Manuale Operativo

Servizi di Certificazione e Marcatura Temporale

Categoria	**Certification Authority**	Codice Documento	**NAM-MO-FDMT**	**Namirial S.p.A.**
Redatto da	**Simone Baldini**	Nota di riservatezza	**Documento Pubblico**	Il Legale Rappresentante
Verificato da	**Giuseppe Benedetti**	Versione	**2.4**	**Davide Ceccucci**
Approvato da	**Davide Ceccucci**	Data di emissione	**14/06/2018**	CECCUCCI DAV

2018.06.15 16:30:29
CN=CECCUCCI DAVIDE
C=IT
O=NAMIRIAL S.p.A.
2.5.4.97=VATIT-02046570
RSA/2048 bits

Namirial S.p.A.

Sede legale, direzione e amministrazione 60019 Senigallia (AN) - via Caduti sul Lavoro, 4
C.F./ISCR. REG. IMPR. ANCONA N.02046570426 - P.I. IT02046570426 - CAP. SOC. € 6.500.000,00 i.v.
Tel. 07163494 s.a. - Fax 199.418016 - info@namirial.com - www.namirial.com

– Questa pagina è lasciata intenzionalmente in bianco –

INDICE

INDICE DELLE TABELLE

STORIA DELLE MODIFICHE

VERSIONE	**2.3**
Data	30/06/2017
Motivazione	Revisione
Modifiche	Revisione del documento per adeguamento al Reg. (UE) 679/2016 §6.1 Aggiornato il DPO §6.2 Aggiornati i diritti degli interessati

VERSIONE	**2.3**
Data	30/06/2017
Motivazione	Aggiornamento
Modifiche	- Inserimento nuova CA per rilascio Certificati Qualificati per Firma elettronica e Sigillo Elettronico

VERSIONE	**2.2**
Data	30/05/2017
Motivazione	Aggiornamento
Modifiche	- Inserimento rilascio Certificati Qualificati per Sigillo Elettronico

VERSIONE	**2.1**
Data	23/05/2017
Motivazione	Aggiornamento
Modifiche	- Inserimento modalità di rilascio busta cartacea con certificati attivi

VERSIONE	**2.0**
Data	12/12/2016
Motivazione	Aggiornamento
Modifiche	Inserimento della modalità di rilascio self-enroll con identificazione presso IR e dispositivo fornito dal Certificatore

VERSIONE	**1.91**
Data	08/07/2016
Motivazione	Aggiornamento
Modifiche	Aggiornamento OID Timestamp Authority

VERSIONE	**1.9**
Data	15/06/2016
Motivazione	Aggiornamento
Modifiche	Aggiornamento in seguito al recepimento del regolamento eIDAS

VERSIONE	**1.8**
Data	08/10/2015
Motivazione	Aggiornamento
Modifiche	Aggiornamento circa le modalità di identificazione e registrazione dell'utente (§ 5.2 e ss.gg.)

VERSIONE	**1.7**
Data	01/07/2014
Motivazione	Aggiornamento
Modifiche	Aggiornamento ai Limiti d'uso e Certificate Policies (§ 4.3, § 0). Aggiunte tipologie di firme al § 5.10. Modificata la procedura di rinnovo al § 5.9.1. Correzione di alcuni refusi all'interno del documento. Modificata la procedura di modalità di consegna dei dispositivi di firma personali e dei codici segreti al § 5.5 e la modalità di visualizzazione della busta cieca digitale al §**Errore. L'origine riferimento non è stata trovata.**.

VERSIONE	**1.6**
Data	31/10/2013
Motivazione	Aggiornamento
Modifiche	Sostituzione riferimenti articoli DPCM 30/03/2009 con DPCM 22/02/2013. Aggiornamento agli obblighi delle LRA (§ 3.4). Aggiornamento policy certificati (§ 4.1). Aggiornamento alla procedura per la visualizzazione della busta cieca digitale (§ 5.4.7.1). Aggiornamento della procedura di identificazione via webcam (§ 5.2.1).

VERSIONE	**1.5**
Data	01.10.2013
Motivazione	Aggiornamento
Modifiche	Rivisitazione generale del documento. Introduzione delle procedure operative per la firma automatica/remota. Modifica della procedura di rinnovo. Introduzione del riconoscimento via webcam.

VERSIONE	**1.41**
Data	20.02.2013
Motivazione	Aggiornamento
Modifiche	Cap. 1 Versioni e Riferimenti Cap. 2 Generalità. Cap. 13 Modalità di identificazione e registrazione dell' utente. Cap. 17 Modalità di consegna della busta cieca. Cap. 26 Macro e Comandi.

VERSIONE	**1.3**
Data	07.03.2011
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	**1.2**
Data	10.01.2011
Motivazione	Aggiornamento
Modifiche	Cap. 21 Modalità operative per l'utilizzo del software di verifica delle firme.

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 INTRODUZIONE

1.1 SCOPO E CAMPO DI APPLICAZIONE

Il presente documento rappresenta il **Manuale Operativo del servizio di certificazione digitale erogato da Namirial S.p.A** (CP e CPS per il regolamento eIDAS) e ha come scopo la descrizione delle regole e delle procedure operative adottate da Namirial per tutte le attività inerenti l'emissione e la gestione dei certificati di sottoscrizione qualificati e delle marche temporali.

Questo documento, a partire dal 1 Luglio 2016, diventa parte integrante del documento Trust Services Practice Statement che descrive le procedure operative per i servizi qualificati come previsto dal regolamento eIDAS (electronic IDentification Authentication and Signature) UE n° 910/2014 sull'identità digitale.

La documentazione del Certificatore è organizzata secondo i principi dello standard ETSI EN 319 serie 400, pertanto viene suddivisa nel seguente modo:

1. NAMIRIAL Trust Services Practice Statement (NAMIRIAL PS) descrive le procedure generali adottate dal Certificatore nell'erogazione dei servizi qualificati;
2. parti specifiche relative al servizio di certificazione (es. policy dei certificati, procedure di identificazione, modalità operative del servizio specifico, etc.) sono descritte nel manuale operativo del servizio (il presente documento), in conformità alle norme nazionali;
3. parti specifiche relative al servizio di marcatura temporale sono descritte nel documento Time-Stamping Authority Practice Statement, che è parte integrante del presente documento.

In caso di conflitto tra le dichiarazioni contenute nei documenti in lingua inglese ed il presente documento, il documento originale in lingua inglese prevarrà.

La disciplina e le indicazioni contenute nel presente documento si applicano anche ai certificati qualificati di firma digitale emessi da Namirial per essere installati sulle CNS (Carta Nazionale dei Servizi) su richiesta delle Pubbliche Amministrazioni emittenti (Enti Emittenti).

Per casi o soggetti particolari, per i quali si rendessero necessari obblighi/regole e/o procedure operative specifiche, vengono rilasciati ulteriori documenti come "addendum".

1.2 RIFERIMENTI TECNICI E NORMATIVI

Il Certificatore, nell' erogazione dei suoi servizi, è conforme alle normative e regolamenti europei e nazionali applicabili. Tutti i regolamenti e le leggi applicabili sono riportati nella seguente tabella ed al personale del Certificatore, e a chi collabora a vario titolo con lo stesso, vengono fornite adeguate policy per il rispetto di tali norme e regolamenti.

NUM	NORMATIVA	DESCRIZIONE
[01]	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.*
[02]	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*
[03]	D.Lgs. 82/2005	Decreto Legislativo 7 marzo 2005, n. 82 *Codice dell'Amministrazione Digitale (CAD)*, con le modifiche ed integrazioni stabilite dal decreto legislativo 26 agosto 2016, n. 179.
[04]	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.*
[05]	DPCM 22/02/2013	Decreto del Presidente del Consiglio dei Ministri 22 Febbraio 2013. *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.*
[06]	Reg (UE) 679/2016	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
[07]	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*
[08]	CNIPA 45/2009	CNIPA Deliberazione n. 45 del 21 maggio 2009 e successive modificazioni. *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.*
[09]	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
[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

NUM	NORMATIVA	DESCRIZIONE
[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.
[18]	D.Lgs. 231/2007	"Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attivita' criminose e di finanziamento del terrorismo nonche' della direttiva 2006/70/CE che ne reca misure di esecuzione".
[19]	D. Lgs. 22 giugno 2012, n. 83	Misure urgenti per le infrastrutture l'edilizia ed i trasporti. art. 22 DigitPA e l'Agenzia per la diffusione delle tecnologie per l'innovazione sono soppressi. I due enti confluiscono nell' Agenzia per l'Italia Digitale.
[20]	RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.
[21]	RFC 3161	Internet X.509 Public key infrastructure Time Stamp Protocol (TSP) PKIW Working Group IETF - Agosto 2001.
[22]	DM 9/12/2004	Decreto del Ministero dell'Interno, del Ministro per l'innovazione e le tecnologie e del Ministro dell'economia e delle finanze 9 Dicembre 2004. *Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta Nazionale dei Servizi" pubblicato nella Gazzetta Ufficiale n.296, 18 dicembre 2004.*
[23]	ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[24]	ETSI EN 319 421	Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
[25]	ETSI EN 319 422	Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
[26]	ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[27]	ETSI EN 319 411-2	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
[28]	ETSI EN 319 411-3	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates
[29]	ETSI EN 319 412-1	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
[30]	ETSI EN 319 412-2	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

NUM	NORMATIVA	DESCRIZIONE
[31]	ETSI EN 319 412-3	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
[32]	ETSI EN 319 412-4	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates
[33]	ETSI EN 319 412-5	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[34]	eIDAS n. 910/2014	Regolamento eIDAS (electronic IDentification Authentication and Signature) UE n° 910/2014 sull'identità digitale.
[35]	eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[36]	QSCD	COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
[37]	TSL	COMMISSION IMPLEMENTING DECISION (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
[38]	Electronic Signature Formats	COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

Tabella 1: Riferimenti tecnici e normativi

1.3 DEFINIZIONI ED ACRONIMI

Sono qui riportati i significati di acronimi e di termini specifici, fatti salvi quelli di uso comune.

