

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0



Centro Nazionale per l'informatica nella Pubblica Amministrazione

UFFICIO SERVIZI DI SICUREZZA E CERTIFICAZIONE

**MANUALE OPERATIVO PER IL SERVIZIO DI CERTIFICAZIONE DI CHIAVI
PUBBLICHE PER LA RETE UNITARIA DELLA PUBBLICA AMMINISTRAZIONE**

Redatto da:	Data	Firma
G. RAGUCCI	29/11/2004	<i>Genaro Ragucci</i>

Verificato da:		
U. BUSSOTTI	01/12/2004	<i>U. Bussotti</i>
A. ROSSI	30/11/2004	<i>A. Rossi</i>

Approvato da:		
M. TERRANOVA	2/12/2004	<i>M. Terranova</i>

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_Certificazione 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0	

DISTRIBUZIONE

Disponibile in forma Non Controllata

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

INDICE

1	MODIFICHE DOCUMENTO	5
2	DEFINIZIONI	6
3	RIFERIMENTI NORMATIVI	10
4	INTRODUZIONE	10
4.1	PREMESSA.....	10
5	DATI IDENTIFICATIVI DEL CERTIFICATORE.....	10
6	MANUALE OPERATIVO	10
6.1	DATI IDENTIFICATIVI DEL MANUALE OPERATIVO	10
6.2	RESPONSABILE DEL MANUALE OPERATIVO	10
7	OBBLIGHI DEL CERTIFICATORE, DEL TITOLARE E DI QUANTI ACCEDONO PER LA VERIFICA DELLE FIRME	10
7.1	OBBLIGHI DEL CERTIFICATORE.....	10
7.2	OBBLIGHI DEL TITOLARE.....	10
7.3	OBBLIGHI DEI DESTINATARI.....	10
7.4	OBBLIGHI DEL TERZO INTERESSATO.....	10
8	RESPONSABILITÀ.....	10
8.1	RESPONSABILITÀ DEL CERTIFICATORE	10
8.2	LIMITAZIONE AGLI INDENNIZZI	10
9	TARIFFE....	10
10	PROCEDURE OPERATIVE	10
10.1	ORGANIZZAZIONE DEL CERTIFICATORE	10
10.1.1	<i>Attivazione dei referenti delle amministrazioni.....</i>	<i>10</i>
10.2	MODALITÀ DI IDENTIFICAZIONE E REGISTRAZIONE DEGLI UTENTI.....	10
10.2.1	<i>Identificazione.....</i>	<i>10</i>
10.2.2	<i>Compilazione e trasmissione della domanda di certificazione</i>	<i>10</i>
10.2.3	<i>Controllo e verifica dei dati</i>	<i>10</i>
10.2.4	<i>Produzione di ordini di lavoro per il gestore.....</i>	<i>10</i>
10.3	MODALITÀ DI GENERAZIONE DELLE CHIAVI PER LA CREAZIONE E LA VERIFICA DELLA FIRMA ED EMISSIONE DEI CERTIFICATI	10
10.3.1	<i>Sistemi di generazione.....</i>	<i>10</i>
10.3.2	<i>Dispositivo sicuro di firma.....</i>	<i>10</i>
10.3.3	<i>Personalizzazione del dispositivo di firma.....</i>	<i>10</i>
10.4	MODALITÀ CON CUI SI INDIVIDUA UN CERTIFICATO QUALIFICATO	10
10.4.1	<i>Limitazioni d'uso.....</i>	<i>10</i>
10.5	REVOCA E SOSPENSIONE DEI CERTIFICATI DEI TITOLARI.....	10
10.5.1	<i>Motivi per la revoca dei certificati dei titolari.....</i>	<i>10</i>
10.5.2	<i>Motivi per la sospensione dei certificati dei titolari</i>	<i>10</i>

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_Certificazione 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: n.ro allegati:	2.0 0

10.5.3	<i>Motivi per la revoca di certificati relativi a chiavi di certificazione.....</i>	<i>10</i>
10.5.4	<i>Motivi per la revoca di certificati relativi a chiavi di marcatura temporale</i>	<i>10</i>
10.5.5	<i>Modalità di revoca o sospensione.....</i>	<i>10</i>
10.5.6	<i>Modalità di revoca o sospensione dei certificati su iniziativa del Certificatore.....</i>	<i>10</i>
10.5.7	<i>Riattivazione di un certificato sospeso.....</i>	<i>10</i>
10.6	REVOCA DEI CERTIFICATI RELATIVI A CHIAVI DI CERTIFICAZIONE	10
10.7	REVOCA DEI CERTIFICATI RELATIVI A CHIAVI DI MARCATURA TEMPORALE	10
10.8	MODALITÀ DI RINNOVO DELLE CHIAVI DI FIRMA DEL TITOLARE.....	10
10.9	SOSTITUZIONE DELLE CHIAVI DI CERTIFICAZIONE	10
10.10	SOSTITUZIONE DELLE CHIAVI DI MARCATURA TEMPORALE.....	10
10.11	PROCEDURA DI RECUPERO DELLE CHIAVI PRIVATE PER SCOPI AUSILIARI	10
10.12	MODALITÀ DI GESTIONE DEL REGISTRO DEI CERTIFICATI.....	10
10.13	MODALITÀ DI PROTEZIONE DELLA RISERVATEZZA.....	10
10.14	MODALITÀ PER L'APPOSIZIONE E LA DEFINIZIONE DEL RIFERIMENTO TEMPORALE	10
10.14.1	<i>Chiavi di marcatura temporale.....</i>	<i>10</i>
10.15	MODALITÀ OPERATIVE PER L'UTILIZZO DEL SISTEMA DI VERIFICA DELLE FIRME	10
10.16	MODALITÀ OPERATIVE PER L'UTILIZZO E LA GENERAZIONE DELLE FIRME DIGITALI	10
10.16.1	<i>Formato dei documenti.....</i>	<i>10</i>

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_Certificazione 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: n.ro allegati:	2.0 0

1 MODIFICHE DOCUMENTO

DESCRIZIONE MODIFICA	EDIZIONE	DATA
Prima emissione	1.0	26/01/2001
Par. 3.1.1 - aggiornamento normativa di riferimento Par. 2 – aggiornamento nomenclatura da Area Sicurezza in Sezione Sicurezza Par. 5.1 – aggiornamento indirizzo Internet dove è presente il Manuale Operativo Par. 8 – aggiornamento gestione tariffe Par. 12.2.1 – aggiornamento disponibilità servizi di revoca Par. 12.4 – aggiornamento disponibilità servizi d'assistenza telefonica Par. 18.1 – aggiornamento durata certificati Par. 19 – aggiornamento procedura recupero chiavi di cifratura Par. 20.4 – aggiornamento indirizzo ldap	1.1	04/05/2001
Adeguamento CNIPA Adeguamento DPCM 13 gennaio 2004 Adeguamento DPR 445/00 e successive modificazioni Adeguamento Dlvo 196/03 Adeguamento DM 2 luglio 2004	2.0	29/11/2004

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

2 DEFINIZIONI

Ai fini del presente Manuale si applicano le definizioni contenute nel DPR 445/2000 e DPCM 13 gennaio 2004 e successive modificazioni.

Nel seguito vengono invece indicati i termini specifici utilizzati nel presente Manuale.

