rinnovo del certificato consiste nella generazione di una nuova coppia di chiavi (da parte del titolare) ed emissione di un ulteriore certificato (da parte del certificatore) con periodo di validità normalmente uguale al periodo di validità del certificato in scadenza. La procedura di rinnovo deve essere

avviata almeno trenta giorni prima della data di scadenza del periodo di validità del certificato. Il mancato rispetto di tale termine richiede l'avvio di procedure non standard con conseguenti possibili ritardi non quantificabili a priori.

La procedura seguita per il rinnovo è sostanzialmente identica a quella seguita per il rilascio del primo certificato. Essendo tuttavia il titolare già registrato, non è richiesta una nuova registrazione a meno che non siano intervenute variazioni dei suoi dati (variazioni che il titolare è comunque tenuto a segnalare tempestivamente al certificatore).

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

Nel caso di certificato abbinato alla CNS, secondo gli specifici accordi in essere con la PA emittente, la durata del certificato di firma può essere maggiore di 3 anni e può anche coincidere con la durata delle carte CNS (in quest'ultimo caso, il rinnovo del certificato non è ammesso).

4.6.2 Sostituzione delle chiavi di certificazione

Avviene nel rispetto dell'art. 26 del [DPCM]

È svolta a cura del responsabile della certificazione o sotto la sua supervisione.

4.6.3 Sostituzione delle chiavi di marcatura temporale

Avviene nel rispetto dell'art. 45 del [DPCM].

È svolta ogni tre mesi dal responsabile del servizio di certificazione o sotto la sua supervisione.

4.7 Gestione del registro dei certificati (art. 36/3/n)

4.7.1 Realizzazione del registro dei certificati

Il registro dei certificati è realizzato con software di tipo "directory server". La sua copia pubblica è interrogabile con protocollo LDAP attraverso Internet. 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

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 apposto un riferimento temporale come richiesto dall'art. 32 comma 3 del [DPCM].

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

4.7.3 Pubblicazione dei certificati e delle CRL

Nel directory vengono pubblicati i seguenti oggetti:

- solo nei casi previsti, i certificati dei titolari che ne hanno autorizzato la pubblicazione (rif. art. 29, comma 2 del [DPCM]);

- certificati delle chiavi di certificazione;
- certificati relativi ad accordi di certificazione;
- certificati delle chiavi di firma del DigitPA ove previsto;
- le liste dei certificati sospesi o revocati;

Con riferimento all'art. 18, 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.

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. 30 del [DPCM]. Un riferimento temporale (data/ora) attesta la pubblicazione della CRL.

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

- i certificati sono pubblicati, nei casi previsti, al momento 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 revocazioni, secondo una frequenza dipendente dalla 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, nonché la disponibilità del servizio.

4.8 Accesso al registro dei certificati (art. 36/3/o)

4.8.1 Protocolli supportati

L'accesso al registro dei certificati è consentito attraverso la rete Internet. L'indirizzo del server può variare secondo lo specifico servizio; questo può infatti presentare caratteristiche diverse in base al particolare cliente, alla policy dei certificati, alle specifiche condizioni contrattuali, ecc.

Il certificatore consente l'accesso al registro dei certificati col protocollo LDAP definito nella specifica pubblica RFC 2251 [LDAP3]. Il registro dei certificati è utilizzabile per le finalità di cui all'art.30 del [DPCM].

Per l'interrogazione del registro dei certificati può essere utilizzata qualsiasi applicazione client LDAP conforme alla specifica pubblica [LDAP3].

Il certificatore si riserva facoltà di rendere disponibili anche altre 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 Protezione dei dati personali (art. 36/3/q)

Actalis è titolare dei dati personali raccolti in fase di identificazione e registrazione degli utenti che richiedono certificati e si obbliga quindi a trattare tali dati con la massima riservatezza e nel rispetto di quanto previsto dal D.lgs. 196/03.

Nel caso in cui l'attività di identificazione e registrazione degli utenti avvenga presso una struttura delegata (RA), quest'ultima è qualificata come "titolare di trattamento autonomo correlato".

Nel caso della CNS, tuttavia, la responsabilità del rispetto delle normative vigenti in merito alla tutela dei dati personali è anzitutto in capo alla PA emittente, come sancito dalle [RTCNS].

