MANUALE OPERATIVO

FIRMA DIGITALE

www.firmacerta.it

INDICE

1. Versioni e Riferimenti

1.1 Versioni del documento [36.3.b]

Versione:	1.2
Data:	07.03.2010
Motivazione:	Aggiornamento
Modifiche:	Cap. 21. Modalità operative per l'utilizzo del software di verifica delle firme. Cap. 22 Modalità operative per la generazione della firma digitale. Cap. 19 Registro dei certificati.

Versione:	1.1
Data:	08.10.2010
Motivazione:	Specificata la durata massima del Certificato Qualificato.
Modifiche:	Capitolo 17.1 Rinnovo del Certificato qualificato

Versione:	1.0
Data:	23.08.2010
Motivazione:	Prima stesura
Modifiche:	

1.2 Referenti [36.3.c]

Versione:	1.2	Data
Redatto e modificata da:	Luca Romagnoli	25.02.2011
Verificato da:	Enrico Giacomelli Simone Francescangeli	01.03.2011 28.02.2011
Approvato da:	Claudio Gabellini	02.03.2011
Responsabile del documento:	Simone Francescangeli Namirial S.p.A. Tel. 071 63494 Fax 071 60910 E-mail info@firmacerta.it	

Versione:	1.1	Data
Redatto e modificata da:	Luca Romagnoli	15/09/2010
Verificato da:	Enrico Giacomelli Luca Romagnoli	15/09/2010 15/09/2010
Approvato da:	Claudio Gabellini	15/09/2010
Responsabile del documento:	Simone Francescangeli Namirial S.p.A. Tel. 071 63494 Fax 071 60910 E-mail info@firmacerta.it	

Versione:	1.0	Data
Redatto da:	Luca Romagnoli	
Verificato da:	Enrico Giacomelli Luca Romagnoli	10/08/2010 11/08/2010
Approvato da:	Claudio Gabellini	23/08/2010
Responsabile del documento:	Simone Francescangeli Namirial S.p.A. Tel. 071 63494 Fax 071 60910 E-mail info@firmacerta.it	

1.3 Dati Identificativi del Certificatore [36.3.a]

Ai sensi dell' art. 29 del D. Lgs. n. 82/2005 e successive modifiche, Namirial S.p.A. è Certificatore Accreditato che emette, pubblica nel registro e revoca i Certificati Qualificati, in conformità alle regole tecniche vigenti [5]

Ragione Sociale	**Namirial S.p.A.**
Rappresentante legale:	Dott. Claudio Gabellini
Sede legale:	via Caduti sul Lavoro, 4 60019 Senigallia (AN) Tel. 071 63494 Fax 071 60910 E-mail: info@namiril.com
Sede Operativa:	via Caduti sul Lavoro, 4 60019 Senigallia (AN) Tel. 071 63494 Fax 071 60910 E-mail: info@namiril.com
Partita IVA	IT02046570426
Registro Imprese	Ancona
REA	02046570426
Capitale Sociale	6.500.000 euro I.V.
Sito web del servizio	http://www.firmacerta.it
E-Mail del servizio	firmacerta@sicurezzapostale.it
Sito web del gestore	http://www.namirial.com
E-Mail del gestore	firmacerta@namirial.com

1.4 Informazioni commerciali

Per ricevere informazioni commerciali sull'offerta Namirial S.p.A. e sui servizi di Certificazione sono disponibili i seguenti recapiti:

- Telefono: 071 63494
- E-Mail: commerciale@firmacerta.it
- Web: http://www.firmacerta.it

1.5 Help Desk ed assistenza al cliente

Per ricevere informazioni ed assistenza sul servizio sono attivi i seguenti recapiti:

- Telefono: 071 63494
- E-Mail: helpdesk@firmacerta.it
- Web: http://www.firmacerta.it

il servizio è attivo nei giorni feriali con i seguenti orari:
dalle **9.00** alle **13.00** e dalle ore **15.00** alle **19.00.**

2. Generalità

2.1 Scopo del documento

Lo scopo del documento è la descrizione delle regole e le procedure operative adottate dall'unità organizzativa di Certificazione digitale di Namirial per tutte le attività inerenti l'emissione e la gestione dei certificati di sottoscrizione qualificati e delle marche temporali.
Il Documento contiene obblighi e responsabilità per i soggetti che entrano in relazione con il

Certificatore:

- Titolare
- Terzo Interessato
- Destinatario (nel caso in cui verifica la firma)
- Soggetti delegati dal certificatore a svolgere operazioni di registrazione dei titolari

nonché le procedure per l'erogazione del servizio di validazione temporale, se richiesta dagli utenti, in conformità con la vigente normativa in materia di firma digitale.

Il presente documento descrive anche le specifiche Certificate Policy e Certification Practices Statement del Certificatore recependo le raccomandazioni del documento [10] "Certificate Policy and Certification Practices Framework".

Con frequenza non superiore all'anno, il Certificatore esegue un controllo di conformità del processo di erogazione del servizio di certificazione e, ove necessario, aggiorna questo documento anche in considerazione dell'evoluzione della normativa e standard tecnologici.

2.2 Attori

Gli attori indicati nel presente documento sono:

- il Certificatore,
- la Registration Authority (RA),
- la Local Registration Authority (LRA),
- la Local Identification Authority (LIA),
- il Titolare,
- il Terzo Interessato,
- Destinatario.

La definizione di tali attori e contenuta nel paragrafo 2.3.

2.2 Contesto normativo

Riferimenti normativi

[1]	D.Lgs. 4/4/2006 n. 159	Decreto Legislativo 4 aprile 2006 n. 159 Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale.
[2]	DPCM 12/10/2007	Decreto del Presidente del Consiglio dei Ministri 12 ottobre 2007 Differimento del termine che autorizza l'autodichiarazione circa la rispondenza ai requisiti di sicurezza di cui all'art. 13, comma 4, del DPCM", pubblicato sulla GU 30 ottobre 2003, n. 13
[3]	D.Lgs. 82/2005	Decreto Legislativo 7 marzo 2005, n. 82 *Codice dell'amministrazione digitale*
[4]	CNIPA/CR/48	Circolare CNIPA 6 settembre 2005 Modalità per presentare la domanda di iscrizione nell'elenco pubblico dei certificatori di cui all'articolo 28, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.
[5]	DPCM 30/03/2009	Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 Il presente decreto ha abrogato il Decreto del Presidente del Consiglio dei Ministri *13 gennaio 2004* Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici. (GU n. 129 del 6-6-2009)
[6]	D.Lgs. 196/2003	Decreto Legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali.
[7]	DPR 445/2000	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
[8]	CNIPA 45/2009	CNIPA Deliberazione n. 45 del 21 maggio 2009 La presente deliberazione ha abrogato: Deliberazione CNIPA 17 febbraio 2005 n. 4 Deliberazione CNIPA 18 maggio 2006 n. 34 Regole per il riconoscimento e la verifica del documento informatico.
[9]	CNIPA Limiti d'uso nei CQ	Limiti d'uso garantiti agli utenti ai sensi dell'articolo 12, comma 6, lettera c) della Deliberazione CNIPA 21 maggio 2009, n. 45 http://www.cnipa.gov.it/site/_contentfiles/01386700/1386700_Limiti%20uso%20nei%20CQ.pdf
[10]	RFC 3647	Certificate Policy and Certification Practices Framework
[11]	RFC 5280	Internet X.509 Public Key Infrastructure - Certificate and CRL Profile
[12]	ETSI TS 101 456	Policy requirements for certification authorities issuing qualified certificates
[13]	ETSI TS 101 862	Qualified Certificate profile
[14]	ETSI TS 102 023	Policy requirements for time-stamping authorities
[15]	ITU-T X.509 ISO/IEC 9594-8	Information Technology – Open Systems Interconnection – The Directory: Authentication Framework
[16]	DigitPA DC 69/2010	DigitPA - Determinazione Commissariale n. 69/2010

		Modifica della Deliberazione 21 maggio2009 n. 45 del Centro Nazionale per l'Informatica nella pubblica Amministrazione, recante "Regole per il riconoscimento e la verifica del documento informatico", pubblicata il 3 dicembre 2009 sulla Gazzetta Ufficiale della Repubblica Italiana – serie generale – n. 282.
[17]	CAD 30/12/2010 n.235	Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69.

2.3 Definizioni

Appartenenti all'Organizzazione dipendenti e/o associati a favore dei quali l'Organizzazione richiede l'emissione di un certificato qualificato (Es. Aziende, Enti, Associazioni di categoria, ecc.)
Autorità per la marcatura temporale [Time-stamping authority] è il sistema software/hardware, gestito dal Certificatore, che eroga il servizio di marcatura temporale.
Certificato digitale, **Certificato qualificato,** è un documento elettronico che attesta, con una firma digitale, l'associazione tra una chiave pubblica e l'identità di un soggetto (persona fisica). [1] Art.28
Certificatore [Certification Authority] è l'ente, pubblico o privato, abilitato a rilasciare certificati digitali tramite procedura di certificazione che segue standard internazionali e conforme alla normativa italiana ed europea in materia.
Chiava privata è la chiave crittografica utilizzata in un sistema di crittografia asimmetrica; ogni chiave privata è associata ad una chiave pubblica, ed è solo in possesso dal Titolare che la utilizza per firmare digitalmente i documenti.
Chiava pubblica è la chiave crittografica utilizzata in un sistema di crittografia asimmetrica; ogni chiave pubblica è associata ad una chiave privata, ed è utilizzata per verificare la firma digitale apposta su un documento informatico dal Titolare della chiave asimmetrica.
CNIPA Centro Nazionale per l'Informatica nella Pubblica Amministrazione, l'Organismo di controllo istituito dal Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri.
CRL – Lista di revoca e sospensione dei certificati È una lista di certificati che sono stati resi "non validi" dal certificatore prima della loro naturale scadenza. La revoca rende i certificati "non validi" definitivamente. La sospensione rende i certificati "non validi" per un tempo determinato.
CUC E' il Codice Univoco Certificato ed è indicato sulla Richiesta di Registrazione ed inserito nel certificato. Identifica in modo univoco il certificato emesso dal Certificatore.
CUT E' il Codice Univoco Titolare ed è indicato sulla Richiesta di Registrazione
Destinatario è il soggetto a cui è destinato il documento e/o di una evidenza informatica firmata digitalmente.
Dispositivo Sicuro per la Creazione della Firma Dispositivo hardware capace di proteggere efficacemente la segretezza della chiave privata.