DEFINIZIONE	DESCRIZIONE
AIPA	Autorità per l'Informatica nella Pubblica Amministrazione.
Amministrazione	Insieme di utenti pubblici operante sulla Rete Unitaria della Pubblica Amministrazione che stipula un accordo con il Certificatore per il rilascio di certificati di firma digitale e di cifratura ai propri dipendenti e/o associati per un utilizzo limitato agli scopi da esso indicati.
Appartenenti all'Amministrazione	Dipendenti e/o associati a favore dei quali l'Amministrazione richiede l'emissione di un certificato digitale.
CACNIPA	L'infrastruttura organizzativa e tecnologica, realizzata nel 2004 dal CNIPA-Ufficio Servizi Sicurezza e Certificazione, che è subentrata nei compiti e attività della CACTRUPA.
CACTRUPA	L'infrastruttura organizzativa e tecnologica, realizzata nel 2001 dall'ex Centro Tecnico, per la certificazione e validazione temporale per i soggetti che utilizzano la Rete Unitaria della PA.
Centro Tecnico per la Rete Unitaria della Pubblica Amministrazione / Centro Tecnico	Unità organizzativa che svolgeva la funzione di Certificatore ai sensi del D.P.C.M. 8 febbraio 1999, poi incorporato nel CNIPA.

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

DEFINIZIONE	DESCRIZIONE
Certificatore	Il CNIPA, nella sua attività di certificazione, responsabile della generazione, dell'emissione, della conservazione, della revoca e della sospensione dei certificati. In questo Manuale si utilizza con la stessa accezione la denominazione "CACNIPA". Il CNIPA opera in facility management utilizzando beni e servizi messi a disposizione dal gestore dell'infrastruttura aggiudicatario di una specifica gara d'appalto.
Chiavi ausiliarie – certificato ausiliario	Coppia di chiavi crittografiche, con relativo certificato, fornite al Titolare con il dispositivo di firma, in aggiunta a quelle di firma digitale, per utilizzi diversi dalla sottoscrizione. Tali chiavi sono fuori dal dispositivo di firma, quindi importate in esso e una copia ne è memorizzata in un sistema sicuro ai fini di key recovery.
CNIPA	Il Centro nazionale per l'Informatica nella Pubblica Amministrazione, che opera presso la Presidenza del Consiglio dei Ministri, è stato istituito con l'articolo 176 del Decreto legislativo n. 196 del 30 giugno 2003, in sostituzione dell'Autorità per l'informatica nella Pubblica Amministrazione. A decorrere dal 1° gennaio 2004, a seguito dell'art. 5 del decreto legislativo 5 dicembre 2003, n. 343, il CNIPA è divenuto Titolare anche dei compiti, funzioni e attività esercitate dal Centro Tecnico, tra cui quella di certificazione.
Codice di sospensione (Codice di emergenza)	Un codice riservato, fornito dal CNIPA al Titolare, il quale lo utilizza per autenticarsi al "call center", ai fini della eventuale richiesta di sospensione del certificato.
CRL	Vedi: Lista di revoca dei certificati.
CSL	Vedi: Lista di sospensione dei certificati.
Dipartimento	Il Dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio dei Ministri o altro organismo di cui si avvale il Ministro per l'innovazione e le tecnologie.
Destinatario	Destinatario di un messaggio e/o di un'evidenza informatica firmati digitalmente.

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

DEFINIZIONE	DESCRIZIONE
Gestore di infrastruttura o Gestore	Gestore dell'infrastruttura aggiudicatario di una specifica gara d'appalto tra i certificatori accreditati.
Lista di revoca dei certificati (CRL)	La lista dei certificati revocati di cui all. art 21 del DPCM 13 gennaio 2004.
Lista di sospensione dei certificati (CSL)	La lista dei certificati sospesi di cui all. art 21 del DPCM 13 gennaio 2004.
Manuale operativo	Documento pubblico depositato presso il Dipartimento che definisce le procedure applicate dal Certificatore che rilascia certificati qualificati nello svolgimento della propria attività. Il presente documento.
PIN	Personal Identification Number. Codice riservato modificabile che il Titolare utilizza per attivare le funzioni di firma digitale del proprio dispositivo di firma.
PUK	PIN Unlock Key. Codice riservato che il Titolare utilizza per sbloccare il proprio dispositivo di firma in caso di raggiungimento del massimo numero di PIN errati o di smarrimento del PIN stesso.
PKI	Infrastruttura a Chiave Pubblica (Public Key Infrastructure).
Referente/Referente per la firma digitale/Referente dell'Amministrazione	La persona o l'insieme di persone delegate dall'Amministrazione alla gestione dei rapporti con il Certificatore, alla richiesta di registrazione degli appartenenti all'Amministrazione, nonché all'inoltro della richiesta di revoca o sospensione dei certificati.
Registrazione	Attività d'acquisizione, verifica e archiviazione dei dati dei richiedenti. La registrazione del richiedente costituisce condizione vincolante per l'accoglimento della domanda di certificazione.
Registro dei certificati	Registro contenente i certificati emessi dal Certificatore, la lista dei certificati revocati e la lista dei certificati sospesi, accessibili telematicamente.
Revoca del certificato	Operazione con cui il Certificatore annulla la validità del Certificato da un dato momento in poi.

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

DEFINIZIONE	DESCRIZIONE
Richiedente	Persona che richiede la certificazione delle proprie chiavi pubbliche. Una volta certificato diviene Titolare.
RUPA	Rete Unitaria della Pubblica Amministrazione.
Sospensione del certificato	Operazione con cui il Certificatore sospende la validità del certificato, da un dato momento, e per un determinato periodo di tempo.
Terzo interessato	Soggetto diverso dal Titolare che dispone della facoltà di revocare/sospendere il certificato a questi rilasciato. In questo caso il Referente dell'Amministrazione ne fa le veci.
Validità del certificato	Efficacia ed opponibilità al Titolare della chiave pubblica, dei dati contenuti nel certificato stesso.

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_Certificazione 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: n.ro allegati:	2.0 0

3 RIFERIMENTI NORMATIVI

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

RIFERIMENTO	DESCRIZIONE
[L5997A15]	art.15, comma 2, Legge 15 marzo 1997, n°59
[DPR44500]	DPR 28 dicembre 2000, n° 445 e successive modificazioni
[DPCM130104]	DPCM 13 gennaio 2004
[AIPACR27]	Circolare A.I.P.A. 16/02/2001 – n° AIPA/CR/27
[AIPACR24]	Circolare A.I.P.A. 19/06/2000 – n° AIPA/CR/24
[DLVO19603]	Decreto Legislativo 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”
[DM020704]	Decreto Ministeriale 2 luglio 2004

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

4 INTRODUZIONE

4.1 Premessa

Con l'art. 5 del decreto legislativo 5 dicembre 2003, n. 343, dal 1° gennaio 2004 il CNIPA, con una propria infrastruttura organizzativa e tecnologica, è subentrato al Centro Tecnico nelle attività di certificazione e validazione temporale per i soggetti che utilizzano la Rete Unitaria per la Pubblica Amministrazione (RUPA).

Il Certificatore Centro Tecnico per la RUPA (CACTRUPA), gestito dal CNIPA, continua ad assicurare i servizi relativi ai certificati da lui emessi, che rimangono validi, a meno di eventuali revoche o sospensioni, fino alla naturale scadenza.

Il Manuale Operativo definisce le procedure applicate dal Certificatore, che rilascia certificati qualificati, nello svolgimento della propria attività di certificazione ([DPCM130104], art.38, comma 1).

Il Manuale Operativo è rivolto a tutti i soggetti che entrano in relazione con il Certificatore:

- Titolare;
- Terzo interessato;
- Destinatario, ovvero quanti verificano la firma.

Questo Manuale Operativo si applica, relativamente ai servizi attivi, ad entrambe le infrastrutture di certificazione CACNIPA e CACTRUPA.