TERMINE O ACRONIMO	SIGNIFICATO
AgID	Agenzia per Italia Digitale [19].
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). Vedi [01] Art.28

TERMINE O ACRONIMO	SIGNIFICATO
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.
Chiave 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.
Chiave 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.
CIE	Carta d'Identità Elettronica, è il documento di identificazione destinato a sostituire la carta d'identità cartacea sul territorio italiano.
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.
CNS	Carta Nazionale dei Servizi
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.
CRS	Carta regionale dei servizi
CUC	È 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	È 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.
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	È la persona fisica o giuridica delegata dal Certificatore allo svolgimento delle operazioni di emissione dei Certificati, secondo le modalità individuate e descritte nel presente Manuale. L'ente deve aver preventivamente stipulato accordi di servizio con il Certificatore. L'LRA può avvalersi di RAO per le operazioni identificazione, registrazione ed emissione.
Marca temporale [Timestamp]	È il riferimento temporale che consente la validazione temporale.
Manuale Operativo	È il documento pubblico depositato presso AgID 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.

TERMINE O ACRONIMO	SIGNIFICATO
OCSP [Online Certificate Status Protocol]	È un protocollo che consente di verificare la validità di un certificato in tempo reale.
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.
OTP	One-Time-Password. Codice numerico generato da un dispositivo fisico utilizzato per effettuare un'autenticazione a due fattori.
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 Authority, soggetto che esegue l'identificazione dei Richiedenti dei certificati qualificati applicando le procedure definite dal Certificatore.
RAO	È soggetto espressamente delegato da Namirial allo svolgimento, per conto di quest'ultima, delle Operazioni di identificazione e registrazione del Titolare, nonché l'emissione dei Certificati. Tale soggetto deve appartenere ad una LRA.
Referente	È la persona fisica incaricata alla predisposizione di ogni documento necessario per il ciclo di vita della firma e che 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.
RSA	Algoritmo di crittografia asimmetrica, basato su chiavi pubbliche e private.
SHA-1 [Secure Hash Algorithm]	Algoritmo di crittografia che genera una impronta digitale di 160 bit.
SHA-256 [Secure Hash Algorithm]	Algoritmo di crittografia che genera una 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 dà 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 risultano modificati i requisiti in base ai quali lo stesso è stato rilasciato
Titolare	È la persona fisica, identificata dal Certificatore, cui è attribuita la firma digitale.
Token	È il dispositivo fisico (smart card, o chiave USB) che contiene la chiave privata del Titolare.
X.509	È uno standard ITU-T per le infrastrutture a chiave pubblica (PKI)

Tabella 2: Definizioni e Acronimi

1.4 TABELLA DI CORRISPONDENZA

La seguente tabella incrocia i temi previsti dal Art. 40, comma 3) del [05] con le corrispondenti sezioni del presente documento.

Art. 40, comma 3) del DPCM 22 febbraio 2013		Manuale Operativo
a	dati identificativi del certificatore	2.1
b	dati identificativi della versione del manuale operativo	2.4
c	responsabile del manuale operativo	2.6
d	definizione degli obblighi del certificatore, del titolare e dei richiedenti le informazioni per la verifica delle firme	3.2
e	definizione delle responsabilità e delle eventuali limitazioni agli indennizzi	3.3
f	indirizzo del sito web del certificatore ove sono pubblicate le tariffe	3.5
g	modalità di identificazione e registrazione degli utenti	5.2
h	modalità di generazione delle chiavi per la creazione e la verifica della firma	5.3
i	modalità di emissione dei certificati	5.4
l	modalità di inoltro delle richieste e della gestione di sospensione e revoca dei certificati	5.8
m	modalità di sostituzione delle chiavi	5.9
n	modalità di gestione del registro dei certificati	4.5.2
o	modalità di accesso al registro dei certificati	4.5.1
p	modalità per l'apposizione e la definizione del riferimento temporale	5.11
q	modalità di protezione dei dati personali	3.4
r	modalità operative per l'utilizzo del sistema di verifica delle firme di cui all'art. 14, comma 1	5.10
s	modalità operative per la generazione della firma elettronica qualificata e della firma digitale	5.10

2 IL CERTIFICATORE

2.1 DATI IDENTIFICATIVI DEL CERTIFICATORE[(A)]

Ai sensi del [03] e successive modifiche, Namirial S.p.A. è **Certificatore Accreditato** che emette, pubblica nel registro e revoca Certificati Qualificati (o Certificati di Sottoscrizione) e CNS, in conformità alle regole tecniche vigenti. Il Certificatore è identificato come riportato nella seguente tabella.

Ragione Sociale:	**Namirial S.p.A.**
Sede Legale:	VIA CADUTI SUL LAVORO, 4 60019 - SENIGALLIA (AN) TEL: 071.63494 FAX: 071.60910
Sede di erogazione del servizio:	VIA CADUTI SUL LAVORO, 4 60019 - SENIGALLIA (AN) TEL: 071.63494 FAX: 071.60910
Partita IVA:	IT02046570426
Iscrizione registro delle imprese:	Ancona
REA:	02046570426
Capitale sociale:	6.500.000 € I.V.
Sito web del servizio:	http://www.firmacerta.it
URL del Portale utente:	https://cms.firmacerta.it/areaPrivata
Sito web del certificatore:	http://www.namirial.com
Email del servizio (PEC):	firmacerta@sicurezzapostale.it
Email del certificatore:	firmacerta@namirial.com

Tabella 3: Dati identificativi del Certificatore

2.2 DESCRIZIONE SINTETICA DI NAMIRIAL S.P.A.

Namirial S.p.A. è una società di informatica e web engineering che ha trovato una propria specifica collocazione all'interno dell'Information Technology orientando la propria produzione di software verso le nuove e sempre più manifeste esigenze di adeguamento del sistema produttivo italiano ai nuovi scenari economici fortemente competitivi e globalizzati.
All'interno di una struttura economica nazionale caratterizzata per la gran parte dall'attività di piccole e medie realtà imprenditoriali si è ritenuto essenziale sviluppare soluzioni e servizi software accessibili anche sulla rete internet ed in grado

di rispondere alle problematiche tecnologico-innovative emergenti in maniera professionale mantenendo una grande economicità di esercizio.
La società ha sede in una moderna struttura di oltre duemila metri quadrati, dove è operativo un *Internet Data Center* dotato di tutti i sistemi di sicurezza necessari all'inviolabilità della struttura ed in grado di supportare gli utenti anche per quanto concerne eventuali necessità di hosting, housing e in genere di server farm.

Namirial S.p.A. è:

Autorità di Certificazione accreditata presso AgID (ex DigitPA) ed è autorizzata all'emissione di certificati qualificati conformi alla Direttiva Europea 1999/93/CE, Certificati CNS e Marche Temporali.

Gestore di PEC, dal 26/02/2007, accreditato presso AgID (ex DigitPA) ed autorizzato alla gestione di **caselle** e **domini** di Posta Elettronica Certificata.

Certificata UNI EN ISO 9001:2008. Namirial ha conseguito il certificato n. 223776 rilasciato da **Bureau Veritas Italia S.p.A.**

Certificata ISO/IEC 27001:2013. Namirial ha conseguito il certificato n. IT280490 rilasciato da **Bureau Veritas Italia S.p.A.**

Certificata da Adobe. Da giugno 2013 Namirial è **membro dell'AATL** (Adobe Approved Trust List).

2.2.1 CERTIFICAZIONE ISO 9001

Namirial S.p.A. ha conseguito il certificato ISO 9001:2000 n. 223776 presso la Bureau Veritas Italia S.p.A. in data 28/11/2007. Lo stesso certificato è stato rinnovato in data 14.11.2013 ed è disponibile al seguente link:
http://download.namirial.com/certifications/cert-namirial-bv-iso9001-223776.pdf

2.2.2 CERTIFICAZIONE ISO/IEC 27001:2013

Namirial S.p.A. ha ottenuto la certificazione UNI EN ISO 27001:2013 in data 19.03.2012. Namirial ha conseguito il certificato n. IT280490 presso la Bureau Veritas Italia S.p.A. che l'ha giudicata conforme ai requisiti della norma ISO/IEC 27001:2013. Il certificato è disponibile al seguente link:
http://download.namirial.com/certifications/cert-namirial-bv-isotec-27001-2013-ind15-0059u.pdf

2.2.3 CERTIFICAZIONE AATL

La Certification Authority Namirial, da giugno 2013, è inserita nell'elenco AATL (Adobe Approved Trust List).

2.3 CONTATTI COMMERCIALI E HELPDESK

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

telefono: (+39) 071 63494
e-Mail: commerciale@firmacerta.it
web: http://www.firmacerta.it

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

telefono: (+39) 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 **15.00** alle **19.00**.

2.4 VERSIONE DEL DOCUMENTO(B)

Il presente documento denominato "NAMIRIAL-FDMT-MO" è identificato attraverso il livello di revisione e la data di rilascio presente su tutte le pagine. Nel preambolo del documento è inoltre riportato un paragrafo con la storia delle modifiche apportate.

Il Certificatore esegue, almeno una volta all'anno, 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.

2.5 PUBBLICAZIONE DEL DOCUMENTO

Il presente documento e gli eventuali ulteriori documenti rilasciati per soggetti e casi particolari, come *addendum* al Manuale Operativo, sono pubblicati dal Certificatore e da AgID e sono consultabili, per via telematica, ai seguenti indirizzi internet (ai sensi dell'art.40 comma 2 del [05]):

http://www.firmacerta.it/manuali-MO

Tale URI è indicata nel campo *cSPuri* dell'estensione "Certificate Policies" dei certificati qualificati, dei server di Marcatura Temporale e OCSP.
Il documento è pubblicato in formato PDF firmato, in modo tale da assicurarne l'origine e l'integrità.

2.6 RESPONSABILE DEL DOCUMENTO(C)

La responsabilità del presente Manuale Operativo è del Certificatore, nella figura del "Responsabile del servizio di certificazione e validazione temporale" (art. 40 comma 3 lettera c) del [05]), il quale ne cura la stesura, la pubblicazione e l'aggiornamento.