Giornale di controllo Il giornale di controllo consiste nell'insieme delle registrazioni, effettuate automaticamente o manualmente, degli eventi previsti dalle Regole Tecniche di base [5].
IUT Identificativo Univoco del Titolare, diverso per ogni certificato emesso.
LDAP [Lightweight Directory Access Protocol] È un protocollo standard per l'interrogazione e la modifica dei servizi di directory (segue gli standard X.500).
LRA Registration Autority locale.
Marca temporale [Timestamp] è il riferimento temporale che consente la validazione temporale.
Manuale Operativo è il documento pubblico depositato presso CNIPA che definisce le procedure applicate dal Certificatore nello svolgimento della propria attività.
OID [Object Identifier] è una sequenza di numeri, registrata secondo lo standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia.
OCSP [Online Certificate Status Protocol] è un protocollo che permette di verificare la validità di un certificato senza ricorrere alle liste di revoca dei certificati. Fa parte dello standard X.509 e viene descritto in RCF 2560.
Organizzazione è un gruppo organizzato di utenti (es. enti, aziende, società, ordini professionali, Associazioni, ecc.) che hanno stipulato accordi con il Certificatore per il rilascio di certificati di firma digitale ai propri dipendenti e/o associati.
PIN [Personal Identification Number] Codice associato ad un dispositivo sicuro di firma, utilizzato dal Titolare per accedere alle funzioni del dispositivo stesso
PUK Codice personalizzato utilizzato dal Titolare per riattivare il proprio dispositivo in seguito al blocco dello stesso per errata digitazione del PIN.
RA Registration Autority, soggetto che esegue l'identificazione dei Richiedenti dei certificati qualificati applicando le procedure definite dal Certificatore.
Referente è la persona fisica incaricata a predisporre ogni documento necessario e mantiene i contatti con il Certificatore.
Registro dei certificati è la lista dei certificati emessi dal Certificatore, nella lista sono inclusi i certificati revocati e sospesi, accessibile telematicamente.
Revoca del certificato è l'operazione con cui il Certificatore annulla la validità del certificato, prima della sua naturale scadenza, da un dato momento, non retroattivo, in poi.
Richiedente

È il soggetto che richiede al Certificatore il rilascio di certificati qualificati. Se il Soggetto è diverso dal Titolare del Certificato l'identità del Richiedente verrà inserito nel campo Organization del certificato X.509.
RFC 3161 Internet X.509 Public key infrastructure Time Stamp Protocol (TSP) PKIW Working Group IETF -Agosto 2001
RSA algoritmo di crittografia asimmetrica, basato su chiavi pubbliche e private.
SHA-1 [*Secure Hash Algorithm*] Algoritmo di crittografia che genera un impronta digitale di 160 bit.
SHA-256 [*Secure Hash Algorithm*] Algoritmo di crittografia che genera un impronta digitale di 256 bit.
Sospensione del certificato è l'operazione con cui il Certificatore sospende la validità del certificato, prima della sua naturale scadenza, per un periodo di tempo definito, non retroattivo.
Terzo Interessato è la persona fisica o giuridica che da il consenso, in conformità alle norme, al rilascio di certificati qualificati nei quali sia riportata l'appartenenza ad una Organizzazione ovvero eventuali poteri di rappresentanza o titoli e cariche rivestite. Ha il diritto/dovere di richiedere la revoca o sospensione del certificato nel caso mutino i requisiti in base ai quali lo stesso è stato rilasciato
Titolare è la persona fisica, identificata dal Certificatore, cui e' attribuita la firma digitale ed è stata consegnata la chiave privata del certificato stesso.
token è il dispositivo fisico (smart card, o chiave USB) che contiene la chiave privata del Titolare.
Ufficio di Registrazione è l'ente che svolge, per conto del Certificatore e secondo modalità da questo definite, le attività individuate e descritte nel presente Manuale. l'ente deve aver preventivamente stipulato accordi di servizio con il Certificatore.
X.509 è uno standard ITU-T per le infrastrutture a chiave pubblica (PKI)

3. Identifica Manuale Operativo

3.1 Manuale operativo

Il presente documento denominato “Manuale Operativo” è identificato attraverso la versione ed il livello di rilascio presente su tutte le pagine.

Il file del documento identificato dal nome NAMIRIAL-MO.PDF è custodito presso la sede del Certificatore è depositato presso DigitPA ed è consultabile per via telematica all’indirizzo Internet **http://www.firmacerta.it/manuali-MO/**, ai sensi dell’art.36 comma 2 del [5].
Tale URI è indicata nel campo cSPuri dell’estensione Certificate Policies dei certificati qualificati, dei server di Marcatura Temporale e OCSP.

3.2 Certificate Policies

Il Certificatore utilizza i seguenti Object Identifier, (OID):
1.3.6.1.4.1.36203 Namirial S.p.A.
1.3.6.1.4.1.36203.1. Certification Authority
1.3.6.1.4.1.36203.1.1 Certificate Policy
1.3.6.1.4.1.36203.2 Time Stamping Authority
1.3.6.1.4.1.36203.2.1 TSA Policy (Policy delle Marche Temporali)

I certificati emessi secondo le regole del presente documento sono identificate con i seguenti Object Identifier, (OID):

1.3.6.1.4.1.36203.1.1.1	Policy per certificati associati ai server di marcatura temporale;
1.3.6.1.4.1.36203.1.1.2	Policy per certificati qualificati associati a dispositivo sicuro per la creazione della firma mediante procedura manuale;
1.3.6.1.4.1.36203.1.1.3	Policy per certificati qualificati associati a dispositivo sicuro per la creazione della firma mediante procedura automatica
1.3.6.1.4.1.36203.1.1.4	Policy per certificati associati ai server OCSP dei certificati qualificati;

Tali OID sono utilizzati a scopo identificativo all’interno dell’estensione Certificate Policies.

4. Responsabilità del Certificatore

Il Certificatore è responsabile, verso i Titolari, per l’adempimento degli obblighi di legge derivanti dalle attività previste dal [7], [6], [5], [4], [3], [8] e successive modifiche ed integrazioni.

Il Certificatore, mette a disposizione, del Titolare apposito kit contenente token (smart card, o chiave USB) completo di Certificato e chiave privata e del software, accuratamente testato, per l’apposizione e la verifica delle firme qualificate.

Il Certificatore è responsabile del presente documento.

Il Certificatore non assume responsabilità:

- per l’uso improprio dei certificati emessi,
- per le conseguenze derivanti dal mancato rispetto delle procedure e delle modalità

operative indicate in questo documento da parte del Titolare,
- per il mancato adempimento degli obblighi previsti a suo carico dovuto a cause ad esso non imputabili,
- derivanti dalla non conoscenza o del non corretto utilizzo delle procedure indicate di questo documento.

5. Limitazioni e indennizzi

Il Certificatore ha stipulato polizza assicurativa per la copertura dei rischi dell'attività e dei danni a tutte le parti (Titolari, Terzi Interessati, Destinatari) non superiore ai massimali di seguito indicati.

€ 150.000 per singolo sinistro per un totale di € 1.500.000 per anno assicurativo per tutte le perdite patrimoniali derivanti da tutte le richieste di risarcimento presentate contro il Certificatore per tutte le coperture assicurative combinate.

6. Limiti d'uso

Ferma restando la responsabilità del ***Certificatore*** di cui al **[3]** (art.30 comma 1 lettera a), è responsabilità dell'**Utente** verificare il rispetto dei limiti d'uso inseriti nel certificato.
La richiesta di inserire altre specifiche limitazioni d'uso, il cui testo non potrà comunque superare 200 caratteri, sarà valutata dal ***Certificatore*** per gli aspetti legali, tecnici e di interoperabilità e valorizzata di conseguenza.
In considerazione dei limiti suddetti, il ***Certificatore*** adotta i limiti d'uso indicati dagli utenti, ai sensi dell'articolo 12, comma 6, lettera c) della Deliberazione [8], e garantisce di gestire il rilascio di certificati con le seguenti limitazioni d'uso:

- I titolari fanno uso del certificato solo per le finalità di lavoro per le quali esso è rilasciato. The certificate holder must use the certificate only for the purposes for which it is issued.
  Il presente certificato è valido solo per firme apposte con procedura automatica. La presente dichiarazione costituisce evidenza dell'adozione di tale procedura per i documenti firmati. The certificate may be used only for automatic procedure signature purposes.
- L'utilizzo del certificato è limitato ai rapporti con (indicare il soggetto). The certificate may be used only for relations with the (declare the subject).

7. Certificazione ISO

Namirial S.p.A. ha ottenuto la certificazione UNI EN ISO 9001:2000 in data 28.11.2007. Namirial ha conseguito il certificato N. 223776 presso la Bureau Veritas Italia S.p.A. che l'ha giudicata conforme ai requisiti della normativa ISO 9001:2000 con il seguente scopo:

progettazione, elaborazione ed assistenza post vendita di software, piattaforme gestionali e siti internet. L'erogazione di servizi hosting e collocation per centri assistenza amministrativa e fiscale.
L'erogazione del servizio di posta elettronica certificata, Certificatore qualificato. Settore/i EA di attività:33.

8. Servizio di Help Desk

Il Certificatore ha predisposto uno specifico canale di comunicazione (help desk) per il Titolare ed il Terzo Interessato, per la gestione di segnalazioni relative al servizio di Firma Digitale.
L' help Desk è costituito da persone individuate e preposte all'assistenza clienti per il servizio di Firma Digitale ed è contattabile con le modalità indicate al paragrafo 1.5.

Le richieste effettuate tramite posta elettronica o attraverso il portale, se pervenute fuori dall'orario lavorativo o nei giorni festivi, sono prese in carico a partire dal primo giorno lavorativo successivo.

Tutte le segnalazioni sono gestite con un sistema di trouble ticketing che aggiorna in tempo reale, via e-mail, il richiedente durante l'intera vita della richiesta.

8.1 Trouble ticketing

Il sistema di trouble ticketing tiene traccia di tutte le richieste pervenute al Certificatore.

Il sistema si basa su un sistema Web avanzato, gestito dal servizio Help Desk, ed è in grado di:

- aprire un nuovo ticket su segnalazione del Titolare o Terzo Interessato,
- seguire la "vita" del ticket nella fase di lavorazione e del cambio di stato fino alla risoluzione della segnalazione,
- attingere ad un "knowledge base" contenente le guide ai servizi, le domande più frequenti (FAQ), i casi più significativi.
- ricercare ticket con diverse modalità di ricerca.

Tutti i cambi di stato del ticket sono notificate al richiedente.

9. Tariffe [36.3.f]

Le tariffe del servizio sono pubblicate sul sito www.firmacerta.it nella sezione "Firma Digitale".

10. Tutela dei dati personali

Le politiche di accesso ai dati sono conformi alle misure minime di sicurezza per il trattamento dei dati personali indicate nel [6]; in particolare consentono:

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

Le informazioni relative al Titolare ed al Terzo Interessato di cui il Certificatore viene in possesso durante l'attività, sono da considerarsi, salvo espresso consenso, riservate e non pubblicabili, con l'eccezione di quelle esplicitamente destinate ad uso pubblico (Chiave pubblica, Certificato, Revoca sospensione, ecc.) nei limiti previsti dalla legislazione vigente e dal consenso fornito dal titolare.