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

5 DATI IDENTIFICATIVI DEL CERTIFICATORE

I dati identificativi relativi al CNIPA sono i seguenti:

Denominazione e Ragione sociale	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
Rappresentante legale	Livio Zoffoli
Sede legale	Via Isonzo 21/b, 00198 Roma
Telefono	+39 06 852641
Fax	+39 06 85264414
Sede operativa	Via Isonzo 21/b, 00198 Roma
Indirizzo E-mail	certificazione@cnipa.it
Indirizzo Internet	http://www.cnipa.gov.it
Call Center	+39 06 54573101

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

6 MANUALE OPERATIVO

6.1 Dati identificativi del Manuale operativo

Il presente Manuale operativo è identificato attraverso il numero di versione 2.0.

Esso si riferisce ai servizi di:

- Certificazione chiavi pubbliche della Rete Unitaria della Pubblica Amministrazione;
- Generazione di marche temporali a richiesta per documenti elettronici.

Pertanto il presente Manuale Operativo è referenziato dai seguenti OID (Object Identifier Number):

- 1.3.76.16.1.2.1.1 – Certificazione Chiavi;
- 1.3.76.16.1.2.2.1. – Marcatura documenti a richiesta.

Il corrispondente file in formato elettronico, conservato presso i locali del Certificatore e depositato presso il Dipartimento, è identificabile dal nome “MO_CNIPA_v2.0” ed è consultabile per via telematica all’indirizzo Internet: <http://www.cnipa.gov.it/firmadigitale/manualeoperativo>.

6.2 Responsabile del Manuale operativo

Il Responsabile del Manuale operativo è:

Responsabile del Manuale operativo	
Nome	Gennaro
Cognome	Ragucci
Telefono	+39 06 852641
E-mail	ragucci@cnipa.it

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_Certificazione 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: n.ro allegati:	2.0 0

7 OBBLIGHI DEL CERTIFICATORE, DEL TITOLARE E DI QUANTI ACCEDONO PER LA VERIFICA DELLE FIRME

7.1 Obblighi del Certificatore

Nello svolgimento della sua attività il Certificatore ([DPR44500], art.29 - bis):

1. adotta tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
2. identifica con certezza la persona che effettua richiesta di certificazione;
3. rilascia e rende pubblico il certificato elettronico nei modi e nei casi stabiliti dalle regole tecniche di cui al [DPR44500], art. 8, comma 2, nel rispetto del [DLVO19603];
4. specifica, quando applicabile, nel certificato qualificato su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della sussistenza degli stessi;
5. si attiene alle regole tecniche di cui al [DPR44500], art. 8, comma 2;
6. informa 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;
7. adotta le misure di sicurezza per il trattamento dei dati personali, ai sensi del [DLVO19603];
8. non si rende depositario di dati per la creazione della firma del Titolare;
9. procede alla pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del Titolare o del terzo dal quale derivino i poteri di quest'ultimo, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del Titolare, di sospetti abusi o falsificazioni;
10. garantisce il funzionamento efficiente, puntuale e sicuro dei servizi di elencazione, nonché garantisce un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo;
11. assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

12. tiene la registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato per dieci anni in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
13. non copia, nè conserva le chiavi private di firma del soggetto cui il Certificatore ha fornito il servizio di certificazione;
14. predispone su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione, tra cui in particolare gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie; dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio ed il Certificatore;
15. utilizza sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal Titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato;
16. raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato, fornendo l'informativa prevista dalla disciplina in materia di dati personali. I dati non possono essere raccolti o elaborati per fini diversi senza l'esplicito consenso della persona cui si riferiscono.

Prima di emettere il certificato qualificato il Certificatore ([DPCM130104], art. 14):

17. si accerta dell'autenticità della richiesta;
18. verifica il possesso della chiave privata e il corretto funzionamento della coppia di chiavi;
19. il certificato qualificato è generato con un sistema conforme a quanto previsto dal [DPCM130104], art. 28;
20. l'emissione dei certificati qualificati è registrata nel giornale di controllo con la specificazione della data e dell'ora della generazione;
21. il momento della generazione dei certificati deve essere attestato tramite un riferimento temporale.

Inoltre in quanto Certificatore accreditato il Certificatore ([DPCM130104], art. 40):

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

22. genera un certificato qualificato per ciascuna delle chiavi di firma elettronica avanzata utilizzate dal dipartimento per la sottoscrizione dell'Elenco Pubblico dei certificatori e pubblicarlo nel proprio registro dei certificati;
23. garantisce l'interoperabilità del prodotto di verifica di cui al [DPCM130104], art. 10, ai documenti informatici sottoscritti con firma digitale emessa dalla struttura di certificazione della Rete unitaria della pubblica Amministrazione e successive modifiche tecniche e organizzative;
24. mantiene copia della lista, sottoscritta dal dipartimento, dei certificati relativi alle chiavi di certificazione di cui al [DPCM130104], art. 41, comma 1, lettera f, che è accessibile per via telematica;
25. al fine di ottenere e mantenere il riconoscimento di cui al [DPR44500], art. 28, comma 1, devono svolgere la propria attività in conformità con quanto previsto dalle regole per il riconoscimento e la verifica del documento elettronico.

Il Certificatore fornisce un sistema che consente di effettuare la verifica delle firme digitali.

7.2 Obblighi del Titolare

Il Titolare è tenuto a adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri ([DPR44500], art. 29 - bis, comma 1). Il Titolare della chiave deve inoltre:

1. fornire tutte le informazioni richieste dal Certificatore garantendone, sotto la propria responsabilità, l'attendibilità ai sensi della legge n.15 del 1968 e successive modifiche ed integrazioni;
2. comunicare al Certificatore ogni variazione delle informazioni fornite in fase di registrazione;
3. prendere visione di questo Manuale Operativo prima di inoltrare la richiesta di certificazione;
4. nel caso di fornitura del solo certificato:
 - generare una coppia di chiavi all'interno del dispositivo di firma ([DPCM130104], art.6, comma 3);
 - generare la coppia di chiavi mediante apparati e procedure che assicurino, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e la robustezza della coppia generata, nonché la segretezza della chiave privata ([DPCM130104], art.5, comma 1);

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

5. conservare con la massima diligenza la chiave privata o il dispositivo che la contiene al fine di garantirne l'integrità e la massima riservatezza ([DPCM130104], art. 7, comma 3);
6. conservare le informazioni di abilitazione all'uso della chiave privata separatamente dal dispositivo contenente la chiave ([DPCM130104], art. 7, comma 3);
7. richiedere immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi di firma difettosi o di cui abbia perduto il possesso ([DPCM130104], art. 7, comma 3);
8. sporgere denuncia, in caso di smarrimento o sottrazione del dispositivo di firma, alle Autorità competenti;
9. a seguito di sospensione del certificato, risolta la relativa causa, deve presentarsi presso il proprio Referente e richiedere per iscritto la revoca o la riattivazione dello stesso;
10. custodire con la massima diligenza i codici riservati ricevuti dal Certificatore al fine di preservarne la riservatezza.

E' vietata la duplicazione della chiave privata di firma e dei dispositivi che la contengono ([DPCM130104], art.7, comma 1).

Non è consentito l'uso di una chiave per funzioni diverse da quelle previste dalla sua tipologia ([DPCM130104], art. 4, comma 5).

Il Titolare è tenuto ad utilizzare esclusivamente il dispositivo fornito dal Certificatore, ovvero un dispositivo scelto tra quelli indicati dal Certificatore stesso ([DPCM130104], art. 6, comma 5).