Le comunicazioni riguardanti il presente documento possono essere inviate all'attenzione del suddetto responsabile contattabile mediante i seguenti recapiti:

E-mail: firmacerta@namirial.com
Telefono: (+39) 071 63494
Fax: (+39) 071 60910

3 REGOLE GENERALI

3.1 ATTORI COINVOLTI NEI PROCESSI

Gli attori indicati nel presente documento sono:

- il Certificatore (**CA**)
- la Registration Authority (**RA**)
- la Local Registration Authority (LRA)
- l'Operatore della Registration Authority (RAO)
- il Titolare (Soggetto a cui è intestato il certificato **Subject**)
- il Terzo Interessato (Organizzazione associata al Titolare)
- il Richiedente (Colui che sottopone la richiesta di certificazione alla CA ed assolve alle fasi di identificazione e registrazione **Subscriber**)
- il Destinatario (**Relying party**)
- l'Incaricato alla Registrazione (IR)

3.2 OBBLIGHI DEL CERTIFICATORE, DEL TITOLARE E DEI RICHIEDENTI LA VERIFICA DELLE FIRME (D)

3.2.1 OBBLIGHI DEL CERTIFICATORE

Il Certificatore Namirial S.p.A:

1. si attiene alla normativa vigente in materia di Firma Digitale [03][05][08][17] e successive modificazioni ed al regolamento [34];
2. provvede con certezza all'identificazione del Richiedente e del Titolare;
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 e 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 [03], nel rispetto del [06], 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 ovvero 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 [05] 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 AgID, dei certificati relativi alle chiavi di Certificazione di cui al [05];
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 [06].

3.2.2 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/o OTP) 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. mantenere in modo esclusivo e conservare con la massima diligenza il dispositivo OTP eventualmente fornito;
6. non utilizzare la firma qualificata per funzioni e finalità diverse da quelle per la quale è stata rilasciata;
7. 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;
8. 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;
9. richiedere l'immediata revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi di firma di cui abbia perduto il possesso o difettosi;

10. inoltrare, con le modalità indicate dal Certificatore, la richiesta di revoca specificandone la motivazione e la sua decorrenza;
11. sporgere denuncia, in caso di smarrimento o sottrazione del dispositivo di firma, alle autorità competenti;
12. presentarsi presso l'LRA o dal Certificatore a seguito della richiesta di sospensione del certificato per richiedere, ove del caso, la revoca dello stesso con l'apposito modulo;
13. utilizzare esclusivamente dispositivi di firma indicati ovvero forniti dal certificatore in modo conforme a quanto indicato nel presente manuale;
14. adottare idonee misure di sicurezza (es. anti-virus / anti-malware) al fine di prevenire un utilizzo fraudolento dei dispositivi di firma.

3.2.3 OBBLIGHI DEI RICHIEDENTI LA VERIFICA DELLE FIRME

Coloro che verificano firme digitali generate con chiavi certificate da NAMIRIAL sono tenuti 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;
5. l'integrità del documento ricevuto, tramite un software di verifica conforme alla normativa vigente.

3.2.4 OBBLIGHI DEL TERZO INTERESSATO

Il Terzo Interessato è tenuto a:

1. provvedere, previo esplicito consenso dei richiedenti, a raccogliere i dati necessari alla registrazione, nella forma richiesta dal Certificatore;
2. 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. comunicare tempestivamente al certificatore ogni modifica delle circostanze indicate al momento del rilascio del certificato rilevanti ai fini del suo utilizzo;
4. 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).

3.2.5 OBBLIGHI DELLA REGISTRATION AUTHORITY LOCALE (LRA)

La LRA per mezzo dei RAO è tenuta 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. informare il Titolare riguardo agli obblighi da quest'ultimo assunti in merito a conservare con la massima diligenza il dispositivo OTP eventualmente fornito;
4. richiedere, quando previsto e prima di rilasciare il certificato, la prova del possesso della chiave privata e verificare la correttezza della coppia di chiavi;

5. informare il titolare delle misure di sicurezza adottate per il trattamento dei dati personali, ai sensi del [06];
6. provvedere con certezza all'identificazione della persona che fa richiesta della certificazione;
7. accertare l'autenticità della richiesta di certificazione;
8. 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;
9. verificare ed inoltrare al Certificatore le richieste di revoca/sospensione richieste dal Titolare presso LRA;
10. attenersi scrupolosamente alle regole impartite dal Certificatore e presenti su questo documento;
11. informare il titolare riguardo gli obblighi circa la procedura da seguire per l'emissione di chiavi in Self-Enrollment (§ 5.4.5.2)

Nei casi in cui la Local Registration Authority sia costituita presso uno tra i particolari organi della PA, quali ad esempio le Forze Armate e Forze dell'Ordine, su richiesta espressa della medesima, le attività e responsabilità di raccolta e archiviazione dei dati di cui al punto 8) potranno essere gestite direttamente dalla LRA.

I RAO sono autorizzati ad operare dal Certificatore a seguito di adeguato addestramento del personale addetto. Il Certificatore, salvo diritto di rivalsa, resta comunque l'unico ed il solo responsabile verso terzi dell'attività svolta dall'LRA.

Il Certificatore verifica periodicamente la rispondenza delle procedure adottate dalla LRA e dai suoi RAO e quanto indicato nel presente documento. In ogni caso, a semplice richiesta del Certificatore, la LRA è tenuta a trasmettere allo stesso tutta la documentazione in proprio possesso, relativa a ciascuna richiesta di emissione dei certificati di sottoscrizione proveniente da ciascun Titolare.

3.3 RESPONSABILITÀ E LIMITAZIONI AGLI INDENNIZZI (E)

3.3.1 LIMITAZIONI DI RESPONSABILITÀ DEL CERTIFICATORE

Il Certificatore è responsabile, verso i Titolari, per l'adempimento degli obblighi di legge derivanti dalle attività previste dal [03], [04], [05], [06], [07], [08], [17] e successive modifiche ed integrazioni.
Il Certificatore, ove previsto, mette a disposizione del Titolare un apposito kit configurato secondo due modalità alternative:

- Dispositivo sicuro di firma (smart card, Token SIM USB o Micro SD) completo di Certificato di firma e del software, accuratamente testato, per l'apposizione e la verifica delle firme qualificate.

- Dispositivo sicuro di firma (smart card, Token SIM USB o Micro SD) non personalizzato (senza chiavi di sottoscrizione), procedura di personalizzazione del dispositivo e software, accuratamente testato, per l'apposizione e la verifica delle firme qualificate (art 7 -11)

Il Certificatore non assume responsabilità:

- per l'uso improprio dei certificati emessi;
- per le conseguenze derivanti dalla non conoscenza o dal mancato rispetto, da parte del Titolare, delle procedure e delle modalità operative indicate nel presente documento;
- per il mancato adempimento degli obblighi previsti a suo carico dovuto a cause ad esso non imputabili;

3.3.2 LIMITAZIONI E INDENNIZZI

Ai sensi dell'art. 57, comma 2 del [05] 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.

3.4 TUTELA DEI DATI PERSONALI (Q)

Le politiche di accesso ai dati sono conformi alle misure minime di sicurezza per il trattamento dei dati personali indicate nel [06] 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 esplicitofornito dal Titolare.

3.5 TARIFFE (F)

Le tariffe del servizio sono pubblicate sul sito www.firmacerta.it nella sezione Shop o disponibili presso gli Uffici di Registrazione.

4 POLICY, LIMITI D'USO E GESTIONE DEI CERTIFICATI

4.1 CERTIFICATE PROFILE

Come richiesto dalla normativa Italiana, l'emissione di certificati di firma digitale o di marca temporale avviene utilizzando direttamente i seguenti certificati CA radice:

Nome CA Radice	Scopo	Note
Namirial Qualified eSignature	Emissione certificati per firma digitale	Certificato CA Root
Namirial CA Firma Qualificata	Emissione certificati per firma digitale	Certificato CA Root
Namirial EU Qualified eSignature	Emissione certificati qualificati per firma elettronica	Certificato CA Root
Namirial EU Qualified CA	Emissione certificati qualificati per firma elettronica e sigillo elettronico	Certificato CA Root
Namirial Time Stamping Authority	Emissione certificati per marca temporale	Certificato CA Root
Namirial CA TSA	Emissione certificati per marca temporale	Certificato CA Root

Tabella 4: Certificate profile

4.1.1 CERTIFICATI CA ROOT PER FIRMA ELETTRONICA QUALIFICATA

4.1.1.1 CERTIFICATO NAMIRIAL QUALIFIED ESIGNATURE

Field	Value
Version	2 (V3)
Serial Number	6B 5C EB 57 2D DF 17 C2
Signature	RSA/SHA-256
Hash Algorithm	SHA-256
Issuer/Subject DN	C = IT, O = Namirial S.p.A., OU = Namirial Trust Service Provider, CN = Namirial Qualified eSignature
Valid from	21/6/2016 09:48:58
Valid To	21/6/2036 09:48:58

Public Key	RSA 2048 bits

Tabella 5: Certificato Namirial Qualified eSignature

Estensioni:

Field	OID	Critical	Value
subjectKeyIdentifier/ authorityKeyIdentifier	2.5.29.14	No	91 ED 9F DD 08 23 45 E5 08 90 52 4A 23 03 02 08 6C F1 AC AB
keyUsage	2.5.29.15	Yes	keyCertSign, cRLSign
basicConstraints	2.5.29.19	Yes	True (CA, Undefined Maximum Path Length)
certificatePolicies	2.5.29.32	No	2.5.29.32.0 (Any Policy)
cRLDistributionPoints	2.5.29.31	No	http://crl.namirialtsp.com/QES.crl
authorityInfoAccess	1.3.6.1.5.5.7.1.1	No	OCSP (1.3.6.1.5.5.7.48.1) http://ocsp.namirialtsp.com/ocsp/certstatus
ocspNoCheck	1.3.6.1.5.5.7.48.1.5	No	

4.1.1.2 CERTIFICATO NAMIRIAL CA FIRMA QUALIFICATA

Field	Value
Version	2 (V3)
Serial Number	41 58 C1 3A 49 D2 98 19
Signature	RSA/SHA-256
Hash Algorithm	SHA-256
Issuer/Subject DN	CN = Namirial CA Firma Qualificata, OU = Certification Authority, O = Namirial S.p.A./02046570426, C = IT
Valid from	24/11/2010 17:01:29
Valid To	24/11/2030 17:01:29
Public Key	RSA 2048 bits