4.9.1 Informativa ai sensi del D.Lgs. 196/03

Actalis, titolare del trattamento dei dati forniti dal Titolare, informa il Titolare stesso, ai sensi e per gli effetti di cui al D.Lgs. 196/03, che tali dati personali saranno trattati mediante archivi cartacei e strumenti informatici e telematici idonei a garantirne la sicurezza e la riservatezza nel rispetto delle modalità indicate nel succitato Decreto e degli obblighi di riservatezza.

I dati forniti si distinguono tra obbligatori e facoltativi (cfr. la sezione 4.2.1). I dati obbligatori sono necessari allo svolgimento del Servizio; il loro conferimento è dunque indispensabile ed un eventuale rifiuto dal parte del Titolare comporterà l'impossibilità di concludere il contratto. Si noti che la pubblicazione del certificato nel Registro dei Certificati (cfr. la sezione 4.7) – ove prevista – comporta la diffusione a terzi, anche in Paesi al di fuori dell'Unione Europea, delle informazioni contenute nel certificato stesso (cfr. la sezione 4.2.1). I dati facoltativi agevolano semplicemente il Servizio ed il loro mancato conferimento non ostacola la conclusione del contratto.

I dati forniti saranno trattati esclusivamente per finalità relative al rilascio o al rinnovo di certificati ai sensi del D.lgs. n.82/2005 e s.m.i. e del DPCM 30/03/2009, e potranno essere comunicati alle società che forniscono consulenza ed assistenza tecnica al Certificatore. In relazione ai predetti trattamenti dei dati, il Titolare potrà esercitare i diritti di cui al D.Lgs. 196/03.

4.9.2 Archivi contenenti dati personali

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

- le informazioni relative ai titolari dei certificati 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, ovvero – nel caso di certificato abbinato alla CNS – comunicati dalla PA emittente. I dati obbligatori sono indispensabili per il rilascio del certificato qualificato. 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.

I dati personali contenuti nei certificati, sono resi pubblici su autorizzazione del titolare e comunicati a terzi nei casi consentiti dal titolare e nel rispetto del [DLGS196].

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 un identificativo utente e una parola chiave personale;
- l'applicazione mantiene traccia, in un apposito registro, 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.

4.9.3 Misure di tutela della riservatezza

Ai sensi dell'art. 32 del [DLGS82] e successive modificazioni, il certificatore tratta tali dati personali nel rispetto del [DLGS196] 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 Apposizione e definizione del riferimento temporale (art. 36/3/p)

4.10.1 Riferimento temporale

Il riferimento temporale è un'informazione contenente la data e l'ora associata ad uno o più documenti informatici.

Il riferimento temporale è generato con un sistema che garantisce stabilmente uno scarto non superiore ad un minuto secondo rispetto alla scala UTC.

Le indicazioni temporali sono fornite in formato leggibile dall'utente e con riferimento all'ora legale vigente al momento indicato per l'operazione. Per la data il formato impiegato è "gg/mm/aaaa" mentre per l'indicazione oraria si utilizza il formato "hh:mm:ss", dove hh è in formato 24 ore. Al dato temporale è fatta seguire tra parentesi la "zona" ossia la differenza (in ore e minuti) tra l'ora legale locale ed UTC. La rappresentazione di tale valore è in formato "[+|-]hhmm", dove il primo carattere indica una differenza positiva o negativa.

Il riferimento temporale principale usato da Actalis è ottenuto da un dispositivo di alta precisione che garantisce una differenza non superiore ad un minuto secondo rispetto alla scala di tempo UTC(IEN). In aggiunta a tale fonte, si accede anche ad un servizio NTP pubblico affidabile.

Il sistema effettua continuamente cicli auto-diagnostici per verificare la disponibilità delle sorgenti di tempo ed eventualmente si pone nello stato "fuori linea" se le sorgenti vengono a mancare.

4.10.2 La marca temporale

Una marca temporale è un messaggio firmato digitalmente da una terza parte fidata che lega in modo sicuro e verificabile un qualsiasi documento informatico (o altro tipo di file) ad un riferimento temporale affidabile. Avendo a disposizione la marca temporale ottenuta per un certo documento, è possibile dimostrare a terzi che tale documento effettivamente esisteva almeno alla data/ora riportata nella marca (ossia, non più tardi di tale data/ora).

I certificatori accreditati devono disporre di un sistema di validazione temporale conforme al Titolo IV del [DPCM] che prevede la generazione di una marca temporale. Di seguito sono pertanto descritte le modalità operative di erogazione di marche temporali da parte di Actalis.