7.3 Obblighi dei destinatari

I destinatari dei messaggi elettronici e/o delle evidenze informatiche firmate digitalmente da Titolare della CACTRUPA e CACNIPA devono verificare:

1. che il certificato contenente la chiave pubblica del Titolare firmatario del messaggio e/o evidenza informatica non sia temporalmente scaduto;
2. che il certificato del Titolare sia stato firmato con le chiavi di certificazione della CACNIPA o CACTRUPA presenti nell'Elenco Pubblico mantenuto dal Dipartimento;
3. l'assenza del certificato dalle Liste di Revoca (CRL) e dalle Liste di Sospensione (CSL) dei certificati;
4. l'esistenza di eventuali limitazioni all'uso del certificato utilizzato dal Titolare;
5. che la tipologia di uso della chiave del certificato sia "Non Ripudio".

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_Certificazione 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: n.ro allegati:	2.0 0

7.4 Obblighi del terzo interessato

Il terzo interessato, sia esso persona fisica o Amministrazione, ha l'obbligo di richiedere la revoca dei certificati ogni qualvolta vengano meno i requisiti in base ai quali il certificato è stato rilasciato, previa sua autorizzazione, al Titolare. Egli agisce per mezzo dei referenti delle amministrazioni.

La richiesta di revoca o sospensione da parte del terzo interessato di cui al [DPR44500], art.29 – septies, comma 1, lett.c, deve essere inoltrata munita di sottoscrizione e corredata di documentazione giustificativa e della data di decorrenza (revoca) o della durata (sospensione) ([DPCM130104], art.20, comma 1 e art. 24, comma 1).

L'Amministrazione, nel caso la fornitura si riferisca unicamente alla produzione del certificato (senza dispositivo di firma), deve assicurare la rispondenza del dispositivo di firma, del sistema di generazione delle chiavi e dell'ambiente operativo ai requisiti di Legge. Tale assicurazione deve essere espressa tramite dichiarazione resa al Certificatore al momento della Registrazione dei richiedenti.

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_Certificazione 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: n.ro allegati:	2.0 0

8 RESPONSABILITÀ

8.1 Responsabilità del Certificatore

Il Certificatore è responsabile verso i titolari, per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività previste dal [DPR44500], dal [DPCM130104], dalla [AIPACR27], dal [DLVO19603] e successive modificazioni e integrazioni (Vedi paragrafo 7.1, "Obblighi del Certificatore").

Il Certificatore non assume responsabilità:

- per l'uso improprio dei certificati;
- pur garantendo l'interoperabilità dei propri certificati ai sensi della circolare [AIPACR24], per le tematiche afferenti il loro utilizzo in dispositivi di firma non consegnati dal Certificatore.

8.2 Limitazione agli indennizzi

Non applicabile.

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_Certificazione 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: n.ro allegati:	2.0 0

9 TARIFFE

Il CNIPA fornisce i servizi di certificazione ai soggetti che utilizzano la RUPA. in base alle condizioni corrispondenti alla aggiudicazione della procedura concorsuale per la realizzazione e gestione di una infrastruttura a chiave pubblica per la Rete Unitaria della Pubblica Amministrazione.

Le tariffe sono pubblicate sul sito del CNIPA all'indirizzo <http://www.cnipa.gov.it>.

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

10 PROCEDURE OPERATIVE

10.1 Organizzazione del Certificatore

Il personale preposto alla erogazione e controllo del servizio di certificazione prevede le seguenti figure organizzative:

- Responsabile della Registrazione;
- Responsabile della Certificazione;
- Responsabile della Sicurezza;
- Responsabile dell'Auditing;
- Responsabile dei Servizi Tecnici.

Le figure sopraelencate per lo svolgimento delle funzioni di loro competenza si avvalgono di addetti e operatori e delle corrispondenti figure presso il gestore di infrastruttura. In particolare ci si avvale dei referenti presso le amministrazioni aderenti al servizio.

10.1.1 Attivazione dei referenti delle amministrazioni

Il rilascio dei certificati ad appartenenti ad amministrazioni è oggetto di accordo tra queste ed il CNIPA.

Nell'ambito dell'accordo l'Amministrazione delega, con lettera ufficiale al Certificatore, uno o più soggetti alla gestione dei rapporti con il Certificatore. Tali figure vengono denominati "Referenti".

I referenti, considerati come parte integrante dell'infrastruttura del Certificatore, dovranno recarsi presso il Certificatore per l'identificazione e per seguire un corso di formazione specifico.

Nell'ambito del corso di formazione i referenti vengono certificati e apprendono le procedure operative per:

- Identificare i dipendenti a favore dei quali l'Amministrazione richiede l'emissione del certificato di firma;
- comunicare al CNIPA i dati di detti dipendenti;
- inoltrare la richiesta di revoca o sospensione dei certificati emessi a favore degli appartenenti all'Amministrazione.

L'Amministrazione, per mezzo del Referente, si assume l'obbligo di comunicare al Certificatore tutte le variazioni e di richiedere la revoca (o sospensione) dei certificati emessi a favore dei suoi appartenenti, ogniqualvolta vengano meno i requisiti in base ai quali il certificato è stato rilasciato.

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

10.2 Modalità di identificazione e registrazione degli utenti

La registrazione degli utenti delle amministrazioni avviene secondo i seguenti passi operativi:

- Identificazione del richiedente;
- Compilazione e trasmissione della domanda di certificazione;
- Controllo e verifica dei dati;
- Produzione di ordini di lavoro per il gestore.

Responsabile del processo è il Responsabile della Registrazione. Collaborano i referenti delle amministrazioni e gli operatori CNIPA.

10.2.1 Identificazione

Il Certificatore è responsabile dell'identificazione del richiedente il certificato.

Il Certificatore con l'eventuale ausilio dei referenti, effettua l'identificazione degli utenti da certificare.

L'identificazione del richiedente avviene attraverso l'esibizione di uno dei documenti di riconoscimento definiti al [DPR44500], art. 35. In queste sono incluse le tessere di riconoscimento delle amministrazioni munite di fotografia e dati anagrafici:

10.2.2 Compilazione e trasmissione della domanda di certificazione

Dopo essere stato identificato, il richiedente compila un apposito modulo per la richiesta di certificazione fornito dal Certificatore unitamente all'informativa di cui al [DLVO19603], art. 13.

Con la firma su detto modulo il richiedente:

- fornisce i propri dati anagrafici e alcuni dati lavorativi presso l'Amministrazione di appartenenza, in particolare un indirizzo valido di posta elettronica che verrà utilizzato dal Certificatore per comunicare con il richiedente;
- si assume esplicitamente gli obblighi di cui al paragrafo 7.2 "Obblighi del Titolare";
- acconsente alla pubblicazione del certificato nel Registro dei certificati.

Qualora il certificato venga richiesto da un soggetto in quanto rappresentante di una persona fisica/giuridica previo consenso della stessa ("terzo interessato"), ai suddetti documenti deve aggiungersi:

- delega o procura attestante la sussistenza dei poteri di rappresentanza.

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

Qualora il richiedente il certificato desideri citare nello stesso la sussistenza di eventuali ruoli ricoperti, in assenza di accordi tra il Certificatore e le eventuali organizzazioni d'appartenenza l'emissione sarà vincolata alla presentazione dei documenti di cui sopra ed, in aggiunta, alla:

- documentazione comprovante il possesso della qualifica dichiarata.

Salvo i casi in cui la domanda sia raccolta direttamente dal Certificatore, il Referente effettua un primo controllo di completezza e correttezza dei dati forniti dal richiedente e raccoglie una copia fotostatica del documento di identità e del tesserino del codice fiscale. In caso di mancanza di quest'ultimo il dato imputato sulla domanda ha il valore di dichiarazione sostitutiva.