Tabella 6: Certificato Namirial CA Firma Qualificata

Estensioni:

Field	OID	Critical	Value

subjectKeyIdentifier/ authorityKeyIdentifier	2.5.29.14	No	63 FD ED E6 8C 62 47 48 CF EA 09 41 73 76 11 E2 64 62 7B 10
keyUsage	2.5.29.15	Yes	keyCertSign, cRLSign
basicConstraints	2.5.29.19	Yes	True (CA, Undefined Maximum Path Length)
certificatePolicies	2.5.29.32	No	2.5.29.32.0 (Any Policy)
cRLDistributionPoints	2.5.29.31	No	URL=http://crl.firmacerta.it/FirmaCertaQualificata1.crl
authorityInfoAccess	1.3.6.1.5.5.7.1.1	No	OCSP (1.3.6.1.5.5.7.48.1) http://ocsp.firmacerta.it/ocsp/certstatus

4.1.1.3 CERTIFICATO NAMIRIAL EU QUALIFIED ESIGNATURE

Field	Value
Version	2 (V3)
Serial Number	21 0d 6c b1 7c 11 0b 9b
Signature	RSA/SHA-256
Hash Algorithm	SHA-256
Issuer/Subject DN	CN = Namirial EU Qualified eSignature, OU = Trust Service Provider, O = Namirial S.p.A., OrgID= VATIT-02046570426 C = IT
Valid from	24/11/2010 17:01:29
Valid To	24/11/2030 17:01:29
Public Key	RSA 4096 bits

Tabella 7: Certificato Namirial CA Firma Qualificata

Estensioni:

Field	OID	Critical	Value
subjectKeyIdentifier/ authorityKeyIdentifier	2.5.29.14	No	30 45 db 26 02 3d bf 0d 9a d8 b8 10 ea 7c cd a4 ae 8e 5c 27
keyUsage	2.5.29.15	Yes	keyCertSign, cRLSign
basicConstraints	2.5.29.19	Yes	True (CA, Undefined Maximum Path Length)
certificatePolicies	2.5.29.32	No	1.3.6.1.4.1.36203.1.1 (https://docs.namirialtsp.com/)
cRLDistributionPoints	2.5.29.31	No	URL=http://crl.namirialtsp.com/QES4K.crl

4.1.2 CERTIFICATI CA ROOT PER TSA

4.1.2.1 CERTIFICATO NAMIRIAL TIME STAMPING AUTHORITY

Field	Value
Version	2 (V3)
Serial Number	71 AA 6D 05 CF B2 08 52
Signature	RSA/SHA-256
Hash Algorithm	SHA-256
Issuer/Subject DN	C = IT, O = Namirial S.p.A., OU = Namirial Trust Service Provider, CN = Namirial Time Stamping Authority
Valid from	27/6/2016 10:15:44
Valid To	27/6/2036 10:15:44
Public Key	RSA 2048 bits

Tabella 8: Certificato Namirial Time Stamping Authority

Estensioni:

Field	OID	Critical	Value
subjectKeyIdentifier/ authorityKeyIdentifier	2.5.29.14	No	31 E3 9F 5B 9D 0E 36 AC 60 1A 1B 39 BF 7D 63 B7 12 48 B4 C3
KeyUsage	2.5.29.15	Yes	keyCertSign, cRLSign
BasicConstraints	2.5.29.19	Yes	True (CA, Undefined Maximum Path Length)
certificatePolicies	2.5.29.32	No	2.5.29.32.0 (Any Policy)
cRLDistributionPoints	2.5.29.31	No	http://crl.namirialtsp.com/TSA.crl

4.1.2.2 CERTIFICATO NAMIRIAL CA TSA

Field	Value
Version	2 (V3)
Serial Number	20 CA FE AF CA 99 FA 96
Signature	RSA/SHA-256
Hash Algorithm	SHA-256
Issuer/Subject DN	CN = Namirial CA TSA, OU = Certification Authority, O = Namirial S.p.A./02046570426, C = IT
Valid from	24/11/2010 17:01:35
Valid To	24/11/2030 17:01:35
Public Key	RSA 2048 bits

Tabella 9: Certificato Namirial CA TSA

Estensioni:

Field	OID	Critical	Value
subjectKeyIdentifier/ authorityKeyIdentifier	2.5.29.14	No	96 BE FC C7 A7 57 72 AD 82 5A 61 AE E6 AF 90 98 9D A1 11 5D
keyUsage	2.5.29.15	Yes	keyCertSign, cRLSign
basicConstraints	2.5.29.19	Yes	True (CA, Undefined Maximum Path Length)
certificatePolicies	2.5.29.32	No	2.5.29.32.0 (Any Policy)
cRLDistributionPoints	2.5.29.31	No	URL=http://crl.firmacerta.it/FirmaCertaTSA.crl
authorityInfoAccess	1.3.6.1.5.5.7.1.1	No	OCSP (1.3.6.1.5.5.7.48.1) http://ocsp.firmacerta.it/ocsp/certstatus

4.2 CERTIFICATE POLICIES

Il Certificatore utilizza i seguenti Object Identifier, (OID) afferenti al proprio Private Enterprise Number:

1.3.6.1.4.1.36203	Namirial S.p.A.
1.3.6.1.4.1.36203.1	CA FirmaQualificata
1.3.6.1.4.1.36203.1.1	Policy CA FirmaQualificata
1.3.6.1.4.1.36203.2	CA TSA
1.3.6.1.4.1.36203.2.1	Policy CA TSA
1.3.6.1.4.1.36203.4	CA Autenticazione
1.3.6.1.4.1.36203.4.1	Policy CA Autenticazione

Tabella 10: Namirial CA Object Identifier

I certificati emessi secondo le regole del presente documento sono identificati 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 (utilizzata fino a Gennaio 2014). La policy identifica emissioni di marche temporali conformi al [21].
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 ad apparato sicuro per la creazione della firma mediante procedura automatica. User Notice: Il presente certificato è valido solo per firme apposte con procedura automatica. This certificate may only be used for unattended/automated digital signatures.
1.3.6.1.4.1.36203.1.1.4	Policy per certificati associati ai server OCSP relativi ai certificati di Sottoscrizione.
1.3.6.1.4.1.36203.1.1.5	Policy per certificati qualificati associati ad apparato sicuro per la creazione della firma mediante procedura remota.
1.3.6.1.4.1.36203.1.2.1	Policy per certificati qualificati emessi a legal person la cui chiave privata non risiede in un Qualified Seal Creation Device
1.3.6.1.4.1.36203.1.2.3	Policy per certificati qualificati emessi a legal person la cui chiave privata risiede un Qualified Seal Creation Device
1.3.6.1.4.1.36203.2.1.1	Policy per certificati associati ai server di marcatura temporale (utilizzata da Gennaio 2014). La policy identifica emissioni di marche temporali conformi al [21], al [34] e al [23] e successive modificazioni.
1.3.6.1.4.1.36203.2.1.2	Policy per certificati usati per l'emissione di marche temporali qualificate. La policy identifica emissioni di marche temporali conformi al [21], al [34], al [23] e al [24] e successive modificazioni.
1.3.6.1.4.1.36203.4.1.2	Policy per certificati di Autenticazione.

1.3.6.1.4.1.36203.4.1.4	Policy per certificati associati ai server OCSP relativi ai certificati di Autenticazione.

Tabella 11: Object Identifier dei certificati emessi da Namirial CA

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

4.3 LIMITI D'USO

Ferma restando la responsabilità del ***Certificatore*** di cui al [03] (art.30 comma 1 lettera a), è responsabilità del ***Titolare*** 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 [08] e successive modificazioni, e provvede ad inserire, su richiesta del titolare o della persona giuridica che ha richiesto il certificato, almeno i seguenti **limiti 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. / *This certificate may only be used for unattended/automated digital signatures.*
- 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).*

4.4 INFORMAZIONI CONTENUTE NEI CERTIFICATI

Le tipologie di certificati emessi da Namirial sono:

- Certificati di Sottoscrizione (Firma Qualificata, Firma Automatica, Firma Remota, Sigillo Elettronico);
- Certificati di Autenticazione (CNS);
- Certificati di Marcatura Temporale;
- Certificati Root della CA.

Tutti i certificati emessi soddisfano lo standard ISO 9594-8-2001, sono conformi alle norme vigenti e, in particolare, a quanto indicato nella deliberazione [08] e successive modificazioni.
Conseguentemente è garantita la loro interoperabilità nel contesto delle attività dei certificatori accreditati italiani.

4.5 REGISTRO DEI CERTIFICATI

Il registro dei certificati contiene:

- tutti i certificati emessi dal Certificatore;
- la lista dei certificati sospesi e revocati (CRL).

4.5.1 ACCESSO AL REGISTRO DEI CERTIFICATI(O)

La copia di riferimento del registro dei certificati è accessibile esclusivamente 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 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.

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 RFC 5280, con particolare riferimento alle estensioni necessarie al partizionamento delle CRL qui descritto.

Ai sensi dell'art. 42 comma 3 del [05] il Certificatore rende inoltre accessibile al seguente URL copia della lista, sottoscritta dall'Agenzia, dei certificati relativi alle chiavi di certificazione di cui all'articolo 43, comma 1, lettera e) del [05]:

- https://cms.firmacerta.it/certificatori/certificatori.zip.p7m

4.5.2 GESTIONE DEL REGISTRO DEI CERTIFICATI (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 (CRL).
Le liste di revoca dei certificati (CRL) sono accessibili pubblicamente in sola lettura e contengono i certificati di sottoscrizione revocati o sospesi. La pubblicazione delle liste di revoca è aggiornata in modo sincrono ad ogni aggiornamento del registro dei certificati revocati o sospesi.

4.6 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.

5 OPERATIVITÀ

Questa sezione descrive le modalità con le quali opera il Certificatore ed in particolare l'organizzazione e le funzioni del personale addetto al servizio di certificazione, le modalità di richiesta del certificato, di identificazione del richiedente e le modalità di comunicazione con il richiedente il certificato ovvero con il Titolare del certificato.