4.10.2.1 Modalità di erogazione del servizio

Il servizio è regolato da un apposito contratto, indipendente da quello che si applica al servizio di certificazione, nel quale sono precisati i livelli di servizio, le responsabilità, etc. Il servizio consiste nell'erogazione da parte di Actalis di marche temporali via rete (Internet od altre reti) su richiesta del cliente. Di seguito si descrivono le principali caratteristiche tecnico-operative del servizio erogato da Actalis in conformità al Titolo IV del [DPCM].

La marca temporale è firmata ed emessa da un apposito sistema operante presso Actalis, a fronte delle richieste degli utenti pervenute attraverso la rete. Il sistema verifica le richieste e la posizione contrattuale dell'utente, quindi genera le marche temporali richieste e le restituisce agli utenti.

Sono accettate solo le richieste codificate nel rispetto della specifica pubblica [RFC 3161]. Le marche temporali restituite agli utenti sono a loro volta conformi alla specifica pubblica [RFC 3161].

Tutte le marche emesse sono conservate dal certificatore per 20 anni.

4.10.2.2 Accesso al servizio

La responsabilità della costruzione della richiesta di marca temporale e della lettura, validazione e visualizzazione della marca temporale ottenuta è a carico dell'applicazione client.

Il protocollo utilizzato per la comunicazione è HTTPS. Il servizio adotta un sistema di riconoscimento degli utenti autorizzati basato sulla presentazione di un codice utente e di una password. Tali informazioni sono fornite all'utente successivamente alla sottoscrizione del contratto di servizio.

Il servizio - per sua natura - tutela la riservatezza dei documenti degli utenti, poiché non richiede che il documento per il quale si richiede una marca temporale venga inviato ad Actalis, ma solo la sua impronta (fingerprint), come del resto è previsto dalla specifica pubblica [RFC 3161].

4.10.2.3 Modalità di utilizzo del servizio

Il servizio può essere utilizzato con qualunque applicazione in grado di produrre una struttura "TimeStampRequest" ed inviare tale struttura ad una URL su protocollo HTTPS, nel rispetto della specifica [RFC 3161], quindi leggere e conservare la "TimeStampResponse" prodotta dal servizio.

La URL a cui inviare la "TimeStampRequest" e le credenziali di identificazione da specificare nelle richieste sono forniti da Actalis all'utente successivamente alla sottoscrizione del contratto.

Pur confermando l'aderenza del servizio allo standard [RFC 3161], Actalis garantisce la corretta fruizione del servizio solo nel caso in cui il cliente utilizzi strumenti software forniti da Actalis stessa.

4.10.2.4 Sicurezza fisica

Il servizio di marcatura temporale di Actalis si basa su un server web di front-end che gestisce le transazioni con i client, l'autenticazione, l'accounting e l'archiviazione delle marche temporali ed un server di back-end che si occupa della creazione delle marche temporali e della gestione degli apparati di acquisizione e sincronizzazione del riferimento temporale.

I server di marcatura temporale della Actalis sono ospitati in sale tecniche ad accesso controllato con badge e in alcuni casi badge + PIN. Solo il personale autorizzato può accedere a tale sala. La sala tecnica è protetta da allagamenti ed incendi mediante appositi presidi (sensori, spruzzatori, condizionamento, etc). Il server è alimentato con linea elettrica preferenziale, sorretta da gruppo di continuità.

4.10.2.5 Sicurezza logica

Il server di marcatura temporale di Actalis firma le marche temporali mediante un dispositivo crittografico hardware (o "dispositivo di firma") di altissima qualità e sicurezza. Viene usato l'algoritmo RSA con una chiave di lunghezza 1024 bit usata esclusivamente a scopo di marcatura temporale. La coppia di chiavi RSA è generata all'interno del dispositivo di firma. La chiave privata della coppia è usata all'interno del dispositivo di firma. Il dispositivo di firma può essere attivato solo da un operatore appositamente autorizzato e dotato della necessaria parola-chiave.

4.11 Utilizzo del sistema di verifica delle firme (art. 36/3/r)

In riferimento all'art. 10 del [DPCM], Actalis offre due diverse modalità: un'applicazione di tipo stand-alone, denominata commercialmente "File Protector", ed un servizio di verifica on-line accessibile dal sito web www.actalis.it. Entrambe le soluzioni consentono la verifica delle firme digitali apposte su documenti informatici sotto forma di "buste crittografiche" in standard PKCS#7. L'applicazione File Protector consente la verifica di firme digitali in formato PKCS#7, CMS, PDF e XMLDSIG.