11. Obblighi [36.3.d]

L'utilizzatore di sistemi di chiavi asimmetriche e di firma digitale è tenuto ad adattare tutte le misure organizzative e tecniche idonee ad evitare danni ad altri.

11.1 Obblighi del Certificatore

Il Certificatore che rilascia certificati qualificati:

1. si attiene alla normativa vigente in materia di Firma Digitale [3] [5] [8],
2. provvede con certezza all'identificazione della persona che fa richiesta della certificazione,
3. si accerta dell'autenticità della richiesta di certificazione,
4. specifica, nel certificato qualificato su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della documentazione presentata dal richiedente che attesta la sussistenza degli stessi,
5. richiede, quando previsto e prima di emettere il certificato, la prova del possesso della chiave privata. Verifica la correttezza della coppia di chiavi,
6. rilascia e gestisce il certificato qualificato esclusivamente nei casi consentiti dal titolare del certificato nei modi o nei casi stabiliti nell'art. 32, comma 3, lettera b) del [3], nel rispetto del [6], e successive modificazioni,
7. Fornisce o indica al Titolare i dispositivi sicuri di firma utilizzati nell'ambito del processo di rilascio del certificato qualificato per la generazione delle chiavi, la conservazione della chiave privata e le operazioni di firma, idonei a proteggere la chiave privata ed i dati per la creazione della firma del Titolare con criteri di sicurezza adeguati alla normativa vigente e alle conoscenze scientifiche e tecnologiche più recenti.
8. informa il Titolare in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi, sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione,
9. non si rende depositario, nella loro interezza, dei dati per la creazione della firma del Titolare,
10. non copia, ne' duplica, le chiavi private di firma del soggetto cui il certificatore ha fornito il servizio di certificazione,
11. procede alla tempestiva pubblicazione della revoca e della sospensione del certificato qualificato, nei seguenti casi:
    - richiesta da parte del **Titolare;**
    - richiesta del **Terzo Interessato** dal quale derivino i poteri di quest'ultimo;
    - perdita di possesso del dispositivo chiave
    - compromissione della chiave;
    - provvedimento dell'autorità;
    - acquisizione della conoscenza di cause limitative della capacità del titolare;
    - sospetti abusi o falsificazioni;

    secondo quanto previsto dalle regole tecniche di cui al [5] e successive modifiche ed integrazioni,
12. garantisce un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo nonché garantisce la pubblicazione affidabile, puntuale e sicura degli elenchi dei certificati di firma sospesi e revocati, garantendo che non trascorrano più di 24 ore dalla richiesta di revoca o sospensione alla relativa pubblicazione
13. assicura la precisa determinazione della data e dell'ora di rilascio, scadenza, revoca e

sospensione dei certificati qualificati,
14. registra sul giornale di controllo, l'emissione dei certificati qualificati, con la specificazione della data e dell'ora di generazione; il momento di generazione del certificato è attestato tramite riferimento temporale,
15. tiene registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato dal momento della sua emissione almeno per 20 (venti) anni, anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari,
16. rende accessibile, per via telematica, la copia delle liste, sottoscritte da DigitPA, dei certificati relativi alle chiavi di Certificazione di cui la [5],
17. 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,
18. fornisce almeno un sistema che consenta al Titolare di effettuare la verifica della firma qualificata,
19. nel caso di cessazione del servizio informa, almeno 60 (sessanta) giorni prima, i Titolari che tutti i certificati non scaduti al momento della cessazione saranno revocati e a tempo debito provvede alla loro effettiva revoca ovvero indica gli estremi del certificatore sostitutivo che si farà carico di detti certificati
20. adotta le misure di sicurezza per il trattamento dei dati personali, ai sensi del [6].

11.2 Obblighi del Titolare

Il Titolare dei certificati qualificati è tenuto a:

1. prendere visione del presente documento prima di richiedere il Certificato qualificato e rispettarne le prescrizioni per quanto di propria competenza,
2. fornire tutte le informazioni richieste dal Certificatore, garantendone l'attendibilità sotto la propria responsabilità,
3. comunicare al Certificatore eventuali variazioni delle informazioni fornite all'atto della registrazione: dati anagrafici, residenza, recapiti telefonici, indirizzo di posta elettronica, ecc,
4. mantenere in modo esclusivo la conoscenza o la disponibilità dei dati per la creazione della firma (PIN, PUK) e il codice (passphrase) per la sospensione in emergenza, conservandoli con la massima diligenza, separatamente dal dispositivo che contiene la chiave privata, al fine di garantirne l'integrità e la massima riservatezza,
5. non utilizzare la firma qualificata per funzioni e finalità diverse da quelle per la quale è stata rilasciata,
6. adottare le misure indicate nel presente manuale al fine di evitare di apporre firme qualificate su documenti contenenti macro istruzioni o codici eseguibili che ne modifichino gli atti o i fatti negli stessi rappresentati e che renderebbero, quindi, nulla l'efficacia della sottoscrizione,
7. inoltrare, con le modalità indicate dal Certificatore, la richiesta di sospensione specificando la motivazione ed il periodo durante il quale la validità del certificato deve essere sospesa,
8. richiedere l'immediata revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi di firma di cui abbia perduto il possesso o difettosi,
9. inoltrare, con le modalità indicate dal Certificatore, la richiesta di revoca specificandone la motivazione e la sua decorrenza,

10. sporgere denuncia, in caso di smarrimento o sottrazione del dispositivo di firma, alle autorità competenti,
11. presentarsi presso l'Ufficio di Registrazione o del Certificatore a seguito della richiesta telefonica di sospensione immediata del certificato, e richiedere per iscritto la revoca o la riattivazione dello stesso,
12. utilizzare esclusivamente dispositivi di firma indicati ovvero forniti dal certificatore in modo conforme a quanto indicato nel presente manuale.

11.3 Obblighi del Terzo Interessato

Il Terzo Interessato è tenuto:

1. a provvedere, previo esplicito consenso dei richiedenti, a raccogliere i dati necessari alla registrazione, nella forma richiesta dal Certificatore,
2. a chiedere la revoca e la sospensione dei certificati, secondo le modalità indicate nel presente Documento, ogniqualvolta vengano meno i presupposti in base ai quali il certificato è stato rilasciato al titolare. (cessazione della propria attività, cambio mansioni, sospensioni, ecc.),
3. a comunicare tempestivamente al certificatore ogni modifica delle circostanze indicate al momento del rilascio del certificato rilevanti ai fini del suo utilizzo
4. A inoltrare la richiesta di revoca o sospensione al Certificatore munita di sottoscrizione e della motivazione, con la specificazione della sua decorrenza (e durata, nel caso di sospensione).

11.4 Obblighi dei Destinatari di documenti informatici

Il destinatario è tenuto a verificare:

1. che il certificato del Titolare sia stato emesso da un Certificatore accreditato,
2. l'autenticità del certificato contenente la chiave pubblica del firmatario del documento,
3. l'assenza del certificato dalla Lista di Revoca e Sospensione (CRL) dei certificati,
4. l'esistenza ed il rispetto di eventuali limitazioni all'uso del certificato utilizzato dal titolare.

11.5 Obblighi della Registration Authority locale (LRA)

L'Ufficio di Registrazione è tenuto a:

1. informare il Titolare in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti per accedervi, sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione,
2. informare il Titolare riguardo agli obblighi da quest'ultimo assunti in merito a conservare con la massima diligenza, e separatamente dal dispositivo per l'apposizione della firma che contiene la chiave privata, i codici segreti (PIN, PUK e pass-phrase) ricevuti dal Certificatore, al fine di garantirne l'integrità e la massima riservatezza,

3. richiedere, quando previsto e prima di rilasciare il certificato, la prova del possesso della chiave privata e verificare la correttezza della coppia di chiavi,
4. informare il titolare delle misure di sicurezza adottate per il trattamento dei dati personali, ai sensi del [6],
5. provvedere con certezza all'identificazione della persona che fa richiesta della certificazione,
6. accertare l'autenticità della richiesta di certificazione,
7. comunicare al Certificatore tutti i dati e documenti acquisiti durante l'identificazione del Titolare e previsti dalle procedure del Certificatore al fine di attivare tempestivamente la procedura di emissione del certificato,
8. verificare ed inoltrare al Certificatore le richieste di revoca, sospensione e rinnovo richieste dal Titolare presso l'Ufficio di Registrazione,
9. attenersi scrupolosamente alle regole impartite dal Certificatore e presenti su questo documento.

Gli Uffici di Registrazione sono autorizzati ad operare dal Certificatore a seguito di adeguato addestramento del personale addetto.

Il Certificatore verifica periodicamente la rispondenza delle procedure adottate dall'Ufficio di Registrazione a quanto indicato nel presente documento.

Il Certificatore, salvo diritto di rivalsa, resta comunque l'unico ed il solo responsabile verso terzi dell'attività svolta dall'Ufficio di registrazione.

12. Tipologia di Certificati qualificati

12.1 Certificati per persone fisiche

Il Richiedente è identificato dall'incaricato della registrazione del Certificatore che:

- verifica i dati identificativi personali,
- verifica l'identità attraverso un documento di riconoscimento in corso di validità,
- verifica la correttezza del codice fiscale o, se applicabile, di altro codice identificativo previsto dalle vigenti norme;
- verifica la richiesta di emissione dei certificati.

Il Certificatore si riserva di effettuare delle verifiche sull'autenticità della documentazione fornita.

12.2 Certificati per appartenenti ad Organizzazioni

Il rilascio di Certificati qualificati a persone fisiche appartenenti ad una Organizzazione, può avvenire secondo le seguenti modalità:

- **MODALITA' 1**: il Certificatore e l'Organizzazione sottoscrivono una Convenzione, identificano il "Referente" dell'Organizzazione che opererà nei confronti del Certificatore come Terzo Interessato e avrà il compito di:
  - raccogliere i dati e i documenti identificativi dei Richiedenti,
  - verificare l'identità del richiedente,
  - compilare le richieste di emissione dei certificati,
  - inviare al Certificatore i dati nelle modalità indicate.

- **MODALITA' 2**: il Richiedente fornisce al Certificatore oltre ai dati identificativi personali, un documento ufficiale comprovante il possesso dei requisiti che si richiede vengano inseriti all'interno del certificato qualificato e l'autorizzazione da parte dell' Organizzazione all'inserimento dei propri dati nel certificato stesso. La documentazione non deve essere antecedente a 30 giorni dalla data di richiesta al Certificatore dell'emissione del Certificato qualificato. Il Richiedente si incontra con l'incaricato della registrazione del Certificatore che verificherà l'identità dello stesso attraverso un documento di riconoscimento in corso di validità.