5.1 ORGANIZZAZIONE DEL PERSONALE(ART. 38)

Il personale preposto all'erogazione e controllo del servizio di certificazione è organizzato nel rispetto dell'art. 38 del [05] In particolare, sono definite le seguenti figure organizzative:

- Responsabile della sicurezza
- Responsabile del servizio di certificazione e validazione temporale
- Responsabile della conduzione tecnica dei sistemi
- Responsabile dei servizi tecnici e logistici
- Responsabile delle verifiche e delle ispezioni (auditing)
- Responsabile della registrazione dei titolari (RA) e dell'HelpDesk;

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

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

Al fine di ampliare le possibilità operative, le funzioni di registrazione possono essere svolte anche da terze parti, con sedi distribuite sul territorio, sulla base di appositi accordi stipulati con Namirial. In tal caso, tali terze parti ("Local Registration Authority", abbreviato LRA) operano secondo quanto descritto dal presente documento e, per soggetti e/o casi particolari, dall'eventuale "addendum al manuale operativo" specifico.

5.2 MODALITÀ DI IDENTIFICAZIONE E REGISTRAZIONE DEL RICHIEDENTE E DEL TITOLARE (G)

5.2.1 CERTIFICATI QUALIFICATI PER PERSONE FISICHE

Identificazione "de visu"
Per il rilascio di Certificati Qualificati a persone fisiche, nel caso in cui il Titolare coincida con il Richiedente, lo stesso può essere identificato "de visu":

- dal personale autorizzato del Certificatore o dagli uffici di registrazione LRA, tramite i RAO;
- da un pubblico ufficiale;
- da un soggetto incaricato dall'Ente Certificatore denominato Incaricato alla Registrazione (IR).

Nel caso in cui il Titolare non coincida con il Richiedente, viene coinvolta la figura del Terzo Interessato, ovvero della società od organizzazione a cui risulta collegato il Titolare e che fa le veci del Richiedente.
In questo caso il Titolare viene identificato dal referente del Terzo Interessato che ha scritto una convenzione con la CA.
Il Richiedente (Terzo Interessato) viene identificato in fase di stipula della convenzione e equipaggiato di un dispositivo sicuro di firma che sarà utilizzato come strumento di identificazione elettronica per sottomettere le successive richieste di certificazione verso alla CA.

Identificazione telematica
Il Titolare può essere anche identificato attraverso la propria identità elettronica associata ad un certificato di firma digitale, ovvero di autenticazione, in suo possesso

5.2.2 CERTIFICATI QUALIFICATI PER PERSONE GIURIDICHE

Identificazione "de visu"
Per il rilascio di Certificati Qualificati a persone giuridiche, il Titolare coincide con la persona giuridica a cui sarà intestato il Certificato Qualificato di Sigillo, il Richiedente coincide con la persona fisica che sottopone la richiesta al Certificatore ed espleta la fase di identificazione. L'identificazione avviene "de visu".

La procedura di identificazione e registrazione degli utenti si articola sostanzialmente nelle seguenti fasi:

- identificazione "de visu" o elettronica;
- sottomissione della richiesta, corredata della necessaria documentazione;
- verifica delle informazioni fornite ed accettazione o rifiuto della richiesta.

Nei successivi paragrafi si riportano i dettagli delle suddette modalità.

5.2.3 IDENTIFICAZIONE DA PARTE DEL PERSONALE DEL CERTIFICATORE O DEGLI UFFICI DI REGISTRAZIONE LRA (RAO)

Il Titolare o Richiedente possono identificarsi recandosi presso il Certificatore (o un ufficio di registrazione LRA) con un documento d'identità o un documento di riconoscimento equipollente ai sensi dell'art.35 del [07] in corso di validità.
Il Titolare o Richiedente possono altresì essere identificati per via telematica attraverso il sistema di identificazione remota "ViSI" del Certificatore; a tal fine, è necessario che il Titolare sia in possesso di un pc, una webcam ad esso collegata e un sistema audio pc funzionante.
Per garantire la tutela e la gestione dei propri dati personali in piena aderenza al Reg UE 679/2016, ad ogni richiedente verrà preventivamente fornita l'informativa sulla privacy e, nel caso di identificazione tramite sistema di video conferenza, richiesto il consenso alla videoregistrazione ed al trattamento dei dati da parte degli incaricati del Certificatore.

ViSi
Ciascun richiedente sarà altresì informato circa il fatto che per ragioni di sicurezza la videochiamata (video/voce) sarà registrata e conservata in conformità a quanto indicato nell'art. 32, comma 3, lettera j) del CAD e che in caso di dichiarazioni mendaci, falsità negli atti, uso o esibizione di atti falsi o contenenti dati non più rispondenti a verità, sarà soggetto alle sanzioni penali previste ai sensi dall'art 76 del [07].
Solo dopo l'assenso del richiedente potrà essere avviata la registrazione della video conferenza che inizierà con la ripetizione della procedura di richiesta del consenso.
Le specifiche procedure telematiche di identificazione e registrazione studiate dal Certificatore e attuate dai propri incaricati in tale sede, non sono rese pubbliche per ragioni di sicurezza.

In dettaglio, i dati di registrazione, costituiti da file audio video e metadati strutturati in formato elettronico, vengono conservati in forma protetta per una durata ventennale, presso il Certificatore. Tale procedura in uso soddisfa quanto richiesto dall'art. 32, comma 3, lettera a) del CAD.
Il soggetto che effettua l'identificazione verifica l'identità del Titolare tramite il riscontro con un documento di riconoscimento in corso di validità, purché munito di fotografia recente e riconoscibile del Titolare, firma autografa del Titolare e di timbro, rilasciato da un'Amministrazione dello Stato. A titolo esemplificativo si riporta una lista di documenti accettati:

a) Carta d'identità,
b) Passaporto,
c) Patente di guida,
d) Patente nautica,
e) Libretto di pensione,
f) Patentino di abilitazione alla conduzione di impianti termici,
g) Porto d'armi.

È facoltà del soggetto che effettua l'identificazione escludere l'ammissibilità del documento utilizzato dal Titolare se ritenuto carente delle caratteristiche elencate.

La modalità di identificazione e registrazione tramite LRA e RAO può essere utilizzata per il rilascio di Certificati Qualificati a persone fisiche (§ 5.2.1) e giuridiche (§ 5.2.2).

5.2.4 IDENTIFICAZIONE DA PARTE DEL REFERENTE DEL TERZO INTERESSATO CHE HA SOTTOSCRITTO UNA CONVENZIONE

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

a) modulo di richiesta emissione certificato
b) una copia di un documento d'identità o un documento di riconoscimento equipollente ai sensi dell'art.35 del [07] in corso di validità.

I suddetti documenti potranno essere firmati attraverso firma elettronica avanzata, qualificata, digitale o autografa.

5.2.5 IDENTIFICAZIONE DA PARTE DI UN PUBBLICO UFFICIALE

Il Richiedente, qualora coincida con il Titolare, compila la richiesta di emissione di certificati e la dichiarazione sostitutiva dell'atto di notorietà (scaricando il modulo dalla sezione "*Documenti*" del sito http://www.firmacerta.it), si reca presso un Pubblico Ufficiale e sottoscrive la richiesta e la dichiarazione facendo autenticare le proprie firme autografe, ai sensi della normativa che disciplina le loro attività e da quanto indicato nel D.L. 3 Maggio 1991 n. 143 e successive modifiche ed integrazioni.

Il Richiedente invia al Certificatore:

a) il modulo di richiesta di emissione certificato (in originale);
b) la dichiarazione sostitutiva dell'atto di notorietà (in originale);
c) una copia di un documento d'identità o un documento di riconoscimento equipollente ai sensi dell'art. 35 del [07] in corso di validità.

5.2.6 IDENTIFICAZIONE DA PARTE DI UN SOGGETTO INCARICATO ALLA REGISTRAZIONE (IR)

In tale modalità l'identificazione è effettuata da un soggetto denominato Incaricato alla Registrazione (IR) appartenente ad una società terza, ed è prevista la presenza fisica del Richiedente (che deve coincidere con il Titolare del certificato) dinnanzi al suddetto incaricato. Tali soggetti (gli IR) possono operare successivamente alla stipula di un contratto tra il Certificatore e la Società Terza. Quest'ultima indica il proprio personale, che viene individuato come Incaricato di Registrazione (IR) e che deve operare secondo le procedure stabilite e contenute nel presente manuale operativo per quanto concerne le fasi di identificazione, registrazione dei dati del richiedente qualora quest'ultimo non abbia usato la procedura di pre-registrazione, verifica della corretta compilazione del Modulo di Registrazione e Richiesta del Certificato, dell'apposizione della firma autografa sul contratto e, quando previsto, consegna "brevi manu" del dispositivo.
Il Richiedente deve presentarsi all'IR esibendo:

- il Modulo di Registrazione e Richiesta del Certificato contenente i dati anagrafici del Richiedente eventualmente già forniti in modalità elettronica (ad esempio con procedura di pre-registrazione web);
- il Documento di Riconoscimento rispondente a quelli previsti al paragrafo 5.2.3. Il Documento può essere anticipato dal Richiedente via Web tramite procedura di pre-registrazione;
- le condizioni generali di contratto;
- l'informativa sulla privacy;
- il dispositivo di firma, se richiesto.

Per l'identificazione del Richiedente, l'IR deve usare la modalità "tramite il riscontro con un documento di riconoscimento in corso di validità", così come descritta nel paragrafo 5.2.3., verificando che, nel caso di pre-registrazione via Web, il Documento sia lo stesso già caricato in procedura e deve astenersi dall'accettare qualsiasi altro modulo che non sia quello emesso dal Certificatore.

Il Modulo di Registrazione e Richiesta del Certificato vengono sottoscritti con firma autografa dal soggetto Richiedente dinnanzi all'IR.

Nel caso d'utilizzo della busta cieca digitale (§ **Errore. L'origine riferimento non è stata trovata.**), successivamente alla consegna del dispositivo, il Certificatore inoltra la busta all'indirizzo email fornito dal Titolare e sottoscritto al momento della consegna del dispositivo in presenza dell'IR.

Si rende noto in tal senso che il soggetto Richiedente, firmando il Modulo di Registrazione e Richiesta del Certificato, si assume gli obblighi di cui al paragrafo 3.2.2.