Nei casi in cui la richiesta si riferisce al solo certificato il Referente deve allegare anche:

- la richiesta di certificazione in formato PKCS#10;
- la dichiarazione che il sistema di generazione delle chiavi, il dispositivo di firma e l'ambiente operativo sono conformi ai requisiti di Legge.

Il Referente sulla base di quanto concordato con il Certificatore invia al CNIPA la domanda controfirmata con modalità sicure.

10.2.3 Controllo e verifica dei dati

Il Referente trasmette, con modalità sicure, le domande di certificazione in formato elettronico, concordato di volta in volta con il CNIPA, al Responsabile della Registrazione.

I dati in formato elettronico vengono importati nel database detto di pre-registrazione presso la struttura del CNIPA.

Attraverso un canale tradizionale (es. tramite corriere), il Referente trasmette le domande in formato cartaceo, firmate in modo autografo dai richiedenti, e i relativi allegati.

Il Certificatore effettua una serie di verifiche di completezza, correttezza e corrispondenza dei dati ricevuti ed in particolare si accerta che il codice fiscale sia valido ed attribuito alla persona cui si riferiscono i dati anagrafi, mediante una validazione sulla base di dati forniti dall'Agenzia delle Entrate.

10.2.4 Produzione di ordini di lavoro per il gestore

Alle domande che superano tutti i suddetti controlli viene attribuito un codice identificativo unico e un codice di sospensione (codice di emergenza) che il Titolare dovrà utilizzare per autenticare la richiesta di sospensione immediata attraverso "call center" in caso di furto o smarrimento del dispositivo di firma.

Alla domanda viene attribuito un codice di lavorazione e viene inoltrata al gestore sotto forma di ordinativo di lavoro. La domanda viene trasmessa, solo in formato elettronico, firmata digitalmente, con modalità sicure dal CNIPA al gestore.

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

Una volta emesso l'ordinativo di lavoro, la domanda di certificazione viene archiviata per 10 anni.

10.2.4.1 Codice identificativo univoco (Codice Univoco)

Il codice identificativo, facente parte del Common Name (come previsto dalla Circolare [AIPACR24]), è strutturato secondo il seguente schema XYNNNNNNNN:

Sottocodice	Descrizione del sottocodice	Valori possibili
X	Tipologia di utenza	2=Referente
		3=Titolare
Y	Caratteristica del certificato	T=certificato di Test
		S=certificato di servizio
		0-9=certificato ordinario
NNNNNNNN	Numero progressivo	< 00100000 = certificato emesso dal Centro Tecnico per la Rupa
		> 00100000 = certificato emesso dal CNIPA

10.3 Modalità di generazione delle chiavi per la creazione e la verifica della firma ed emissione dei certificati

In considerazione della esigenza di generare un numero consistente di certificati e della difficoltà logistica di provvedere alla generazione delle chiavi da parte dei richiedenti, il CNIPA adotta una modalità di certificazione definita "Centralizzata".

Il Certificatore con strumenti automatici provvede alla generazione delle chiavi e al Titolare perviene un dispositivo di firma pronto all'uso.

I dati validati dal CNIPA e trasmessi al gestore, vengono caricati nel database di pre-registrazione del sistema per la produzione dei certificati e per la personalizzazione dei dispositivi di firma.

Il sistema:

- associa un dispositivo di firma parzialmente personalizzato ai dati del richiedente;
- genera le coppie di chiavi di firma e ausiliarie;
- provvede alla generazione, emissione e eventuale pubblicazione del certificato;

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

- all'emissione del certificato associa un riferimento temporale che viene annotato nel Registro operativo; la precisione del riferimento è assicurata dall'utilizzo del medesimo sistema di misura del tempo di cui al paragrafo 10.14;
- all'eventuale pubblicazione del certificato associa una marca temporale la cui emissione viene annotata nel Registro operativo;
- invia al Titolare una e-mail contenente il certificato prodotto;
- termina la personalizzazione del dispositivo di firma con l'importazione dei certificati dell'utente;
- si interfaccia ai sistemi di distribuzione per la consegna del dispositivo di firma e dei relativi codici di attivazione PIN e PUK e del codice di sospensione.

Nel caso di produzione dei soli certificati:

Il sistema:

- provvede alla generazione, emissione e eventuale pubblicazione del certificato;
- all'emissione del certificato associa un riferimento temporale che viene annotato nel Registro operativo; la precisione del riferimento è assicurata dall'utilizzo del medesimo sistema di misura del tempo di cui al paragrafo 10.14;
- all'eventuale pubblicazione del certificato associa una marca temporale la cui emissione viene annotata nel Registro operativo;
- invia una e-mail al Titolare contenente il certificato generato.

10.3.1 Sistemi di generazione

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

Il sistema di generazione delle chiavi assicura:

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

La generazione delle chiavi avviene all'interno del dispositivo di firma.

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

La lunghezza delle chiavi di sottoscrizione e ausiliaria è 1024 bit.

10.3.2 Dispositivo sicuro di firma

Con riferimento al [DPCM130104], artt. 6 e 9, il dispositivo sicuro di firma utilizzato per la generazione delle firme è conforme almeno ai requisiti di sicurezza imposti dai criteri previsti dal livello di valutazione E3 e robustezza dei meccanismi HIGH dell'ITSEC.

Le chiavi private sono conservate e custodite all'interno del dispositivo di firma, ed è possibile utilizzare lo stesso dispositivo per conservare più chiavi.

Una coppia di chiavi è attribuita ad un solo Titolare ([DPCM130104], art.4, comma 1).

10.3.3 Personalizzazione del dispositivo di firma

Prima della generazione della coppia di chiavi da parte del richiedente, l'operatore procede alla personalizzazione del dispositivo di firma.

Attraverso il processo di personalizzazione del dispositivo di firma, si svolgono le seguenti operazioni:

- acquisizione dei dati identificativi del dispositivo di firma utilizzato, e loro associazione al Titolare. Detta associazione viene annotata nel Giornale di controllo;
- registrazione, nel dispositivo di firma, dei dati identificativi del Titolare presso il Certificatore;
- registrazione, nel dispositivo di firma, dei certificati relativi alle chiavi di certificazione del Certificatore.

Durante quest'operazione, l'operatore verifica il corretto funzionamento del dispositivo di firma.

10.4 Modalità con cui si individua un certificato qualificato

I certificati qualificati vengono individuati tramite il loro codice univoco.

Con riferimento alla tabella di cui al paragrafo 10.2.4.1 i certificati per i quali X=3 (certificato del Titolare) e Y=0-9 (certificato ordinario), sono certificati qualificati.

10.4.1 Limitazioni d'uso

- I certificati con X=2 (Certificato del Referente) possono essere utilizzati dai Referenti esclusivamente per la regolazione del ciclo di vita dei certificati e per comunicazioni sicure con il CNIPA;

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

- I certificati con Y=T (Certificato di Test) possono essere utilizzati dalle amministrazioni esclusivamente per attività di sperimentazione nello sviluppo di applicazioni di firma digitale nei processi amministrativi;
- I certificati con Y=S (Certificato di Servizio), o privi del codice univoco, vengono utilizzati esclusivamente dal Certificatore per scopi di funzionamento dell'infrastruttura.

10.5 Revoca e Sospensione dei Certificati dei titolari

Allo stato delle tecnologie attuali, non esistono standard in grado di descrivere il formato delle Liste dei certificati sospesi, o di operare una distinzione tra queste e quelle dei certificati revocati.

Il Certificatore, al fine di soddisfare il dettato normativo che prevede la creazione di Liste di sospensione (CSL) dei certificati, utilizza sia per la revoca sia per la sospensione un'unica lista (la Lista dei certificati revocati- CRL).