12.3 Certificati di qualifica professionale

Il rilascio di Certificati qualificati a persone fisiche aventi qualifiche professionali, con l'indicazione dell'Ordine/Albo/Collegio nel campo "Organizzazione" richiede la verifica da parte dell'Ordine/Albo/Collegio professionale dell'iscrizione del richiedente e della sussistenza dei requisiti necessari. Le modalità di rilascio del Certificato qualificato sono le seguenti:

- **MODALITA' 1**: il Certificatore e l'Ordine/Albo/Collegio professionale, sottoscrivono una Convenzione, identificano il "Referente" dell'Ordine/Albo/Collegio professionale che avrà il compito di:
  - raccogliere i dati e i documenti identificativi dei Richiedenti,
  - verificare l'identità del richiedente, l'iscrizione all'Ordine/Albo/Collegio e la sussistenza dei requisiti
  - compilare le richieste di emissione dei certificati,
  - inviare al Certificatore i dati nelle modalità indicate.

- **MODALITA' 2**: il Richiedente fornisce al Certificatore oltre ai dati identificativi personali, un documento di riconoscimento in corso di validità, un certificato di iscrizione rilasciato all'Ordine o Albo o Collegio da cui risulti la qualifica e l'autorizzazione dell'Ordine o Albo o Collegio all' inserimento del ruolo/qualifica nel certificato. La documentazione non deve essere antecedente a 30 giorni dalla data di richiesta al Certificatore dell'emissione del Certificato qualificato. Il Certificatore si riserva di effettuare delle verifiche di autenticità della documentazione fornita.

L'Ordine/Albo/Collegio assumono in questo caso il ruolo di Terzo Interessato. L'indicazione che il certificato con tale ruolo è stato richiesto/autorizzato dall'Ordine/Albo/Collegio, consiste nell'indicazione nel campo "Organizzazione" del certificato qualificato dell''Ordine/Albo/Collegio e nell'opportuna valorizzazione del campo "Title".

Le medesime modalità sono applicabili nel caso di appartenenza ad una organizzazione per l'inserimento di eventuali ruoli ricoperti all'interno dell'organizzazione medesima.

Resta salva la facoltà per il Richiedente di ottenere l'indicazione di una qualifica/ruolo/titolo all'interno del certificato qualificato senza l'intervento del terzo interessato. In questo caso il campo "Organizzazione" conterrà il valore "Non presente" e l'indicazione della qualifica mediante il campo "Title", assumerà mero valore di autocertificazione effettuata dal titolare ai sensi della normativa vigente.

13. Modalità di identificazione e registrazione degli utenti[36.3.g]

Le procedure per il rilascio del certificato prevedono:

- che il Richiedente sia registrato presso il Certificatore,

- che il Richiedente venga identificato con certezza dal Certificatore.

Le attività di identificazione, oltre che svolte direttamente dal personale autorizzato del Certificatore, possono essere svolte dagli Uffici di Registrazione e dal Referente del Terzo Interessato che ha sottoscritto una Convenzione.

Le attività di registrazione, oltre che svolte direttamente dal personale autorizzato del Certificatore, possono essere svolte dagli Uffici di Registrazione.

Da qui a seguire Certificatore e Ufficio di Registrazione saranno indicati come Certificatore.

13.1 Identificazione da parte del Certificatore

Il Richiedente si reca presso il Certificatore con i seguenti documenti:

- Uno dei seguenti documenti di riconoscimento in corso di validità secondo quanto previsto dall'art. 35 del [7]:
  - Carta d'identità,
  - passaporto,
  - patente di guida,
  - patente nautica,
  - libretto di pensione,
  - patentino di abilitazione alla conduzione di impianti termici,
  - porto d'armi,

Sono consentite altre tessere di riconoscimento, purché munite di fotografia e di timbro e di altre segnature equivalenti, rilasciate da un'Amministrazione dello Stato.

- Il Tesserino contenente il Codice Fiscale.
- Se si richiede l'inserimento del Ruolo e dell'Organizzazione nel certificato qualificato si deve fornire:
  - Documento dell' Organizzazione su carta intestata, recante data e numero di protocollo, che autorizza all'inserimento dei dati nel Certificato qualificato del Richiedente, non antecedente a 30 (trenta) giorni dalla data di richiesta di registrazione.
  - Attestazione che l'Organizzazione ha ricevuto l'informativa di cui l'Art. 13 del [6].
- Se si richiede l'inserimento del Titolo e/o Abilitazione Professionale nel certificato qualificato si deve fornire:
  - Documento rilasciato l'Ordine/Albo/Collegio professionale che attesti l'effettiva appartenenza, non antecedente a 30 (trenta) dalla data di richiesta di registrazione.

Il Richiedente dovrà sottoscrivere:

- Domanda di richiesta di emissione del Certificato qualificato debitamente compilata in tutte le sue parti.
- Attestazione che ha ricevuto l'informativa di cui l'Art. 13 del [6].
- Attestazione che ha preso visione di questo documento e si impegna a rispettarlo per quanto di propria competenza.

13.2 Identificazione da parte del Terzo Interessato del Titolare

Il Terzo Interessato, nella persona del Referente, raccoglie ed inoltra al Certificatore i seguenti documenti:

- Domanda di richiesta di emissione del Certificato qualificato debitamente compilata in tutte le sue parti.
- Attestazione che il Richiedente ha ricevuto l'informativa di cui l'Art. 13 del [6].

- Attestazione che ha preso visione di questo documento.
- Copia di uno dei seguenti documenti di riconoscimento in corso di validità secondo quanto previsto dall'art. 35 del [7]:
  - Carta d'identità,
  - passaporto,
  - patente di guida,
  - patente nautica,
  - libretto di pensione,
  - patentino di abilitazione alla conduzione di impianti termici,
  - porto d'armi,
  - Sono consentite altre tessere di riconoscimento, purché munite di fotografia e di timbro e di altre segnature equivalenti, rilasciate da un'Amministrazione dello Stato.
- Copia del Tesserino contenente il Codice Fiscale.
- Se si richiede l'inserimento del Ruolo e del Terzo Interessato nel certificato qualificato si deve fornire:
  - Documento dell' Organizzazione su carta intestata, recante data e numero di protocollo, che autorizza all'inserimento dei dati nel Certificato qualificato del Richiedente, non antecedente a 30 (trenta) giorni dalla data di richiesta di registrazione.
  - Attestazione che l'Organizzazione ha ricevuto l'informativa di cui l'Art. 13 del [6].
- Se si richiede l'inserimento del Titolo e/o Abilitazione Professionale nel certificato qualificato si deve fornire:
  - Documento rilasciato l'Ordine/Albo/Collegio professionale che attesti l'effettiva appartenenza, non antecedente a 30 (trenta) dalla data di richiesta di registrazione.

La firma apposta sui documenti che lo richiedono potrà essere digitale od autografa.

13.3 Registrazione

Per emettere il Certificato qualificato è necessario procedere alla registrazione del Richiedente, dopo aver verificato la documentazione consegnata al Certificatore.

Conclusa la fase di registrazione iniziale, il rilascio del certificato qualificato e, ove previsto, la consegna del token può avvenire con diverse modalità.

Il Richiedente con il rilascio del certificato assume la qualifica di Titolare.

14. Modalità di generazione delle chiavi [36.3.h]

La generazione della coppia di chiavi asimmetriche (pubblica e privata) è effettuata mediante dispositivi e procedure che assicurano, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e la robustezza della chiavi generate, 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.

Il Certificato qualificato attribuito ad un Titolare risiede su un unico dispositivo.
La chiave privata del Titolare è creata all'interno del dispositivo dove è utilizzata. La chiave privata non è esportabile e non è tecnicamente possibile effettuarne copie di backup.

L'utilizzo della chiave privata del Titolare può avvenire solo dopo l'autenticazione con PIN.
La duplicazione della chiave privata e dei token che la contengono è vietata.
I dispositivi per la creazione della firma utilizzati dai Titolari sono certificati Common Criteria EAL4+ secondo un traguardo di sicurezza conforme alla norma CWA 14169 o sono comunque conformi alle disposizioni vigenti.

14.1 Algoritmi e lunghezza delle chiavi

Nelle operazioni di firma è usato l'algoritmo RSA.
Le chiavi usate dal Certificatore per firmare i certificati hanno lunghezza pari a 2048 bit.
La lunghezza della chiave di sottoscrizione dei titolari è pari almeno a 1024 bit.

14.2 Algoritmi di hash

Per la generazione dell'impronta è utilizzata la funzione di hash SHA-256. L'algoritmo SHA-1 è supportato solo in modalità di verifica delle firme nei limiti dell'articolo 27 comma 4 e articolo 29 della Deliberazione 45/2009.

15. Modalità di emissione dei certificati [36.3.i]

L'emissione dei certificati è effettuata in modo automatico dalla procedura del Certificatore e vengono effettuate le seguenti verifiche:

1. che il Titolare sia stato registrato correttamente,
2. che la documentazione fornita sia conforme a questo documento,
3. che il Richiedente sia in possesso della chiave privata corrispondente alla chiave pubblica per la quale viene richiesto il certificato (mediante verifica crittografica della firma sulla richiesta in formato PKCS#10),
4. l'autenticità della firma dell'incaricato che ha convalidato la richiesta,
5. che la chiave sia della lunghezza prevista.

Si procede:

1. all' associazione della busta cieca al Richiedente,
2. all'assegnazione del dispositivo di firma al Richiedente,
3. all' assegnazione al Richiedente di un codice identificativo univoco nell'ambito degli utenti del Certificatore (CUC), diverso per ogni certificato emesso,
4. alla connessone al dispositivo di firma con il PIN di default,
5. al cambio del PIN di default con quello associato alla busta cieca,
6. alla generazione del certificato contenente la chiave pubblica e i dati previsti mediante la firma con la chiave di certificazione della CA,
7. all'inserimento del certificato nel registro dei certificati,
8. alla registrazione sul registro di controllo dell'avvenuta generazione,
9. alla trasmissione del certificato dalla CA alla LRA
10. all'inserimento del certificato nel dispositivo di firma,
11. alla verifica dell'inserimento del certificato nel dispositivo di firma,
12. alla cancellazione dal DB cifrato del record della busta cieca associata al titolare,
13. alla registrazione sul giornale di controllo dell'avvenuta personalizzazione del dispositivo di firma,

L'operatore LRA procede:

1. a stampare e far sottoscrivere al Titolare due copie del contratto (che prevede l'accettazione da parte del Titolare dei dati inseriti nel certificato),
2. alla consegna di una delle due copie,
3. alla consegna del dispositivo di firma al Titolare,
4. alla consegna della busta cieca associata al titolare ed individuata dal numero di riferimento visibile all'esterno e contenente il PIN, il PUK ed il codice d'emergenza,
5. alla consegna di copia del manuale.