In ogni caso la responsabilità delle operazioni di registrazione, identificazione e validazione è del Certificatore.

5.2.7 REGISTRAZIONE DEGLI UTENTI

Le procedure per la registrazione del Richiedente (e Titolare nel caso non coincida con il Richiedente) e il rilascio del certificato prevedono:

a) che il Richiedente ed il Titolare vengano identificati con certezza dal Certificatore con una delle modalità descritte ai precedenti paragrafi. Le attività di identificazione possono essere svolte, oltre che direttamente dal personale autorizzato del Certificatore, dagli Uffici di Registrazione (LRA) tramite la figura del RAO e dagli IR;
b) che il Richiedente abbiano preso visione dell'informativa di cui l'art. 13 del [06];
c) che il Richiedente abbia espresso il consenso alla videoregistrazione ed al trattamento dei dati, nel caso di identificazione telematica;

d) che il Richiedente e Titolare abbiano preso visione delle Condizioni Generali di contratto e del presente Manuale Operativo;
e) che il Richiedente e Titolare sottoscrivano il Modulo di Richiesta di Emissione del Certificato qualificato (reperibile dalla sezione "Documenti" del sito https://docs.namirialtsp.com), debitamente compilato in tutte le sue parti;

Se è richiesto l'inserimento del Ruolo e del Terzo Interessato nel certificato qualificato devono essere inoltre forniti:

a) 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;
b) attestazione che l'Organizzazione ha ricevuto l'informativa di cui l'art. 13 del [06].

Se è richiesto l'inserimento del Titolo e/o Abilitazione Professionale nel certificato qualificato deve essere inoltre fornito:

- documento rilasciato l'Ordine/Albo/Collegio professionale che attesti l'effettiva appartenenza, non antecedente a 30 (trenta) giorni dalla data di richiesta di registrazione.

Il Certificatore, terminata la fase di identificazione, effettua l'operazione di registrazione del Richiedente/Titolare attraverso il portale web del servizio di certificazione digitale, il quale registra i dati forniti nel "database degli utenti". Il Certificatore provvede successivamente al rilascio del certificato qualificato e, ove previsto, all'invio del dispositivo di firma.

Le attività di registrazione, oltre che essere svolte direttamente dal personale autorizzato del Certificatore, possono essere svolte dal personale delle LRA, i RAO, o dal personale indicato come IR, dopo apposito corso di formazione.

Le credenziali per l'accesso all'area privata del portale del servizio di certificazione digitale, il dispositivo di firma e/o il dispositivo OTP, il PIN/PUK del dispositivo di firma e il codice di emergenza da utilizzarsi per la prima attivazione e la sospensione o revoca del certificato, ovvero le credenziali per l'uso del Certificato Qualificato per Sigillo Elettronico, sono consegnati al Titolare come indicato nei Paragrafi 5.5 e 5.6.

Una volta terminato il processo di identificazione e registrazione da parte dell'LRA o dell'IR, l'operatore, utilizzando canali di comunicazione sicuri, invia tutte le informazioni raccolte durante le fasi di identificazione e registrazione ai sistemi della CA.
Le informazioni scambiate durante le operazioni sopradescritte sono utilizzate dall'Ente Certificatore per il rilascio del Certificato Qualificato di Firma Elettronica o Sigillo Elettronico e archiviate nel database di registrazione in automatico.
Nel caso di LRA e Certificato Qualificato di Firma Elettronica, il RAO, è abilitato a procedere con la personalizzazione elettrica del dispositivo di firma che verrà quindi consegnato in modo sicuro nelle mani del Titolare.
Nel caso di LRA e Certificato Qualificato di Sigillo Elettronico, il RAO, è abilitato a procedere con la personalizzazione elettrica del dispositivo di firma custodito dal Certificatore e consegna sicura delle credenziali per l'utilizzo presso i riferimenti indicati dal Richiedente/Titolare.
Nel caso di IR, l'operatore si limita a trasmettere i dati della richiesta di certificazione alla CA per la loro validazione. Il rilascio del certificato qualificato avviene dopo la verifica della CA utilizzando un dispositivo sicuro, consegnato e personalizzato secondo le indicazioni contenute in § 5.3.2, 5.4 e 5.5

Esclusivamente nel caso in cui il Richiedente coincida con i dati contenuti nel campo Subject del certificato, esso assume la qualifica di Titolare.

5.3 MODALITÀ DI GENERAZIONE DELLE CHIAVI(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 delle 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.

Le chiavi appartenenti ad una delle tipologie elencate nell'art. 5, comma 4, del [05] sono generate (art. 6 e 7), conservate (art. 8) ed utilizzate (art. 11, comma 1) all'interno di uno stesso dispositivo elettronico avente le caratteristiche di sicurezza di cui all'art. 12 del [05].
Le chiavi hanno le caratteristiche previste dagli art. 4 e 5 del [05].
La generazione delle chiavi avviene all'interno del dispositivo sicuro per la generazione delle firme.
Nel caso in cui la generazione avvenga al di fuori di tale dispositivo, il sistema di generazione è conforme alle disposizioni di cui all'art. 9 del [05].
Nel caso di certificato abbinato ad una CNS, la generazione delle chiavi di firma può avvenire centralmente ed anche al di fuori della CNS stessa; inoltre essa può essere svolta presso il certificatore secondo gli specifici accordi in essere con la PA emittente, comunque nel rispetto del [22] e dell'art. 9 del [05].

Le chiavi corrispondenti a Certificati Qualificati per Sigillo Elettronico sono generate utilizzando le stesse procedure e meccanismi adottati per la generazione delle chiavi corrispondenti a Certificati Qualificati per Firma Elettronica. Questo garantisce l'applicazione delle medesime misure di sicurezza già in essere per le chiavi di Firma Elettronica.

5.3.1 MODALITÀ DI GENERAZIONE DELLE CHIAVI DI CERTIFICAZIONE

La generazione delle chiavi all'interno dei dispositivi di firma avviene in presenza del Responsabile del servizio di Certificazione, come previsto dall'art. 7 del [05] ed è preceduta dall'inizializzazione dei dispositivi di firma per il sistema di generazione dei certificati con i quali si firmano i certificati dei Titolari e quelli del sistema di validazione temporale. In generale vengono osservati i seguenti criteri:

- la procedura avviene in presenza di un numero di responsabili aziendali ritenuto adeguato e sufficiente ad evitare operazioni illecite;
- una volta generate le coppie di chiavi, quelle private vengono suddivise in più parti, ciascuna delle quali viene trascritta su due set di smart card;
- le smart card di ogni set vengono assegnate ciascuna ad una delle persone aziendali presenti, le quali vi associeranno una propria password che manterranno segreta;
- le smart card di ogni set e le relative password sono conservate in modo sicuro.

5.3.2 MODALITÀ DI GENERAZIONE DELLE CHIAVI DI SOTTOSCRIZIONE DEGLI UTENTI

Completata la fase di registrazione, durante la quale i dati del Richiedente e del Titolare vengono memorizzati negli archivi del Certificatore (o LRA), è possibile procedere alla generazione delle chiavi di sottoscrizione. Questa operazione può avvenire in due diverse modalità:

- Chiavi generate dal Certificatore (o LRA).

- Chiavi generate dal Richiedente.

In ogni caso, avendo a disposizione il dispositivo di firma, il Titolare o gli operatori RA/RAO, potranno generare una nuova coppia di chiavi mediante la funzione di generazione di chiavi asimmetriche dello stesso dispositivo. Le chiavi vengono generate in conformità con il [05], art. 6, comma 2, e 7, comma 3.
I dispositivi di firma utilizzati rispondono ai requisiti di sicurezza previsti dal [05], art. 12, comma 1.
Le chiavi corrispondenti a Certificati Qualificati di Sigillo Elettronico possono essere generate solo dal Certificatore

5.3.2.1 CHIAVI GENERATE DAL CERTIFICATORE

Questa procedura viene effettuata dagli operatori RA del Certificatore presso i propri locali, o dagli operatori RAO delle LRA.
Sono effettuate le seguenti operazioni:

- l'operatore si autentica all'applicazione CMS, seleziona i dati di registrazione del Richiedente e attiva la procedura di richiesta di certificato;
- l'applicazione accede al dispositivo di firma con il PIN di default e genera la coppia di chiavi.

5.3.2.2 CHIAVI GENERATE DAL RICHIEDENTE

RILASCIO SELF-ENROLL
Questa procedura prevede che la personalizzazione del dispositivo di firma sia svolta sotto il controllo dell'utente, o comunque in sua presenza, e si basa su interazioni telematiche sicure con il certificatore (generalmente connessioni via Internet protette da protocolli che garantiscano un adeguato livello di sicurezza).
In questa fase le chiavi di sottoscrizione sono generate dal richiedente stesso attivando con l'applicazione approvata dalla CA il dispositivo sicuro per la generazione della firma fornito o indicato dallo stesso Certificatore.
Il richiedente è:

- riconosciuto dal Certificatore tramite un codice personale riservato o una password;
- autenticato dal dispositivo sicuro per la generazione della firma tramite l'inserimento del PIN contenuto nella busta cieca (scratch-card) consegnata a seguito dell'identificazione da parte dell'IR/RAO

RINNOVO
Questa procedura può essere utilizzata per le operazioni di rinnovo di un precedente certificato generato dal Certificatore nei casi in cui il Richiedente disponga di un certificato di sottoscrizione valido e del relativo dispositivo di firma fornito dal Certificatore. Il Certificatore fornisce allo scopo l'applicazione client "FirmaCerta" in grado di generare la coppia di chiavi all'interno del dispositivo di firma e la richiesta di certificato in formato PKCS#10.
I prerequisiti hardware e software, nonché tutte le indicazioni per l'installazione del prodotto "FirmaCerta", sono riportate nella "Guida rapida all'utilizzo" del software, disponibile all'URL:

http://www.firmacerta.it/manuali.php

Nel documento, che è parte integrante del presente Manuale Operativo, sono riportate le modalità operative per il rinnovo dei certificati di firma.

Non ricadono in questa casistica le chiavi corrispondenti a Certificati Qualificati per Sigillo Elettronico.