Nell'unica lista sono quindi mantenuti sia i certificati revocati che i certificati sospesi. Questi ultimi si differenzieranno nella motivazione della revoca "sospensione".

Il Certificatore provvede a rimuovere dalla lista i certificati che non sono più sospesi.

Sarà cura del Certificatore mantenere traccia del periodo di sospensione.

La revoca di un certificato determina la cessazione anticipata della sua validità. La sospensione di un certificato provoca invece un'interruzione della sua validità per un periodo di tempo determinato.

La revoca e la sospensione sono registrate nel Giornale di controllo ([DPCM130104], art. 17, comma 3 e art. 21, comma 2), e sono efficaci a partire dal momento della pubblicazione della lista che le contiene. Il momento di pubblicazione della lista è asseverato mediante l'apposizione di una marca temporale.

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

Il certificato può essere revocato o sospeso su iniziativa del ([DPCM130104], artt.18-19-20-22-23-24):

- Certificatore;
- Titolare;
- Terzo interessato.

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

10.5.1 Motivi per la revoca dei certificati dei titolari

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

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

- Perdita del possesso del dispositivo di firma (smarrimento, furto);
- Guasto o cattivo funzionamento del dispositivo di firma¹;
- Compromissione della segretezza della chiave privata;
- Fine del rapporto di lavoro con la Pubblica Amministrazione o altre cause analoghe (per esempio la perdita del potere di firma).

In caso di smarrimento o sottrazione del dispositivo di firma, il Titolare deve richiedere la sospensione immediata del certificato, chiamando il "call center" del Certificatore, e sporgere denuncia alle Autorità competenti. Confermato il caso di furto o smarrimento deve inoltrare richiesta di revoca al Certificatore allegando copia della relativa denuncia.

Il Titolare ha facoltà di richiedere la revoca di un certificato per un qualunque motivo dallo stesso ritenuto valido ed in qualsiasi momento.

Il terzo interessato (nello scenario in esame il Referente per conto dell'Amministrazione) ha l'onere di richiedere la revoca dei certificati ogniqualvolta vengano meno i requisiti in base ai quali questi ultimi sono stati rilasciati al Titolare (esempio dimissioni o pensionamento del Titolare dalla Amministrazione di appartenenza).

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

La richiesta di revoca deve essere presentata 2 (due) giorni feriali in anticipo rispetto alla data di entrata in vigore.

¹ Nel caso di revoca per malfunzionamento della smart card il Titolare può richiedere, attraverso una richiesta scritta al Referente, una nuova smart card. Il Referente inoltra al responsabile della Registrazione una richiesta sottoscritta di remissione con conferma dei dati precedentemente inviati.

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

10.5.2 Motivi per la sospensione dei certificati dei titolari

Il Certificatore sospende i certificati ogniqualvolta, ricevuta una richiesta di revoca su iniziativa del Titolare, non ha la possibilità di accertare in tempo utile l'autenticità della richiesta stessa.

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

Il Titolare ed il Referente (per il terzo interessato) possono richiedere la sospensione dei certificati per un determinato periodo di tempo, e sono tenuti a presentare la domanda di sospensione almeno 2 (due) giorni feriali prima dell'inizio del periodo desiderato. Alla fine del periodo di sospensione i certificati sono automaticamente riattivati, a meno di una revoca, e viene inviata all'utente, via posta elettronica, la notifica dell'avvenuta riattivazione.

Il Titolare nei casi di furto e smarrimento deve richiedere la sospensione telefonica immediata, che innesca l'immediata sospensione dei certificati.

10.5.3 Motivi per la revoca di certificati relativi a chiavi di certificazione

Il Certificatore procede alla revoca del certificato relativo ad una coppia di chiavi di certificazione solo in caso di ([DPCM130104], art.26):

- Compromissione della chiave segreta;
- Guasto del dispositivo di firma;
- Cessazione dell'attività.

10.5.4 Motivi per la revoca di certificati relativi a chiavi di marcatura temporale

Il Certificatore procede alla revoca del certificato relativo ad una coppia di chiavi di marcatura temporale solo in caso di:

- Compromissione della chiave segreta;
- Guasto del dispositivo di firma.

10.5.5 Modalità di revoca o sospensione

Esistono per la revoca e sospensione due modalità:

- Richiesta tramite servizi on-line;

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

- Richiesta scritta (con firma autografa o firma digitale).

Per la sospensione, unicamente nei casi di emergenza (es. furto o smarrimento), esiste anche la modalità telefonica tramite “call center” del Certificatore.

10.5.5.1 Richiesta tramite i servizi on-line

Il Certificatore rende disponibile come primaria modalità di richiesta di revoca e sospensione un apposito servizio on-line accessibile dal sito www.cnipa.gov.it

La procedura prevede l’inserimento:

- dei dati identificativi del soggetto della revoca o sospensione
- della motivazione della revoca;
- della data di inizio della revoca o del periodo di sospensione.

La richiesta viene firmata digitalmente dal richiedente prima dell’inoltro al sistema del Certificatore.

Il sistema verifica l’autenticità della firma, il diritto del richiedente alla richiesta, e in caso positivi processa la richiesta inserendo i certificati nelle liste di revoca e sospensione (CRL) a partire dalla data di inizio indicata.

10.5.5.2 Richiesta scritta

La presente modalità è utilizzata dal Referente per i certificati dei titolari o direttamente dal Titolare.

La richiesta di revoca o sospensione è inoltrata al Certificatore per mezzo di un apposito modulo sottoscritto. La revoca o la sospensione avverrà entro due giorni lavorativi dalla ricezione.

Tale modalità è da utilizzare nei casi in cui il Titolare sia impossibilitato ad utilizzare i servizi on-line.

Il Titolare o il Referente deve compilare un modulo di richiesta indicando:

- nome e cognome del richiedente;
- nome e cognome del Titolare oggetto di revoca o sospensione;
- Common Name del Titolare oggetto di revoca o sospensione;
- dati identificativi del/i certificato/i oggetto di revoca o sospensione;
- motivazione e data di decorrenza desiderata della revoca o periodo di sospensione;
- eventuale allegato di denuncia di furto/smarrimento.

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

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

Il Certificatore, ricevuta la richiesta, provvede alla revoca o alla sospensione del certificato, al suo inserimento nell'apposita Lista dei certificati revocati e sospesi (CRL), ed alla pubblicazione della lista nel Registro dei certificati.

10.5.5.3 Call Center

Il Titolare unicamente nei casi di emergenza (es. furto o smarrimento) può avvalersi del servizio di sospensione immediata tramite telefonata al "call center" del Certificatore.

Il Titolare deve fornire il codice di sospensione (codice di emergenza) attribuitogli dal Certificatore e il proprio Distinguished Name.

La telefonata viene ricevuta da un operatore addetto che provvede all'immediata sospensione del certificato attraverso, il suo inserimento nelle Liste dei certificati sospesi (CSL) ed alla pubblicazione della lista nel Registro dei certificati.

La richiesta di sospensione così inoltrata, deve poi essere confermata attraverso una richiesta sottoscritta di revoca o di riattivazione del certificato presentata al Referente che provvede ad inoltrarla al Certificatore. In caso di accertato furto o smarrimento il Titolare deve consegnare anche copia della relativa denuncia presentata alle Autorità competenti.

Qualora il Titolare (o il Referente adeguatamente delegato) ometta la trasmissione al Certificatore della documentazione scritta, il certificato rimane sospeso fino alla naturale scadenza dello stesso.