16. Revoca e sospensione del certificato qualificato [36.3.I]

La revoca e la sospensione del certificato qualificato determinano la fine della validità prima della scadenza naturale e invalidano eventuali firme apposte successivamente al momento della pubblicazione della lista di revoca che contiene il riferimento a tale certificato, la pubblicazione della lista è attestata mediante adeguato riferimento temporale apposto dal Certificatore.
Le liste di revoca e sospensione (CRL) sono pubblicate nel registro dei certificati con periodicità stabilita dal [8] art. 18 com. 4 (vedi 15.5).
Il Certificatore può anticipare l'emissione della CRL in circostanze particolari.
La data della pubblicazione della lista è asseverata da un riferimento temporale è riportata nel Giornale di Controllo del Certificatore, dove sono annotate sospensioni, revoche e riattivazione dei certificati.
La revoca e la sospensione del certificato qualificato determinano la revoca e la sospensione di tutti gli altri certificati presenti sul token.

La sospensione del certificato comporta la NON VALIDITA' delle firme generate durante il periodo di sospensione. Se il certificato è riattivato si annullano tutti gli effetti della sospensione.
Nel caso in cui si proceda alla revoca di un certificato in stato di sospensione, la revoca decorre dalla data di inizio della sospensione.

16.1 Motivi per la revoca, sospensione, sospensione in emergenza del certificato [17.1]

Il mantenimento del Certificato qualificato è sempre a cura del Certificatore, che deve:

- revocarlo in caso di cessazione dell'attività del Certificatore, fatto salvo indicare un certificatore sostitutivo ai sensi dell'art. 37, comma 2 del. [3],
- revocarlo o sospenderlo in esecuzione di un provvedimento dell'autorità,
- revocarlo o sospenderlo a seguito di richiesta del Titolare o del Terzo Interessato dal quale derivino i poteri del Titolare, nei casi in cui:
  - sia stato smarrito il token,
  - sia venuta meno la segretezza della chiave privata o delle credenziali di accesso al dispositivo di generazione della firma,
  - si sia danneggiato il token,
  - si sia verificato un qualunque evento che abbia compromesso l'affidabilità della chiave,
  - siano mutati i dati di riferimento del Titolare indicati nel certificato, ivi compresi quelli relativi al Ruolo.
  - si siano accertati abusi o falsificazioni,
  - sia terminato il rapporto tra Titolare e Certificatore.

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

16.2 Modalità per la revoca o sospensione del certificato

La revoca o la sospensione del certificato qualificato viene inoltrata per iscritto al Certificatore compilando l'apposito modulo messo a disposizione sul sito del Certificatore
Il modulo deve essere compilato in tutte le sue parti ed inoltrato al Certificatore che verifica l'autenticità della richiesta, il Certificatore comunica al Titolare secondo le modalità stabilite all'atto dell'identificazione e procede alla revoca del certificato, inserendolo nella lista da lui gestita e la pubblica.

- La richiesta di revoca contiene la data a decorrere dalla quale il certificato sarà revocato.
- La richiesta di sospensione contiene la data di inizio e di fine della stessa; la data di fine non deve essere successiva alla data di scadenza del certificato.

16.3 Sospensione in emergenza

Il Titolare, in caso di smarrimento o compromissione della chiave privata, richiede tempestivamente al Certificatore la sospensione del certificato.
La richiesta può essere inoltrata:

- per telefono al servizio di Help Desk (par.1.5)
- per e-mail attiva 24 ore su 24, fornendo il codice di emergenza, è gestita durante gli orari d'ufficio (par.1.5)
- via Web il servizio è attivo 24 ore su 24, 7 giorni su 7.

Il Certificatore procede tempestivamente ad inserire il Certificato qualificato nella lista dei certificati revocati e sospesi (CRL) e alla pubblicazione.

Successivamente il Titolare/Terzo Interessato richiede per iscritto, al Certificatore, la revoca o la sospensione o la riattivazione del Certificato, motivandola.
Nel caso in cui il Titolare/Terzo Interessato non avanzi richiesta scritta entro 60 (sessanta) giorni la sospensione si trasformerà in Revoca.
Il Certificatore 10 (dieci) giorni prima del termine notificherà, via e-mail, al Titolare la scadenza del periodo di sospensione.
La Revoca decorre dalla data di inizio della sospensione.

16.4 Modalità per l'inoltro delle richieste per iscritto [20.2]

Il Titolare può richiedere la revoca, la sospensione o la riattivazioni del certificato con le seguenti modalità:

- **Sito Web**, il Titolare Interessato si collega al sito web del Certificatore, compilando l'apposito modulo elettronico.
  Per garantire l'autenticità della richiesta il Titolare prima di accedere al sistema deve inserire nel sistema di autenticazione i seguenti dati:
  - codice del dispositivo di firma,
  - codice d'emergenza.
- **Cartacea**, il Titolare/Terzo Interessato scarica dal sito del Certificatore l'apposito modulo, compila il modulo in tutte le sue parti, si reca presso il certificatore con un

documento di riconoscimento in corso di validità o inoltra il modulo via fax con copia di un documento di riconoscimento in corso di validità.
Il Certificatore verifica l'autenticità della richiesta con le seguenti modalità:
se Titolare

- verifica che la richiesta sia compilata in tutte le sue parti,
- verifica che il documento di riconoscimento sia in corso di validità,

se Terzo Interessato

- verifica che la richiesta sia compilata in tutte le sue parti,
- verifica l'esistenza del timbro o altra segnatura equivalente,
- verifica che il richiedente sia il "Referente" indicato nella Convenzione,
- verifica che il documento di riconoscimento sia in corso di validità,

16.5 Tempi per la gestione delle richieste [20.3]

- Salvo casi di emergenza applicabili alla sospensione, le Richieste di revoca*, sospensione e riattivazione* dei certificati qualificati, saranno gestiti entro un giorno lavorativo dal ricevimento della richiesta.
- La richiesta di *sospensione immediata* potrà essere inoltrata all'Help Desk tramite:
  - Telefono, durante gli orari d'ufficio (par.1.5),
  - E-mail, 24 ore su 24, sarà comunque presa in carico durante gli orari d'ufficio
  - via Web, il servizio è attivo 24 ore su 24, 7 giorni su 7 e sarà tempestivamente presa in carico e processata.
- Il tempo di attesa tra la presa in carico della richiesta di revoca, di sospensione o di riattivazione e la pubblicazione della lista è al massimo di 24 ore; il momento della pubblicazione è asseverato da un riferimento temporale ed annotato nel giornale di controllo.
- Fermo restando che il Certificatore provvederà tempestivamente alla pubblicazione della nuova lista (CRL) in caso di richiesta di sospensione in emergenza; il momento della pubblicazione è asseverato da un riferimento temporale ed annotato nel giornale di controllo.

16.6 Comunicazione dell'avvenuta revoca o sospensione

Il Certificatore dopo aver verificato l'autenticità della richiesta provvede ad avvisare tempestivamente il Titolare e/o il Terzo Interessato con le seguenti modalità:

- se la richiesta è su iniziativa del Titolare, il Certificatore verifica se nel certificato sono presenti informazioni relative all'Organizzazione, in tal caso provvede a comunicare al Terzo Interessato, l'avvenuta revoca o sospensione, via e-mail.

- se la richiesta è su iniziativa del Terzo Interessato, il Certificatore comunica al Titolare e al Terzo Interessato l'avvenuta revoca o sospensione del suo Certificato, via e-mail.

- se l'iniziativa è del Certificatore, il Certificatore comunica al Titolare l'intenzione di revocare o sospendere il Certificato, via e-mail, indicando la motivazione nonché la

data e l'ora di decorrenza; e se nel certificato è presente l'Organizzazione, comunica, via e-mail, al Terzo Interessato, se aveva sottoscritto la Convenzione, la variazione di stato del Certificato.

17. Modalità di sostituzione delle chiavi e rinnovo del Certificato qualificato [36.3.m]

17.1 Rinnovo del Certificato qualificato

La durata del Certificato qualificato ha durata massima 6 (sei) anni.
La richiesta di rinnovo delle chiavi deve essere effettuato prima della scadenza del Certificato.
Il Certificatore può rinnovare solo Certificati qualificati da lui emessi.
Nel caso di richiesta effettuata dopo la scadenza del Certificato si procederà ad una nuova registrazione ed emissione.
La procedura prevede:

- Generazione di una nuova coppia di chiavi
- Richiesta di rinnovo da parte del Titolare, firmata digitalmente per mezzo della chiave privata associata al certificato in scadenza,
- se nel Certificato qualificato sono presenti informazioni relative al Ruolo e Organizzazione, il Certificatore le inserirà nel Certificato Qualificato, come pervenute, ove applicabili,
- Il Certificatore
  - verifica l'autenticità della richiesta,
  - aggiorna tempestivamente i propri dati relativi al Titolare con le informazioni fornite dal Terzo Interessato,
  - emette un nuovo Certificato,
  - scrive sul dispositivo sicuro di firma il Certificato,
  - Registra sul giornale di Controllo l'avvenuta operazione,

17.2 Sostituzione del Certificato qualificato

Qualora si rendesse necessario la sostituzione del Certificato qualificato a causa di variazioni delle informazioni in esso contenute, si procederà a revocare tale certificato e si procederà ad una nuova emissione come descritto nel capitolo 15.

17.3 Sostituzione delle chiavi di marcatura temporale [45.2]

Le chiavi di marcatura temporale sono sostituite dopo non più di 3 (tre) mesi di utilizzo, indipendentemente dalla durata del loro periodo di validità e senza revocare il corrispondente certificato, in conformità all' art. 45, comma 2 del [5].
I certificati relativi alle chiavi di marcatura temporale hanno durata massima pari a 11 (undici) anni.

17.4 Sostituzione del certificato di CA

La sostituzione del Certificato della CA del Certificatore, impiegata per sottoscrivere i Certificati qualificati del Titolare, ha durata 20 anni ed è emesso, un nuovo certificato, ogni 8 anni per garantire la fruibilità di tutti i certificati emessi fino alla naturale scadenza degli

stessi.
La sostituzione del Certificato della CA del Certificatore, impiegata per sottoscrivere i Certificati di marcatura temporale, ha durata 20 anni ed è emesso un nuovo certificato ogni 8 anni per garantire la fruibilità di tutti i certificati emessi fino alla naturale scadenza degli stessi.

18. Archiviazione dei Certificati qualificati e di marcatura temporale

I certificati qualificati e quelli relativi alle chiavi di marcatura temporale sono archiviati e conservati per 20 (venti) anni dalla emissione.
Le chiavi private di firma di cui sia scaduto il certificato non possono più essere utilizzate.

19. Registro dei certificati

Il registro dei certificati contiene:

- Tutti i certificati emessi dal Certificatore,
- la lista dei certificati sospesi (CRL),
- la lista dei certificati revocati (CRL),

19.1 Gestione del Registro dei certificati [36.3.n]

La copia di riferimento del registro dei certificati è gestita dal certificatore, non è accessibile dall'esterno e contiene tutti i certificati qualificati e le liste di revoca emessi dal certificatore.
Tutte le operazioni che modificano i dati all'interno del registro sono automaticamente riportate nel Giornale di Controllo.
Il registro è aggiornato all'emissione di ogni certificato qualificato e alla pubblicazione della lista di revoca.
Le copie operative del registro dei certificati sono accessibili pubblicamente in sola lettura e contengono i certificati emessi per le chiavi di sottoscrizione dell'elenco pubblico dei certificatori emesso dal CNIPA e l'elenco più recente dei certificati revocati e sospesi. la pubblicazione della copia operativa del registro è aggiornata in modo sincrono ad ogni aggiornamento della copia di riferimento del registro stesso.