5.3.3 MODALITÀ DI GENERAZIONE DELLE CHIAVI DI MARCATURA TEMPORALE

La generazione delle chiavi avviene nel rispetto degli art. 49 e 50 del [05]; in particolare:

- La chiavi di certificazione e di marcatura temporale, ai sensi dell'art. 49, comma 4, del [05], sono generate in presenza del responsabile del servizio di certificazione e validazione temporale.
- La coppia di chiavi utilizzata per la validazione temporale è di 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.
Il profilo dei certificati di marcatura temporale è conforme alla [08] e successive modificazioni.

5.3.4 ALGORITMI CRITTOGRAFICI E LUNGHEZZA DELLE CHIAVI

Ai sensi dell'art. 3 della [08] e successive modificazioni:

- nelle operazioni di firma è usato l'algoritmo RSA (Rivest-Shamir-Adleman);
- le chiavi usate dal Certificatore per firmare i certificati hanno lunghezza almeno pari a 2048 bit;
- la lunghezza della chiave di sottoscrizione dei titolari è pari almeno a 1024 bit.

5.3.5 FUNZIONI DI HASH

Per la generazione dell'impronta viene 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 [08] e successive modificazioni.

5.4 MODALITÀ DI EMISSIONE DEI CERTIFICATI(I)

Il Certificatore rilascia certificati per

Persone fisiche:
- indipendenti (certificati standard);
- appartenenti ad Organizzazioni;
- appartenenti ad Ordini Professionali.

Persone giuridiche:
- per uso come Sigillo Elettronico (certificati standard);

I certificati rilasciati possono essere relativi a:

1. chiavi di sottoscrizione generate per la firma attraverso dispositivi di firma personali;
2. chiavi di sottoscrizione generate per la firma attraverso applicazioni di sottoscrizione automatica;
3. chiavi di sottoscrizione generate per l'uso attraverso applicazioni di firma remota;

4. chiavi di sottoscrizione generate per l'uso attraverso applicazioni di sigillo elettronico

I paragrafi che seguono descrivono nel dettaglio le modalità di emissione dei certificati in relazione a tutti i casi previsti.

5.4.1 RILASCIO CERTIFICATI PER PERSONE FISICHE INDIPENDENTI

Il rilascio di Certificati qualificati a persone fisiche avviene previa l'identificazione del Richiedente da parte di uno dei soggetti elencati al paragrafo 5.2, il quale:

- 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 il modulo di richiesta di emissione dei certificati.

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

5.4.2 RILASCIO CERTIFICATI PER PERSONE FISICHE APPARTENENTI AD ORGANIZZAZIONI

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

- **Modalità 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.

- **Modalità 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 (trenta) 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.

5.4.3 RILASCIO CERTIFICATI PER PERSONE FISICHE APPARTENENTI AD ORDINI PROFESSIONALI

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:

- **Modalità 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.

- **Modalità 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 Collegio all' inserimento del ruolo/qualifica nel certificato. La documentazione non deve essere antecedente a 30 (trenta) 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.

5.4.4 RILASCIO CERTIFICATI PER PERSONE GIURIDICHE AD USO SIGILLO ELETTRONICO

Il rilascio di Certificati Qualificati per Sigillo Elettronico può avvenire solo a persone giuridiche (Titolari) previa identificazione di un legale rappresentate ovvero delegato munito di apposita delega notarile. I soggetti che possono effettuar e il riconoscimento ai fini del rilascio del Sigillo Elettronico sono esclusivamente quelli elencati al paragrafo § 5.2.3.
La procedura prevede

- verifica i dati identificativi personali del Richiedente;
- verifica l'identità attraverso un documento di riconoscimento in corso di validità;
- verifica del possesso dei poteri di rappresentanza della persona giuridica da parte del Richiedente (legale rappresentate o persona munita di delega notarile)
- verifica della visura camerale dalla quale si possano evincere i dati identificativi della persona giuridica e gli eventuali poteri di rappresentanza del richiedente
- verifica la correttezza del codice fiscale ovvero partita iva (se disponibile) o, se applicabile, di altro codice identificativo previsto dalle vigenti norme;
- verifica il modulo di richiesta di emissione dei certificati.

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

5.4.5 GENERAZIONE ED EMISSIONE DI CERTIFICATI PER DISPOSITIVI DI FIRMA PERSONALI

La generazione dei certificati per dispositivi di firma personali (Smart Card, Token) avviene nel rispetto dell'art. 18 del [05], utilizzando un processo articolato in diverse fasi e basato su canali di comunicazione sicuri.
Gli utenti coinvolti nelle varie fasi della generazione ed emissione dei certificati sono diversi, in funzione dell'utente che esegue il processo di personalizzazione del dispositivo. Sono previsti i seguenti casi:

5.4.5.1 PERSONALIZZAZIONE A CURA DELLA LRA O DEL CERTIFICATORE

L'operatore LRA/CA presiede l'intera procedura, provvedendo:

1. a verificare che la documentazione fornita sia compilata e sottoscritta in ogni sua parte;
2. alla verifica della presenza dei prerequisiti come previsto nei paragrafi 5.4.1, 5.4.2, 5.4.3;
3. a registrare il Titolare richiedente nel portale CMS, autenticandosi alla propria area riservata;
4. se prevista busta cieca cartacea, ad associare quest'ultima al dispositivo di firma;
5. ad avviare la procedura automatica di generazione delle chiavi (pubblica e privata) sul dispositivo di firma e del certificato;
6. alla stampa e sottoscrizione da ambo le parti del modulo di richiesta e della ricevuta di consegna;
7. alla consegna del dispositivo di firma e di una copia della documentazione al Titolare richiedente;
8. se prevista la busta cieca in formato cartaceo, alla consegna della stessa (contenente il PIN, ed il codice d'emergenza) associata al titolare ed individuata dal numero di riferimento visibile all'esterno.

La procedura automatica di cui al punto 5) provvede più specificatamente:

a) a verificare che la chiave sia della lunghezza prevista;
b) all'assegnazione al Titolare richiedente di un codice identificativo univoco nell'ambito degli utenti del Certificatore (CUC), diverso per ogni certificato emesso;
c) alla connessone al dispositivo di firma con il PIN iniziale;
d) al cambio del PIN e PUK iniziali con nuovi valori generati randomicamente e registrati in modalità protetta su record DB cifrato nei sistemi della CA;
e) alla generazione del certificato contenente la chiave pubblica e i dati previsti mediante la firma con la chiave di certificazione della CA;
f) all'inserimento del certificato nel registro dei certificati;
g) alla registrazione sul registro di controllo dell'avvenuta generazione;
h) alla trasmissione del certificato dalla CA alla LRA su canale sicuro;
i) all'inserimento del certificato nel dispositivo di firma;
j) alla verifica dell'inserimento del certificato nel dispositivo di firma;
k) alla cancellazione dal DB del record cifrato della busta cieca associata al titolare, nel caso la stessa sia in formato cartaceo;
l) alla registrazione sul giornale di controllo dell'avvenuta personalizzazione del dispositivo di firma;
m) all'invio tramite email delle informazioni e credenziali per accedere all'area riservata del portale CMS;
n) all'invio di un codice temporaneo, tramite SMS, da utilizzarsi come ulteriore credenziale di accesso alle pagine riservate del CMS).

5.4.5.2 PERSONALIZZAZIONE A CURA DELL'UTENTE RICHIEDENTE TRAMITE SELF ENROLL

La procedura coinvolge l'IR per le fasi di identificazione e registrazione. La personalizzazione del dispositivo viene **preventivamente autorizzata** dal Certificatore/LRA e **svolta** dal Titolare Richiedente. Il processo si articola come segue:

1. L'IR verifica che la documentazione fornita sia compilata e sottoscritta in ogni sua parte;
2. L'IR verifica la presenza dei prerequisiti come previsto nei paragrafi 5.4.1, 5.4.2, 5.4.3;
3. L'IR registra il Titolare richiedente nel portale CMS, autenticandosi alla propria area riservata;
4. L'IR procede ad associare la busta cieca (o scratch card) al dispositivo di firma e carica i dati della pratica nel CMS, in attesa della validazione da parte della CA/LRA.
5. L'IR consegna la busta cieca e il dispositivo non personalizzato nelle mani del Titolare Richiedente. L'IR stampa, sottoscrive e fa sottoscrivere al Richiedente il modulo di richiesta e la ricevuta di avvenuta consegna del dispositivo non personalizzato.

L'IR anticipa alla CA/LRA, mezzo FAX, copia della documentazione raccolta nei punti precedenti;

6. La CA/LRA, in modalità non necessariamente contestuale, accede al CMS e verifica la richiesta in stato pending. Se non sono riscontrati errori viene autorizzato il rilascio del certificato.
   L'approvazione delle richiesta scatena l'invio di un email al Richiedente con le credenziali da utilizzare per l'utilizzo del servizio di Self- Enrollment;
7. Il Titolare Richiedente accede all'indirizzo indicato nella documentazione accompagnatoria del kit, collega il dispositivo alla propria postazione di lavoro e avvia la procedura automatica di generazione delle chiavi (pubblica e privata) sul dispositivo di firma e del certificato;
8. L'IR invia la documentazione originale alla CA/LRA per l'archiviazione ai sensi del CAD.