Tali applicazioni consentono di verificare:

- l'integrità del documento firmato e i dati del firmatario;
- l'autenticità e l'affidabilità del certificato del firmatario;
- l'eventuale stato di sospensione o revoca del certificato del firmatario.

Pertanto il processo di validazione di una firma richiede:

- il certificato del firmatario (presente nella "busta crittografica" per conformità alla [DLB45/09]);
- il certificato della chiave di certificazione emittente per verificare l'autenticità, integrità ed affidabilità del certificato del firmatario;
- l'accesso alla CRL (lista dei certificati sospesi o revocati) del certificatore emittente per verificare che il certificato del firmatario non sia stato sospeso o revocato.

Entrambe le applicazioni citate sono conformi al [DPCM] ed alla [DLB45/09].

L'uso del servizio di verifica on-line è estremamente semplice:

- l'utente seleziona con l'apposito pulsante "Sfogliala" il file firmato da verificare;

- l'utente, quindi, preme il pulsante "Verifica";
- al termine dell'elaborazione, il sistema visualizza il risultato della verifica ovvero: conferma che si tratta di un documento firmato, elenco dei firmatari ed altre informazioni (data firma, esito della verifica dell'integrità della firma, l'attendibilità o meno del certificato, la disponibilità online della relativa CRL); della stessa schermata, l'utente può recuperare il documento contenuto nella busta firmata;
- cliccando sul nominativo di ogni singolo firmatario, l'utente può accedere ad una schermata successiva per approfondire la verifica ovvero controllare la validità del certificato della CA che ha firmato il certificato del sottoscrittore ed accertarsi che il certificato del firmatario non sia presente nella lista dei certificati sospesi e revocati.

4.12 Generazione della firma digitale (art.38/3/s)

Per la generazione (creazione) della firma digitale sono previste due modalità:

- 1) firma con dispositivo di firma personale (es. smartcard, token USB o simile)
- 2) firma con procedura automatica e/o remota basata sull'impiego di HSM

Di seguito si forniscono alcune indicazioni di massima relative ai due casi.

4.12.1 Firma con dispositivo di firma personale

In questo caso l'utente utilizza un'applicazione di firma generalmente fornita dal Certificatore o comunque da questo approvata. Solitamente, l'utente utilizzerà l'applicazione "File Protector" già citata nella sezione 4.11. Tale applicazione infatti permette anche di:

- apporre una firma digitale producendo come risultato una busta crittografica nei formati standard PKCS#7 (CADES-BES a partire dal 3 settembre 2010) oppure PDF oppure XML DSIG;
- apporre firme multiple, interne o esterne. Una firma multipla interna è apposta ai soli dati all'interno della busta crittografica, una firma multipla esterna è apposta all'insieme della busta crittografica ovvero l'ultimo firmatario aggiunge la propria firma a quella dei firmatari antecedenti.

Firme digitali singole o multiple possono essere apposte a file di qualsiasi dimensione e formato.

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 di firma forniti o indicati da Actalis (ovvero forniti dalla PA emittente nel caso di certificato su CNS). Alla firma digitale viene sempre allegato il certificato qualificato del firmatario, nel rispetto della [DLB45/09].

Operativamente l'utente deve:

- accedere al dispositivo di firma digitando il relativo PIN associato;
- selezionare l'opzione "Firma" dal menu "File" oppure cliccare il bottone corrispondente;
- selezionare il percorso ed il nome del file che si intende firmare;
- premere il pulsante "Apri";
- visualizzare il documento che si intende firmare selezionando l'opzione "Apri documento";
- selezionare il certificato di firma che si intende utilizzare;

- apporre la firma al documento cliccando sul bottone “Aggiungi firma”. Nel caso in cui al documento selezionato sia già associata una firma digitale, è possibile aggiungere una nuova firma (firma multipla);

In fase di firma, l'applicazione “File Protector” verifica che il certificato di firma non sia sospeso, revocato o scaduto; nel caso in cui lo sia, l'applicazione visualizza un messaggio di avvertimento e non consente l'apposizione della firma digitale, poiché la firma basata su un certificato revocato, sospeso o scaduto non sarebbe valida (Art. 21, comma 3 del [DLGS82]). Questo controllo può essere disattivato dall'utente, il quale è comunque responsabile delle proprie firme digitali.

Nel caso di firma mediante CNS, si tenga presente che il PIN di attivazione della chiave di firma è diverso dal “PIN carta” (o PIN di autenticazione) e deve essere inserito prima di ogni singola firma.