19.2 Accesso al Registro dei certificati [36.3.o]

La copia di riferimento del registro dei certificati è accessibile SOLO dal sistema di generazione dei certificati.
La pubblicazione delle informazioni sulle copie operative del registro dei certificati è consentita solamente al certificatore. Tali informazioni sono pubblicamente accessibili in sola lettura e tramite il protocollo http.
Per evitare che di avere CRL di dimensioni troppo elevate, al momento dell'emissione di ogni certificato, il certificatore associa a quest'ultimo una specifica CRL il cui indirizzo completo di scaricamento è inserito nell'estensione CRL Distribution Point.
L'indirizzo di ogni CRL è ottenuto concatenando l'indirizzo base http://www.firmacerta.it/registro con il nome della specifica CRL, distinta mediante un numero progressivo, es. *FirmaCertaQualificata1.crl*, *FirmaCertaQualificata2.crl*, …
All'emissione delle liste di revoca il certificatore garantisce che sia pubblicato l'insieme di tutte le CRL necessarie a coprire tutti i certificati emessi nel loro complesso fino a quel momento dal certificatore.
Certificati e CRL partizionate sono emessi nel rispetto della specifica tecnica RFC5280, con

particolare riferimento alle estensioni necessarie al partizionamento delle CRL qui descritto..
All'indirizzo: http://crl.firmacerta.it/ è possibile visualizzare la lista di tutti gli elementi disponibili e scaricabili contenuti nel registro, l'insieme di CRL emesse aggiornato

All'indirizzo *http://crl.firmacerta.it/* è possibile visualizzare la lista di tutti gli elementi disponibili e scaricabili contenuti nel registro, l'insieme di CRL emesse aggiornato.

All'indirizzo *http://www.firmacerta.it/Certificatori/* è possibile visualizzare la lista:

- dell' elenco pubblico dei certificatori di DigitPA,
- dell' elenco pubblico dei certificati revocati
- dell' elenco pubblico dei certificati revocati relativi alle marche temporali

20. marcature temporale

20.1 Modalità per l'apposizione e la definizione del riferimento temporale [36.3.p]

L'emissione della marca temporale, richiesta dal Titolare del Certificato qualificato è ottenuta mediante un software fornito dal Certificatore ed installato sul computer del Titolare, ed il servizio web è raggiungibile tramite internet con protocollo sicuro.
Il processo di marcatura è il seguente:

- il Titolare, mediante il software fornito con il kit, produce e firma la richiesta di marcatura temporale del documento informatico,
- La richiesta è inoltrata al Certificatore con protocollo sicuro (HTTPS),
- il Certificatore verifica la richiesta e le credenziali del Titolare,
- il Certificatore genera la marca temporale, con un sistema ad alta affidabilità è coincide con il momento della sua generazione, con una differenza non superiore ad un minuto secondo rispetto alla scala di tempo UTC (IEN), del [9],
- la marcatura viene consegnata al Titolare, in modalità sicura, per l'utilizzo.

L'impronta dell'evidenza informatica è calcolata secondo l'algoritmo di hash SHA-256.
Nel caso in cui il sistema di marcatura temporale (TSA) riceva una richiesta non conforme viene restituito un messaggio d'errore.
Non è consentito richiedere l'emissione per una marca temporale specificando una particolare policy.
Il certificatore emette solamente marche temporali la cui policy è definita dal presente manuale ed identificata con il seguente OID:
1.3.6.1.4.1.36203.2.1.1 Time Stamping Authority - Policy 1

20.2 Modalità di generazione delle chiavi di marcatura temporale

La generazione delle chiavi avviene nel rispetto dell'art. 45 del [5].
La chiavi di certificazione e di marcatura temporale sono generate in presenza del responsabile del servizio di certificazione e validazione temporale.
La coppia di chiavi utilizzata per la validazione temporale è di tipo RSA con lunghezza pari a 2048 bit e viene associata in maniera univoca al sistema di validazione temporale al momento della generazione.

Al fine di limitare il numero di marche temporali generate con la medesima coppia, le chiavi di marcatura temporale sono sostituite ed un nuovo certificato emesso dopo non più di 3 (tre) mesi di utilizzazione, indipendentemente dalla durata del loro periodo di validità e senza revocare il corrispondente certificato.

20.3 Archiviazione e validità delle marche temporali

Tutte le marche temporali emesse dal sistema di validazione sono conservate in un apposito archivio digitale non modificabile.

Le marche sono conservate per 20 (venti) anni dalla data di emissione ed hanno validità per l'intero periodo di conservazione.

20.4 Precisione del riferimento temporale

Durante la generazione della marca temporale il server della TSA utilizza la data e l'ora dal clock del sistema, mantenuto allineato con l'ora UTC (Tempo Universale Coordinato) mediante una sonda esterna connesso al sistema della rete satellitare GPS.
La tolleranza non è mai superiore al minuto secondo, come richiesto dalle norme vigenti.

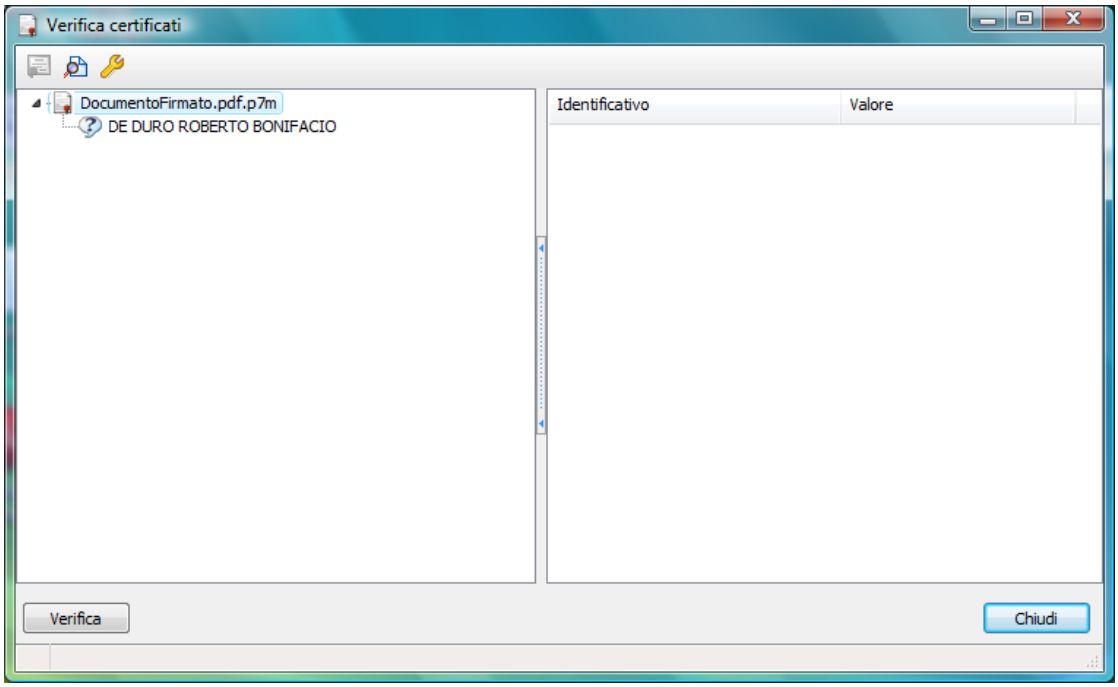
21. Modalità operative per l'utilizzo del sistema di verifica delle firme [36.3.s]

Il Certificatore, attenendosi all'art. 10 del [5] rende disponibile o indica al Titolare un sistema che permetta la verifica delle firme qualificate apposte sui documenti informatici secondo gli standard PKCS#7, CAdES e lo XAdES.

Per la verifica della firma sul documento si deve:

- verificare se il computer è connesso ad internet,
- cliccare sul documento firmato,
- premere il tasto destro del mouse
- posizionarsi su Firma Certa → Verifica

si apre la seguente videata,



Premendo sul tasto verifica l'applicativo verifica presso il Certificatore lo stato del Certificato Qualificato.

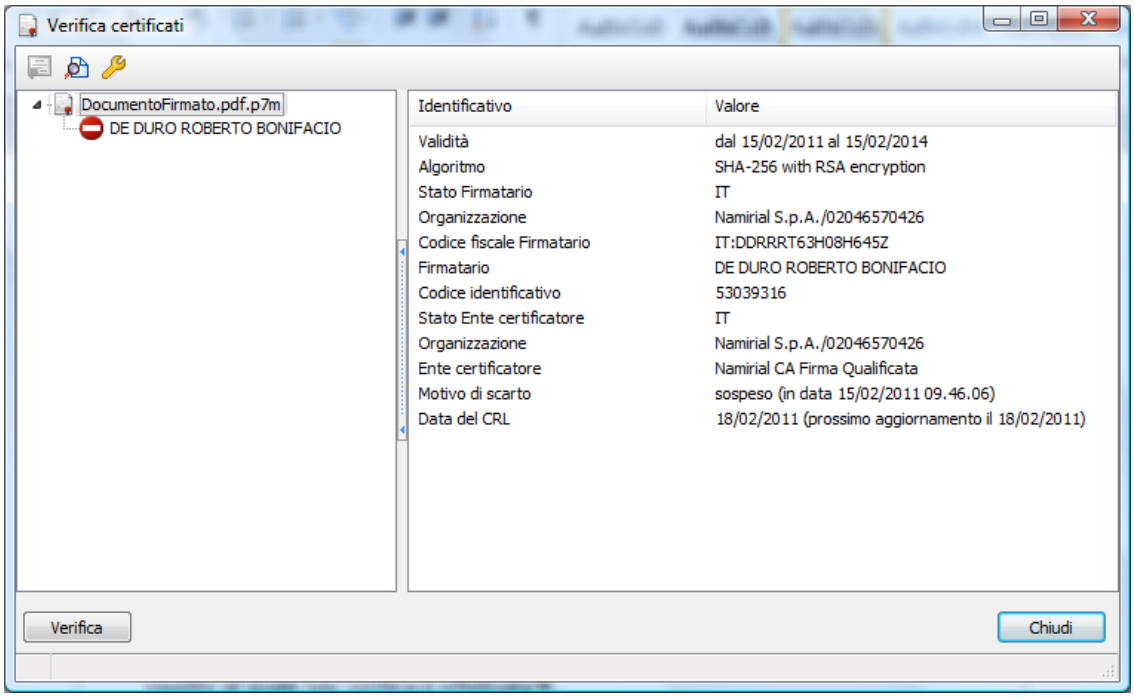
Gli stati possibili sono:

firma non verificata,

la firma non è in corso di validità,

la firma è in corso di validità.