10.5.5.4 Disponibilità dei servizi di revoca o sospensione

Il Certificatore garantisce, per ogni modalità di inoltro delle richieste di revoca o sospensione, una diversa disponibilità del servizio ad esse connesse:

- Per le richieste di revoca o sospensione inoltrate tramite servizi on-line il servizio è attivo in modo continuativo per 24 ore tutti i giorni festivi inclusi;
- in caso di richiesta di revoca o sospensione sottoscritta il servizio è disponibile negli orari di ufficio;
- per le richieste di sospensione immediata inoltrate telefonicamente il servizio sarà disponibile dal Lunedì al Venerdì dalle ore 08.00 alle ore 21.00 e il Sabato dalle ore 08.00 alle ore 15.00.

10.5.5.5 Aggiornamento delle CRL e delle CSL

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

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

La pubblicazione nel Registro dei certificati avviene comunque al massimo ogni 24 (ventiquattro) ore.

10.5.6 Modalità di revoca o sospensione dei certificati su iniziativa del Certificatore

Salvo i casi di motivata urgenza, qualora il Certificatore intenda sospendere o revocare un certificato ne darà preventiva comunicazione al Titolare specificandone i motivi.

10.5.7 Riattivazione di un certificato sospeso

Il certificato sospeso, inserito nella Lista dei certificati sospesi e pubblicato nel Registro dei certificati, acquista nuovamente validità:

- alla scadenza del periodo di sospensione, quindi automaticamente;
- con una richiesta sottoscritta di riattivazione.

10.5.7.1 Modalità di riattivazione a richiesta

Il Titolare presenta richiesta scritta al Referente motivando la necessità di riattivazione.

Il Referente trasmette al CNIPA apposito modulo da lui sottoscritto che riporta i dati identificativi del Titolare e del certificato, le motivazioni e la data desiderata di riattivazione. La riattivazione ha luogo entro 2 (due) giorni lavorativi dalla data di ricezione della richiesta.

Il Certificatore procede alla riattivazione del certificato attraverso la cancellazione dello stesso dalla Lista dei certificati sospesi (CSL).

10.6 Revoca dei certificati relativi a chiavi di certificazione

Il Certificatore procede alla revoca del certificato relativo ad una coppia di chiavi di certificazione esclusivamente nei seguenti casi ([DPCM130104], art.26, comma 1):

- compromissione della chiave segreta;
- guasto del dispositivo di firma;
- cessazione dell'attività.

La revoca è notificata al Dipartimento ed a tutti i possessori di certificati qualificati sottoscritti con la chiave segreta appartenente alla coppia revocata, entro le 24 ore ([DPCM130104], art.26, comma 2). Inoltre tutti i certificati qualificati sottoscritti con la chiave segreta appartenente alla coppia revocata vengono revocati.

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_Certificazione 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: n.ro allegati:	2.0 0

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

Della revoca è fatta annotazione nel Giornale di controllo.

10.7 Revoca dei certificati relativi a chiavi di marcatura temporale

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

- compromissione della chiave segreta;
- guasto del dispositivo di firma.

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

Della revoca è fatta annotazione nel Giornale di controllo.

10.8 Modalità di rinnovo delle chiavi di firma del Titolare

I certificati di firma hanno una validità massima di tre anni.

Tale validità vincola e limita l'utilizzo dei certificati, e delle relative chiavi, da parte del Titolare che, una volta scaduti, dovrà chiederne la sostituzione al Certificatore.

La sostituzione dei certificati del Titolare consiste nella generazione:

- di una nuova coppia di chiavi di firma;
- di una nuova coppia di chiavi per usi ausiliari;
- dei certificati relativi alle chiavi pubbliche della nuove coppie generate.

La prima sostituzione può essere effettuata per via telematica direttamente dal Titolare.

Il processo di rinnovo dei certificati relativi alle chiavi pubbliche del Titolare può essere descritto nel modo seguente:

1. L'utente viene avvertito via posta elettronica prima della scadenza.
2. Il Titolare in accordo con la propria Amministrazione inizia il processo di rinnovo, con gli strumenti messi a sua disposizione dal Certificatore, generando la nuova coppia di chiavi di firma e la richiesta di certificazione, in formato PKCS#10.

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

3. Il Titolare, con gli strumenti messi a sua disposizione dal Certificatore, genera anche una coppia di chiavi per usi ausiliari e la relativa richiesta di certificazione in formato PKCS#10.
4. Il Titolare tramite i servizi on-line invia al Certificatore in modalità sicura le richieste di certificazione PKCS#10 e copia della chiave privata della coppia per usi ausiliari ai fini dell'archiviazione per il key recovery.
5. Il Certificatore verificata l'autenticità della richiesta provvede alla generazione dei relativi certificati, ad inviarli via posta elettronica al Titolare ed eventualmente a pubblicarli nel Registro dei certificati.
6. Il Titolare, con gli strumenti messi a sua disposizione dal Certificatore, importa i certificati nella propria smart card.

Detta procedura può essere seguita solo la prima volta e in assenza di variazioni dei dati presenti nel certificato.

Negli altri casi il processo di rinnovo è equivalente alla prima registrazione.

10.9 Sostituzione delle chiavi di certificazione

Il Certificatore, 90 (novanta) giorni prima della scadenza del certificato relativo ad una chiave di certificazione avvia la procedura di sostituzione, generando una nuova coppia di chiavi.

In aggiunta al certificato (self-signed) relativo alla nuova coppia di chiavi di certificazione di cui sopra, il Certificatore genera:

- un certificato, relativo alla nuova chiave pubblica sottoscritto con la chiave privata della vecchia coppia;
- un certificato relativo alla vecchia chiave pubblica sottoscritto con la nuova chiave privata.

I certificati così generati sono forniti al Dipartimento che provvede all'aggiornamento della lista dei certificati delle chiavi di certificazione contenuta nell'Elenco Pubblico dei certificatori.

10.10 Sostituzione delle chiavi di marcatura temporale

La sostituzione delle chiavi di marcatura temporale per l'emissione dei certificati e per i documenti informatici avviene mensilmente ([DPCM130104], art. 46, comma 2).

10.11 Procedura di recupero delle chiavi private per scopi ausiliari

Il recupero delle chiavi private per scopi ausiliari è un servizio reso disponibile ai seguenti soggetti:

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_Certificazione 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: n.ro allegati:	2.0 0

- Titolare;
- Delegato del Titolare;
- Amministrazione di appartenenza del Titolare (Referente, persona che ha assunto le funzioni del Titolare o altro rappresentante autorizzato);
- Magistratura.

Le motivazioni accettate dal Certificatore sono:

- Per il Titolare: malfunzionamento e/o indisponibilità del dispositivo di firma;
- Per il Delegato del Titolare: in caso di urgenza e impossibilità di attivare dal parte del Titolare la decifratura dei documenti;
- Per l'Amministrazione: indisponibilità del Titolare e del dispositivo di firma;
- Per la Magistratura: per esigenze relative ad indagini in corso.

La richiesta deve essere inoltrata per iscritto al CNIPA.

Il Certificatore verifica le motivazioni e procede ad attivare il recupero della chiave privata di cifra. La chiave viene resa disponibile al richiedente in modalità sicura.

10.12 Modalità di gestione del registro dei certificati

Il Certificatore pubblica le seguenti informazioni nel Registro dei certificati ([DPCM130104], art.29):

1. i certificati di certificazione;
2. i certificati di marcatura temporale;
3. i certificati di accordi di certificazione;
4. i certificati di firma dell'Elenco Pubblico dei certificatori;
5. i certificati di servizio e di test;
6. lista dei certificati revocati (CRL);
7. lista dei certificati sospesi (CSL).

La generazione di ogni nuovo elemento di cui all'elenco su indicato provoca l'aggiornamento del Registro.