4.12.2 Firma con procedura automatica e/o remota

In questo caso l'utente utilizza un'applicazione “client” di firma *generalmente* non fornita dal Certificatore, bensì dal Cliente (es. impresa, banca, ente pubblico, ecc) che eroga *servizi applicativi* ad utenti interni o esterni¹. Le specifiche modalità per l'esecuzione della firma dipendono quindi dalla particolare applicazione client usata dagli utenti caso per caso.

Il sistema di firma automatica e/o remota, basato su HSM, può essere ospitato presso il data center del Certificatore oppure presso il data center del Cliente; nel secondo caso, il Cliente deve rispettare i requisiti di sicurezza fisica, logica, operativa e gestionale indicati dal Certificatore, il quale svolgerà verifiche periodiche sul rispetto di tali requisiti.

L'applicazione client interagisce col server di firma automatica e/o remota attraverso la rete.

Nel caso di firma remota, la richiesta di firma proveniente dal client è sempre autenticata con due fattori. La modalità standard si basa sull'uso di un PIN statico (primo fattore) accompagnato da una password dinamica (OTP: One-Time Password) generata da un apposito dispositivo (“token”) fornito dal certificatore. Modalità alternative di autenticazione forte possono essere implementate, a fronte di situazioni specifiche che lo giustifichino, col previo assenso del DigitPA.

Nel caso di firma con procedura automatica, la richiesta di firma proveniente dal client è autenticata:

- almeno con username e password, nel caso in cui gli utenti accedano al server esclusivamente attraverso una rete locale (LAN) non raggiungibile da Internet e il certificato di firma contenga opportune limitazioni d'uso;
- con un sistema di autenticazione forte (a due fattori) nel caso in cui gli utenti possano accedere al server attraverso Internet e/o il certificato di firma non contenga limitazioni d'uso.

In tutti i casi (firma remota e/o automatica), le comunicazioni tra client e server di firma sono sempre protette con TLS/SSL, con autenticazione del server e cifratura della sessione con chiavi simmetriche di almeno 128 bit.

¹ Anche in questi casi, comunque, è possibile che l'applicazione client sia fornita dal Certificatore e che l'utente acceda direttamente al sistema di firma automatica o remota senza l'intermediazione di altri soggetti.

4.12.3 **Raccomandazioni per evitare la perdita di efficacia della firma digitale**

È importante tener presente che, affinché il documento firmato abbia “l'efficacia prevista dall'articolo 2702 del codice civile” (Art. 21, comma 2 del [DLGS82]), il documento da firmare “non deve contenere macroistruzioni e codice eseguibile tali da attivare funzionalità che possano alterare gli atti, i dati o i fatti rappresentati” (Art. 3, comma 3 del [DPCM]).

È responsabilità dell'utente firmatario accertarsi che tale condizione sia soddisfatta.

Di seguito si forniscono alcune raccomandazioni a titolo esemplificativo e non esaustivo:

- Non apporre firme digitali a documenti che contengono “campi” il cui valore viene aggiornato automaticamente dall'applicazione con cui si visualizza il documento prima della firma (ad es. i campi Page e Date dell'applicazione Microsoft Word™).
- Non apporre firme digitali a documenti che contengono codice eseguibile (ad es. le “macro” della suite Microsoft Office™). Ove possibile, disabilitare la funzionalità prima di aprire il documento da firmare (esempio: in Adobe Reader™, accedere alla finestra delle Preferenze, quindi selezionare la scheda “Javascript” e poi de-selezionare la casella “Abilita Javascript di Acrobat”).
- Prima di firmare un documento, trasformare i “campi” in valori statici (ad es. in Microsoft Word™ selezionare l'intero documento e poi premere la combinazione dei tasti CTRL+MAIUSC+F9).
- Verificare sempre l'esistenza di codice eseguibile incorporato nel documento da firmare (ad es. in Microsoft Word™ selezionare l'opzione “Strumenti” e, successivamente “Macro”; in Adobe Acrobat™ selezionare la voce di menu “Avanzate” > “Elaborazione documento” > “JavaScript documento”).

In generale è preferibile, prima di apporvi una o più firme digitali, *trasformare* il documento in un diverso formato, più aperto ed interoperabile (ad es. PDF). Il processo di trasformazione consente infatti, di eliminare dal documento elementi che possono potenzialmente rendere nulla la sottoscrizione stessa.

FINE DEL DOCUMENTO