Al termine della verifica sul lato destro sono visualizzate una serie di informazioni, tra cui Motivo della sospensione (Sospeso o Revocato) e da che data il certificato non è valido.



L'applicazione supporta la generazione e la verifica di firme multiple come richiesto dalla Deliberazione 45/2009.
Il tempo rispetto al quale è effettuata la verifica della firma è stabilito come segue:

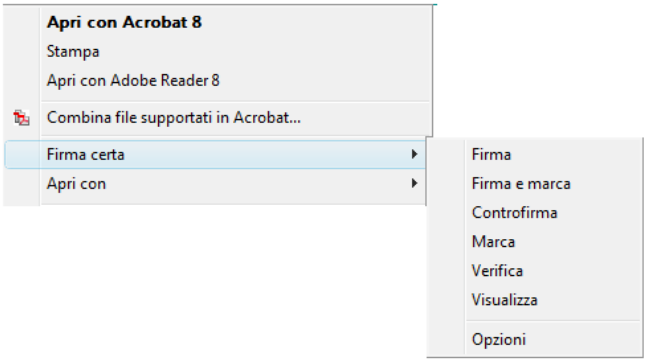
- il tempo indicato nella marca temporale associata alla firma digitale, se presente, oppure
- il tempo indicato dall'utente se fornito, oppure
- la data ed ora corrente

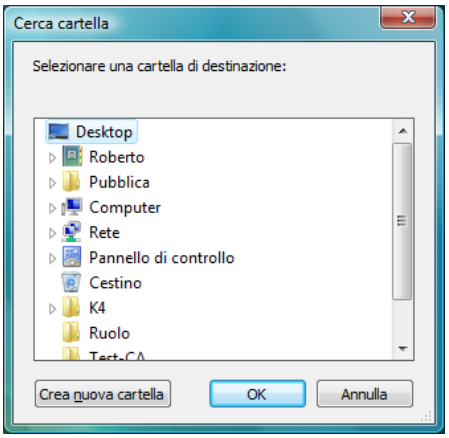
Tra le informazioni fornite nell'esito della verifica di ogni firma viene indicato il tempo rispetto al quale tale verifica è effettuata.
Il certificatore si riserva di adottare nuovi formati in conformità alle norme vigenti.

22. Modalità operative per la generazione della firma digitale 36.3.s

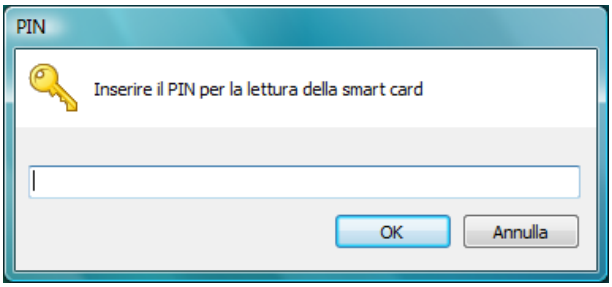
Le modalità dell' apposizione della firma digitale sono:

- Inserimento del token nell'apposito supporto:
  - se il dispositivo di firma è un token USB inserire il dispositivo in una porta USB del computer,
  - se il dispositivo di firma è una SMART CARD, inserirla nell'apposito lettore,
- posizionarsi con il mouse sul documento da firmare,
- premere il tasto destro del mouse,
- comparirà un menu,
- posizionarsi su Firma Certa → Firma





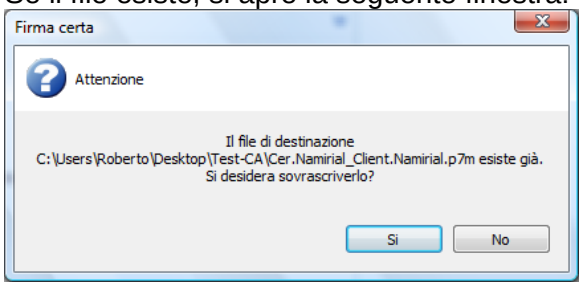
- il software chiede dove salvare il documento firmato,
- premendo sul pulsante OK si ha la seguente finestra:



- è richiesto il PIN del dispositivo di firma,
- dopo l'inserimento si preme OK.

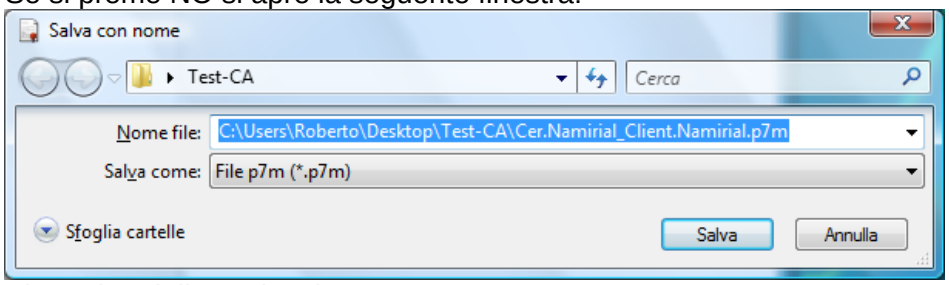
Automaticamente Firma Certa salva il documento con lo stesso nome dell'originale inserendo l'estensione .p7m.

Se il file esiste, si apre la seguente finestra:



Se si preme SI il file viene sovrascritto.

Se si preme NO si apre la seguente finestra:



Al termine della scelta si preme SALVA.

Il software di firma consente di sottoscrivere digitalmente qualsiasi tipo di file, sia in formato P7m che firmare documenti PDF lasciando l'estensione PDF.

E' disponibile sul sito del certificatore il manuale del client Firma Certa.
URL: www.firmaCerta.it nella sezione Documenti

23. Informazioni contenute nei certificati

Il presente capitolo riporta le specifiche del contenuto di tutti i tipi di Certificati emessi dal Certificatore.

23.1 Certificati di certificazione (root)

Il Certificatore emette due certificati di root, il certificato relativo alla chiave di sottoscrizione dei certificati qualificati (CA Titolari) ed uno per la sottoscrizione dei certificati dei server di marcatura temporale (CA TSA).
Il profilo di tali Certificati è conforme a quanto previsto alle norme vigenti in materia. Questo garantisce l'interoperabilità con i certificatori italiani.

IssuerDN della Namirial CA Firma Qualificata*:* (Emittente) – il campo contiene

Attributi	OID	Descrizione
commonName	2.5.4.3	Namirial CA Firma Qualificata
organizationalUnitName	2.5.4.11	Certification Authority
organizationName	2.5.4.10	Namirial S.p.A./02046570426
countryName	2.5.4.6	IT

SubjectDN della Namirial CA Firma Qualificata valorizzato come il relativo campo *IssuerDN*

IssuerDN della CA TSA*:* (Emittente) – il campo contiene

Attributi	OID	Descrizione
commonName	2.5.4.3	Namirial CA TSA
organizationalUnitName	2.5.4.11	Certification Authority
organizationName	2.5.4.10	Namirial S.p.A./02046570426
countryName	2.5.4.6	IT

SubjectDN della CA TSA valorizzato come il relativo campo *IssuerDN*

IssuerDN della CA Autenticazione*:* (Emittente) – il campo contiene

Attributi	OID	Descrizione
commonName	2.5.4.3	Namirial CA Autenticazione
organizationalUnitName	2.5.4.11	Certification Authority
organizationName	2.5.4.10	Namirial S.p.A./02046570426
countryName	2.5.4.6	IT

SubjectDN della CA Autenticazione valorizzato come il relativo campo *IssuerDN*

estensioni utilizzate per CA Titolari e CA TSA:

estensioni	OID	Contenuto
keyUsage	2.5.29.15	Contiene gli attributi *keyCertSign e cRLSign* impostati a True, tutti gli altri sono False. L'estensione è marcata critica
basicConstraints	*2.5.29.19*	*Contiene l'attributo CA=true*
certificatePolicies	2.5.29.32	contiene nel campo policyIdentifier l'OID generico previsto dall'RFC 5280 (2.5.29.32.0). L'estensione non è marcata critica
CRLDistributionPoints	2.5.29.31	URL che punta alla CRL pubblicata dal certificatore dove sarà disponibile l'informazioni relativa alla eventuale revoca del Certificato di Certificazione. L'URL configura un percorso assoluto per l'accesso alla CRL. mediante protocollo HTTP e consente lo scaricamento anonimo della CRL.. L'estensione non è marcata critica
authorityKeyIdentifier	2.5.29.35	Estensione presente e valorizzata con il campo *keyIdentifier*. L'estensione non è marcata.
subjectKeyIdentifier	2.5.29.14	Estensione presente contiene il valore *KeyIdentifier* per identificare il certificato, calcolato secondo il metodo indicato in RFC 5280. L'estensione non è marcata critica
authorityInfoAccess *accessMethod* *accessLocation*	1.3.6.1.5.5.7.1.1	Contiene un campo *accessDescription* con la descrizione delle modalità di accesso al servizio OCSP e i seguenti attributi. contiene l'identificativo *id-ad-ocsp* (OID: 1.3.6.1.5.5.7.48.1) contiene l'URI che punta all'OCSP *Responder* del certificatore, utilizzabile per effettuare la verifica del certificato stesso.

23.2 Certificato qualificato

Il profilo del Certificato Qualificato emesso dal Certificatore è conforme alle norme vigenti e, in particolare, a quanto previsto all'art.12 della Deliberazione CNIPA N. 45 del 21 maggio 2009. Questo garantisce l'interoperabilità con i certificatori italiani.