Il Registro dei certificati è un Internet Directory Server compatibile con le specifiche ITU-T X.500 1993 che supporta LDAP v.3.

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

Il Registro dei certificati è pubblicamente consultabile 24 ore al giorno, 7 giorni la settimana, salvo manutenzione programmata, all'indirizzo ldapca.cnipa.gov.it sulla porta standard 389 con base di ricerca C=IT.

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

La data e l'ora di inizio e fine di ogni intervallo di tempo nel quale il Registro dei certificati non risulta accessibile dall'esterno, nonché quelle relative a ogni intervallo di tempo nel quale una sua funzionalità interna non risulta disponibile sono annotate sul Giornale di controllo.

Una copia di sicurezza della copia operativa e di quella di riferimento del Registro dei certificati sono conservate in armadi di sicurezza distinti, situati in locali diversi.

10.13 Modalità di protezione della riservatezza

Tutti i dati che risiedono su database sono protetti da prodotti che implementano politiche di autorizzazione per l'accesso ai dati legati a meccanismi di autenticazione degli utenti.

Le misure di protezione adottate sono conformi alle misure minime di sicurezza per il trattamento dei dati personali emanate con il [DLVO19603] e il [DPR44500] nell'esecuzione delle seguenti attività:

- individuazione degli incaricati;
- assegnazione di codici identificativi;
- protezione degli elaboratori;
- modalità di designazione degli incaricati del trattamento.

10.14 Modalità per l'apposizione e la definizione del riferimento temporale

Il servizio di emissione di marche temporali associate a documenti informatici è disponibile solo agli utenti in possesso di Certificato per chiavi di Firma Digitale emesso dal Centro Tecnico e dal CNIPA precedentemente abilitati ad accedere a tale servizio.

1. Il Titolare, tramite lo strumento fornito dal CNIPA, produce e firma digitalmente la richiesta di marcatura temporale del documento informatico²;
2. La richiesta viene trasmessa in modalità sicura al sistema del Certificatore;

² La firma si applica all'impronta del documento informatico. Pertanto il documento informatico NON viene trasmesso al Certificatore

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

3. Il sistema del Certificatore verifica l'autenticità della richiesta e l'abilitazione del Titolare;
4. Il sistema genera la marca temporale, conformemente al [DPCM130104], art 45 e 48, garantendo un tempo di risposta non superiore al minuto primo ([DPCM130104], art. 51, comma 5). Detta marca viene registrata in apposito archivio digitale non modificabile per un periodo di cinque anni ([DPCM130104], art. 50). L'emissione viene annotata nel Registro operativo ([DPCM130104], art. 49);
5. La marca temporale viene restituita in modalità sicura allo strumento del Titolare per l'utilizzo successivo.

Lo stesso strumento consente anche la verifica delle marche temporali generate dal sistema di marcatura temporale del Certificatore.

10.14.1 Chiavi di marcatura temporale

Le chiavi di marcatura temporale sono destinate alla generazione e verifica delle marche temporali ([DPCM130104], art.4, comma 4, lett.c).

La marca temporale è un'evidenza informatica sottoposta a firma, contenente una serie di indicazioni ([DPCM130104], art. 45, comma 1):

- identificativo dell'emittente;
- numero di serie della marca temporale;
- algoritmo di sottoscrizione della marca temporale;
- identificativo del certificato relativo alla chiave di verifica della marca;
- data ed ora di generazione della marca;
- identificatore dell'algoritmo di hash (SHA-1) utilizzato per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale;
- valore dell'impronta dell'evidenza informatica.

Ogni coppia di chiavi utilizzata per la validazione temporale è univocamente associata ad un sistema di validazione temporale ([DPCM130104], art. 46, comma 1).

10.15 Modalità operative per l'utilizzo del sistema di verifica delle firme

Il Certificatore indica sul sito www.cnipa.gov.it almeno un sistema che consenta di effettuare la verifica delle firme digitali.

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

La corretta verifica della firma richiede che l'utente utilizzi il sistema con una connessione attiva ad Internet e preventivamente proceda all'aggiornamento dei certificati dell'Elenco Pubblico dei certificatori. Il sistema sarà così in grado di effettuare, oltre che ai controlli di integrità della firma (nessuna modifica del documento elettronico firmato) e validità temporale del certificato del firmatario, anche la sua credibilità (certificato del firmatario rilasciato da uno dei certificatori accreditati). L'utente dovrà inoltre accertarsi che il certificato del firmatario non sia stato revocato o sospeso attraverso l'aggiornamento delle relative CRL.

Un'ulteriore verifica che l'utente deve effettuare è il controllo della conformità con il contenuto del documento firmato di un'eventuale limitazione d'uso presente nel certificato del firmatario ([DPR44500], Art. 28 bis, comma 3). Inoltre si rimanda al paragrafo 10.4.1 per le specifiche limitazioni d'uso dei certificati non qualificati emessi dal CNIPA.

Infine si tenga conto delle problematiche relative alla eventuale presenza di macroistruzioni o codice eseguibile nel documento verificato come descritto al paragrafo 10.16.1.

10.16 Modalità operative per l'utilizzo e la generazione delle firme digitali

Il Certificatore unitamente al dispositivo di firma consegna al Titolare software, disponibile anche sul sito www.cnipa.gov.it, per l'apposizione della firma digitale.

Il software consente la selezione del file da firmare, richiede l'inserimento della smart card nel lettore e la digitazione del PIN per l'attivazione della smartcard.

Il software consente la selezione della coppia di chiavi di firma da utilizzare, consentendo anche la visualizzazione del relativo certificato, e di visualizzare il contenuto del documento elettronico da firmare.

Il software richiede al Titolare di confermare la volontà di firmare il documento elettronico visualizzato.

In caso di assenso, il software procede alla produzione del documento informatico in un file con estensione ".p7m" ([AIPACR24]).

10.16.1 Formato dei documenti

L'automazione di ufficio ha introdotto un largo uso di formati documentali che favoriscono l'interscambio e il riutilizzo all'interno dei processi amministrativi. Tali formati documentali arricchiscono il "contenuto" del documento con elementi di codice interpretati dal software applicativo (es. Microsoft Office), finalizzati ad incrementarne il riuso (es. modulistica, campi data, numerazione pagine, formattazione testo) o, ad esempio, effettuare calcoli matematici.

Occorre però tener presente che l'apposizione della firma su documenti elettronici contenenti "macroistruzioni o codici eseguibili, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati", non produce gli effetti di cui al [DPR44500], art. 10, comma 3 ([DPCM130104], art. 3, comma 3).

Tali elementi di codice possono infatti produrre alterazioni al "contenuto" dipendenti dal contesto dell'ambiente di visualizzazione in uso.

Emesso da: <i>Centro Nazionale per l'informatica nella Pubblica Amministrazione</i> Ufficio Servizi di Sicurezza e Certificazione	Tipo documento: Manuale Operativo Codice doc.: MO_Certificazione Data emissione: 29/11/04
Titolo documento: Manuale operativo per il servizio di certificazione di chiavi pubbliche per la Rete Unitaria della Pubblica Amministrazione	Edizione: 2.0 n.ro allegati: 0

Poiché non sono disponibili metodi certi per la verifica della presenza di tutti gli elementi in grado di alterare i contenuti di tali documenti presentati ai fini della apposizione e della verifica della firma, è sconsigliabile, finché possibile, il loro utilizzo per documenti particolarmente critici.

Pertanto, soprattutto per i documenti critici, si suggerisce l'uso di formati documentali statici quali ad esempio:

- Puro testo - “.txt”,
- Immagine - “.tif”,
- Portable Document Format – “.pdf” (se privo di campi modulo).