Issuer: (Emittente) – il campo contiene

Attributi	OID	Descrizione
commonName	2.5.4.3	Namirial CA Firma Qualificata
organizationalUnitName	2.5.4.11	Certification Authority
organizationName	2.5.4.10	Namirial S.p.A./02046570426
countryName	2.5.4.6	IT

SubjectDN: (Dati identificativi del titolare) – il campo contiene

Attributi	OID	Descrizione
givenName e *surname*	2.5.4.42 e 2.5.4.4	contengono rispettivamente il nome e il cognome del titolare del certificato
countryName	2.5.4.6	nel caso in cui l'*organizationName* contenga il valore "non presente", contiene il *country code* ISO 3166 dello Stato di residenza del titolare; nel caso in cui l'*organizationName* contenga un valore diverso da "non presente", contiene il *country code* ISO 3166 dello Stato che ha assegnato all'organizzazione il codice identificativo riportato nell'attributo *organizationName*
organizationName	2.5.4.10	contiene, se applicabile, la ragione sociale o la denominazione e il codice identificativo dell'organizzazione che ha richiesto o autorizzato il rilascio del certificato del titolare. Il codice identificativo è un codice rilasciato dalla competente autorità dello Stato indicato nell'attributo *countryName*. Se l'*organizationName* non è applicabile, assume il valore "non presente"
serialNumber	2.5.4.5	contiene il codice fiscale del titolare rilasciato dall'autorità fiscale dello Stato di residenza del titolare o, in mancanza, un analogo codice identificativo, quale ad esempio un codice di previdenza sociale o un codice identificativo generale. In mancanza di tale codice identificativo potrà essere utilizzato il numero del passaporto preceduto da "PASSPORT".Allo scopo di definire il contesto per la comprensione del codice in questione, il codice stesso è preceduto dal *country code* ISO 3166 e dal carattere ":"(in notazione esadecimale "0x3A").
dnQualifier	2.5.4.46	contiene il codice identificativo del titolare presso il certificatore. Detto codice, assegnato dal certificatore, è univoco nell'ambito del certificatore stesso

title	2.5.4.12	contiene una indicazione della qualifica specifica del titolare, quale l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, ovvero i poteri di rappresentanza nell'ambito dell'organizzazione specificata nell'attributo *organizationName*. Nel caso in cui l'attributo *organizationName* contenga un valore diverso da "non presente", l'inserimento delle informazioni nel *title* è richiesto dall'organizzazione ivi indicata ed il certificatore deve conservare tale richiesta per il periodo indicato nell'articolo 15, comma 7 delle regole tecniche; in caso contrario deve contenere informazioni derivanti da autocertificazione effettuata dal titolare ai sensi della normativa vigente
commonName	2.5.4.3	Contiene ripetute il Cognome e Nome del Titolare
description	2.5.4.13	Puo contenere anche il codice E.O.R.I. di cui al Regolamento CE N. 312/2009 del 16 aprile 2009. Il codice è preceduto dal testo "EORI" e dal carattere ":"(in notazione esadecimale "0x3A"). Il Codice EORI in Italia sarà rappresentato dal prefisso "IT" seguito dai numeri costituenti la partita IVA, per i soggetti IVA, dal codice fiscale di persona giuridica o dai primi 15 caratteri del C.F. per le persone fisiche
organizationalUnitName	2.5.4.11	contiene ulteriori informazioni inerenti all'organizzazione. Tale attributo può comparire, al massimo, cinque volte

estensioni:

estensioni	OID	Contenuto
keyUsage	2.5.29.15	il parametro *nonRepudiation* impostato a True, tutti gli altri sono False. L'estensione è marcata critica
certificatePolicies	2.5.29.32	contiene nel campo policyIdentifier l'*OID* della *Certificate Policy* (CP) e l'*Uniform Resource Locator (URL*) che punta al *manuale operativo* nel rispetto del quale il certificatore ha emesso il certificato e nel campo userNotice eventuali limiti d'uso del certificato. L'estensione non è marcata critica al momento della stesura del presente documento il valore è: http://www.firmacerta.it/manuali-MO/ in caso di nuove versioni la URL punterà sempre alla versione corrente.
CRLDistributionPoints	2.5.29.31	URL che punta alla CRL partizionata pubblicate dal certificatore dove saranno disponibili le informazioni relative alla eventuale revoca o sospensione del certificato in questione. L'URL configura un percorso assoluto per l'accesso alla CRL. mediante protocollo HTTP e consente lo scaricamento anonimo della CRL.. L'estensione non è marcata critica
authorityKeyIdentifier	2.5.29.35	Estensione presente e valorizzata con il campo *keyIdentifier*. L'estensione non è marcata critica
subjectKeyIdentifier	2.5.29.14	Estensione presente contiene il valore *KeyIdentifier* per identificare il certificato, calcolato secondo il metodo indicato in RFC 5280. L'estensione non è marcata critica
qcStatements	1.3.6.1.5.5.7.0.18 .3	Estensione presente, valorizzata con i campi qui di seguito.
id-etsi-qcs-QcCompliance	0.4.0.1862.1.1	Presente.
id-etsi-qcs-QcLimitValue	0.4.0.1862.1.2	presente ove è applicabile un limite nelle negoziazioni sottoscritte dal certificato, se richiesto dal Titolare o dal Terzo Interessato.
id-etsi-qcs-QcRetentionPeriod	0.4.0.1862.1.3	Presente e con valore indicato pari a "20".
id-etsi-qcs-QcSSCD	0.4.0.1862.1.4	Presente.
authorityInfoAccess	1.3.6.1.5.5.7.1.1	Contiene un campo *accessDescription* con la descrizione delle modalità di accesso al servizio OCSP e i seguenti attributi.
accessMethod		contiene l'identificativo *id-ad-ocsp* (OID:

		1.3.6.1.5.5.7.48.1) contiene l'URI che punta all'OCSP *Responder* del certificatore, utilizzabile per effettuare la verifica del certificato stesso. http://ocsp.firmacerta.it/ocsp/certstatus
accessLocation		

23.3 Certificati dei server di marcatura temporale

Il Certificatore emette il certificato di marcatura temporale, relativo alla chiave di sottoscrizione delle marche temporali, con profilo conforme alle norme vigenti e, in particolare, a quanto previsto all'art.13 e 15 della Deliberazione CNIPA N. 45 del 21 maggio 2009 e con durata pari a 11 (undici) anni.

Issuer: (Emittente) – il campo contiene

Attributi	OID	Descrizione
commonName	2.5.4.3	Namirial CA TSA
organizationalUnitName	2.5.4.11	Certification Authority
organizationName	2.5.4.10	Namirial S.p.A./02046570426
countryName	2.5.4.6	IT

SubjectDN valorizzato come segue

Attributi	OID	Descrizione
commonName	2.5.4.3	TSS – (seguito dal nome server di marcatura temporale come previsto dall'art. 45 comma 1 DPCM 30.03.2009)
organizationalUnitName	2.5.4.11	TSA
organizationName	2.5.4.10	Namirial S.p.A./02046570426
countryName	2.5.4.6	IT

estensioni:

estensioni	OID	Contenuto
keyUsage	2.5.29.15	Contiene l' attributo digital*Signature* impostato a True, tutti gli altri sono False. L'estensione è marcata critica
certificatePolicies	2.5.29.32	Contiene nel campo policyIdentifier l'*OID e* della *Certificate Policy* (CP) e *nel campo cPSuri* l'*Uniform Identifier (URI*) che punta al *manuale operativo* nel rispetto del quale il certificatore ha emesso il certificato. L'estensione non è marcata critica al momento della stesura del presente documento il valore è: http://www.firmacerta.it/manuali-MO/ in caso di nuove versioni del Manuale Operativo la URI sarà concordemente aggiornata.
CRLDistributionPoints	2.5.29.31	URL che punta alla CRL pubblicata dal certificatore dove sarà disponibile l' informazioni relativa alla eventuale revoca del Certificato di marcatura temporale. L'URL configura un percorso assoluto per l'accesso alla CRL. mediante protocollo HTTP e consente lo scaricamento anonimo della CRL.. L'estensione non è marcata critica

authorityKeyIdentifier	2.5.29.35	Estensione presente e valorizzata con il campo *keyIdentifier*. L'estensione non è marcata critica
subjectKeyIdentifier	2.5.29.14	Estensione presente contiene il valore *KeyIdentifier* per identificare il certificato, calcolato secondo il metodo indicato in RFC 5280. L'estensione non è marcata critica
extendedKeyUsage	2.5.29.37	Contenete esclusivamente il campo *keyPurposeId=timeStamping*. L'estensione è marcata critica.

23.4 Certificati del server OCSP

Il Certificatore emette il certificato relativo alla chiave di sottoscrizione temporale del responder OCSP, con profilo conforme RFC 2560

Issuer: (Emittente) – il campo contiene

Attributi	OID	Descrizione
commonName	2.5.4.3	Namirial CA Firma Qualificata
organizationalUnitName	2.5.4.11	Certification Authority
organizationName	2.5.4.10	Namirial S.p.A./02046570426
countryName	2.5.4.6	IT

SubjectDN valorizzato come segue

Attributi	OID	Descrizione
commonName	2.5.4.3	OCSP server
organizationalUnitName	2.5.4.11	Certification Authority
organizationName	2.5.4.10	Namirial S.p.A./02046570426
countryName	2.5.4.6	IT

estensioni:

estensioni	OID	Contenuto
keyUsage	2.5.29.15	Contiene l' attributo digital*Signature* impostato a True, tutti gli altri sono False. L'estensione è marcata critica
certificatePolicies	2.5.29.32	Contiene nel campo policyIdentifier l'*OID e* della *Certificate Policy* (CP) e *nel campo cPSuri* l'*Uniform Identifier (URI*) che punta al *manuale operativo* nel rispetto del quale il certificatore ha emesso il certificato. L'estensione non è marcata critica al momento della stesura del presente documento il valore è: http://www.firmacerta.it/namirial-MO.
CRLDistributionPoints	2.5.29.31	URL che punta alla CRL pubblicata dal certificatore dove sarà disponibile l'informazioni relativa alla eventuale revoca del Certificato di marcatura temporale. L'URL configura un percorso assoluto per l'accesso alla CRL. mediante protocollo HTTP e consente lo scaricamento anonimo della CRL.. L'estensione non è marcata critica
authorityKeyIdentifier	2.5.29.35	Estensione presente e valorizzata con il campo *keyIdentifier*. L'estensione non è marcata critica
subjectKeyIdentifier	2.5.29.14	Estensione presente contiene il valore *KeyIdentifier* per identificare il certificato, calcolato secondo il metodo indicato in RFC 5280. L'estensione non è marcata critica
extendedKeyUsage	2.5.29.37	Contenete esclusivamente il campo *keyPurposeId=id-kp-OCSPSigning*. L'estensione è marcata critica.

24. Macro e Comandi [40]

Il Titolare deve tener presente che macro istruzioni o codici eseguibili presenti all'interno del documento che modifichino gli atti ed i fatti rappresentati nel documento stesso invalidano la firma (Art.3, comma 3 del [5]).E' cura del Titolare assicurarsi, tramite le funzionalità tipiche di ogni procedura, dell'assenza di codici eseguibili sopra descritti.

Di seguito riportiamo le linee guide sugli applicativi di maggiore diffusione, che non vogliono essere esaustive. Per i dettagli è necessario far riferimento ai manuali d'uso forniti a corredo delle applicazioni.

MS Word® 2003 e MS Excel® 2003
Per disattivare le macro seguire la seguente procedura:

- Selezionare tutto il testo e quindi premere contemporaneamente i tasti ctrl+shift+F9

MS Word® 2007 e MS Excel® 2007
Per disattivare le macro seguire i seguenti passi:

- cliccare sul pulsante Office,
- cliccare sul Opzioni,
- cliccare su Centro protezione ,
- posizionarsi su Impostazioni Centro protezione,
- Cliccare su Disattiva tutte le macro con notifica

Adobe Acrobat®
Per disattivare le funzioni di esecuzione di codice JavaScript seguire i passi:

- Cliccare su Modifica,
- Cliccare su Preferenze,
- JavaScript.