La procedura automatica di cui al punto 7) provvede più specificatamente:

a) ad autenticare l'utente in base alla richiesta di inserimento delle credenziali ricevute con l'email di cui al punto 6)
b) ad autenticare il dispositivo tramite la lettura del seriale della carta e verifica dell'analogo dato presente a sistema e associato all'anagrafica del Richiedente
c) alla richiesta del PIN riportato nella scartch card e sua verifica con il dato presente a sistema
d) all'assegnazione al Titolare richiedente di un codice identificativo univoco nell'ambito degli utenti del Certificatore (CUC), diverso per ogni certificato emesso;
e) alla connessone al dispositivo di firma con il PIN iniziale (di trasporto);
f) alla generazione della coppia di chiavi di adeguata lunghezza e l'invio del PKCS#10 di richiesta certificato alla CA su canale cifrato TLS
g) alla generazione del certificato contenente la chiave pubblica e i dati previsti mediante la firma con la chiave di certificazione della CA;
h) all'inserimento del certificato nel registro dei certificati;
i) alla registrazione sul registro di controllo dell'avvenuta generazione;
j) alla trasmissione del certificato dalla CA alla postazione su canale sicuro;
k) all'inserimento del certificato nel dispositivo di firma;
l) alla verifica dell'inserimento del certificato nel dispositivo di firma;
m) alla cancellazione dal DB del record cifrato della busta cieca associata al titolare, nel caso la stessa sia in formato cartaceo;
n) alla registrazione sul giornale di controllo dell'avvenuta personalizzazione del dispositivo di firma;
o) al cambio del PIN iniziale con quello associato alla busta cieca;

5.4.6 GENERAZIONE ED EMISSIONE DI CERTIFICATI PER APPLICAZIONI DI FIRMA AUTOMATICA

La generazione dei certificati per applicazioni di firma automatica (con HSM presso il Certificatore) avviene nel rispetto degli art. 11, 12 e 13 del [05], utilizzando un processo articolato in diverse fasi e basato su canali di comunicazione sicuri. In particolare l'operatore LRA provvede:

1. a verificare che la documentazione fornita sia compilata e sottoscritta in ogni sua parte;
2. alla verifica della presenza dei prerequisiti come previsto nei paragrafi 5.4.1, 5.4.2, 5.4.3;
3. a registrare il Titolare richiedente nel portale CMS, autenticandosi alla propria area riservata;
4. se prevista la busta cieca cartacea, ad associare quest'ultima al dispositivo di firma;
5. ad avviare la procedura automatica di generazione delle chiavi (pubblica e privata) all'interno dell'HSM e di emissione del relativo certificato;
6. alla stampa e sottoscrizione da ambo le parti del modulo di richiesta e della ricevuta di consegna;
7. alla consegna di una copia della documentazione al Titolare richiedente;
8. se prevista la busta cieca in formato cartaceo, alla consegna della stessa (contenente il PIN, ed il codice d'emergenza) associata al titolare ed individuata dal numero di riferimento visibile all'esterno.

La procedura automatica di cui al punto 5) provvede più specificatamente:

a) a generare un dispositivo di firma di tipo virtuale;
b) a generare una chiave, verificando che sia della lunghezza richiesta ed assegnando ad essa il PIN relativo alla busta cieca;
c) ad associare l'utilizzo della chiave al solo scopo di firma automatica;
d) ad impostare la chiave nello stato disabilitato, la chiave potrà essere abilitata dal Titolare mediante i codici consegnati tramite busta cieca o tramite pannello accedibile con credenziali trasmesse via email e SMS;
e) all'assegnazione al Titolare richiedente di un codice identificativo univoco nell'ambito degli utenti del Certificatore (CUC), diverso per ogni certificato emesso;
f) alla generazione del certificato contenente la chiave pubblica e i dati previsti mediante la firma con la chiave di certificazione della CA;
g) all'inserimento del certificato nel registro dei certificati;
h) alla registrazione sul registro di controllo dell'avvenuta generazione;
i) all'inserimento del certificato nel sistema di firma, dopo avere verificato la corrispondenza delle chiavi;
j) alla cancellazione dal DB del record cifrato della busta cieca associata al titolare, nel caso la stessa sia in formato cartaceo;
k) alla registrazione sul giornale di controllo dell'avvenuto intervento sul dispositivo virtuale di firma;
l) all'invio tramite email delle informazioni e credenziali per accedere all'area riservata del portale CMS;
m) all'invio di un codice temporaneo, tramite SMS, da utilizzarsi come ulteriore credenziale di accesso alle pagine riservate del CMS.

5.4.7 GENERAZIONE ED EMISSIONE DI CERTIFICATI PER APPLICAZIONI DI FIRMA REMOTA

La generazione dei certificati per applicazioni di firma remota (con HSM presso il Certificatore) avviene nel rispetto degli art. 11, 12 e 13 del [05], utilizzando un processo articolato in diverse fasi e basato su canali di comunicazione sicuri. In particolare l'operatore LRA provvede:

1. a verificare che la documentazione fornita sia compilata e sottoscritta in ogni sua parte;
2. alla verifica della presenza dei prerequisiti come previsto nei paragrafi 5.4.1, 5.4.2, 5.4.3;
3. a registrare il Titolare richiedente nel portale CMS, autenticandosi alla propria area riservata;
4. a verificare che il Titolare sia in possesso di un meccanismo OTP, e nel caso negativo, ad assegnarne uno;
5. a fornire approvazione al procedimento di generazione chiavi su HSM e rilascio certificato;
6. alla stampa e sottoscrizione da ambo le parti del modulo di richiesta;
7. alla consegna della documentazione al Titolare richiedente;

La procedura di generazione chiavi e rilascio certificato di cui al punto 5) prevede più specificatamente:

a) che il Titolare acceda alla sua area privata all'interno del CMS utilizzando le credenziali ricevute per email e inviate dal sistema al momento della registrazione;
b) che il Titolare effettui il cambio della password d'accesso all'Area Privata assegnata automaticamente con una nuova, scelta autonomamente;
c) che il Titolare, se non lo ha già fatto precedentemente, proceda all'attivazione del meccanismo OTP assegnatogli (e/o consegnatogli);
d) che il Titolare esegua direttamente la procedura di generazione chiavi ed emissione certificato agendo su apposito bottone;
e) che il Titolare scelga personalmente dei codici di adeguata complessità da utilizzare come codice d'emergenza e PIN di protezione della chiave. Il Titolare inserisce detti codici unitamente al nuovo codice OTP;

f) che il sistema generi la nuova chiave nell'HSM proteggendola con il PIN scelto dal Titolare;
g) che la chiave generata sia associata al solo uso di firma remota;
h) l'assegnazione al Titolare richiedente di un codice identificativo univoco nell'ambito degli utenti del Certificatore (CUC), diverso per ogni certificato emesso;
i) la generazione del certificato contenente la chiave pubblica e i dati previsti mediante la firma con la chiave di certificazione della CA;
j) l'inserimento del certificato nel registro dei certificati;
k) la registrazione sul registro di controllo dell'avvenuta generazione;
l) l'inserimento del certificato nel sistema di firma remota, previa verifica della corrispondenza tra chiave privata e certificato;
m) la verifica dell'inserimento del certificato nel dispositivo di firma;
n) la registrazione sul giornale di controllo dell'avvenuto intervento sul dispositivo virtuale di firma;
o) la pubblicazione nell'area privata di un documento contenente l'identificativo univoco della chiave, il nome del dispositivo virtuale e del codice d'emergenza. Il Titolare potrà usare il codice d'emergenza per le operazioni di disattivazione chiave e sospensione del certificato, nel caso in cui non dovesse disporre del codice OTP;

I certificati per firma remota vengono emessi in stato attivo.

5.4.8 GENERAZIONE ED EMISSIONE DI CERTIFICATI QUALIFICATI PER SIGILLO ELETTRONICO

La generazione dei Certificati Qualificati per Sigillo Elettronico (con HSM presso il Certificatore) avviene nel rispetto degli art. 11, 12 e 13 del [05], utilizzando un processo articolato in diverse fasi e basato su canali di comunicazione sicuri. In particolare l'operatore LRA provvede:

1. a verificare che la documentazione fornita sia compilata e sottoscritta in ogni sua parte;
2. alla verifica della presenza dei prerequisiti come previsto nei paragrafi 5.4.4;
3. a registrare il Titolare ed il Richiedente nel portale CMS, autenticandosi alla propria area riservata;
4. se prevista la busta cieca cartacea, ad associare quest'ultima al dispositivo di firma;
5. ad avviare la procedura automatica di generazione delle chiavi (pubblica e privata) all'interno dell'HSM e di emissione del relativo certificato;
6. alla stampa e sottoscrizione da ambo le parti del modulo di richiesta e della ricevuta di consegna;
7. alla consegna di una copia della documentazione al Richiedente;
8. se prevista la busta cieca in formato cartaceo, alla consegna della stessa (contenente il PIN, ed il codice d'emergenza) associata al titolare ed individuata dal numero di riferimento visibile all'esterno.

La procedura automatica di cui al punto 5) provvede più specificatamente:

a) a generare un dispositivo di firma di tipo virtuale;
b) a generare una chiave, verificando che sia della lunghezza corretta ed assegnando ad essa un PIN univoco;
c) ad associare l'utilizzo della chiave al solo scopo di sigillo elettronico;
d) ad impostare la chiave nello stato disabilitato, la chiave potrà essere abilitata dal Titolare mediante i codici consegnati tramite busta cieca o tramite credenziali trasmesse via email e SMS;
e) all'assegnazione al Titolare di un codice identificativo univoco nell'ambito degli utenti del Certificatore (CUC), diverso per ogni certificato emesso;
f) alla generazione del certificato contenente la chiave pubblica e i dati previsti mediante la firma con la chiave di certificazione della CA;
g) all'inserimento del certificato nel registro dei certificati;
h) alla registrazione sul registro di controllo dell'avvenuta generazione;
i) all'inserimento del certificato nel sistema di firma, dopo avere verificato la corrispondenza delle chiavi;
j) alla cancellazione dal DB del record cifrato della busta cieca associata al titolare, nel caso la stessa sia in formato

cartaceo;

k) alla registrazione sul giornale di controllo dell'avvenuto intervento sul dispositivo virtuale di firma;
l) all'invio tramite email delle informazioni e credenziali per accedere all'area riservata del portale CMS;
m) all'invio di un codice temporaneo, tramite SMS, da utilizzarsi come ulteriore credenziale di accesso alle pagine riservate del CMS.

5.5 MODALITÀ DI CONSEGNA DEI DISPOSITIVI DI FIRMA PERSONALI E DEI CODICI SEGRETI

I dispositivi di firma vengono consegnati "a vista", brevi manu al titolare dal RAO o dall'IR, successivamente all'identificazione e registrazione dello stesso

I codici segreti relativi al dispositivo di firma ovvero:

- PIN e PUK del dispositivo fisico (smarcard/token usb)
- PIN del dispositivo virtuale (certificato per firma automatica o sigillo)
- Password del certificato software (sigillo elettronico software)
- Codice di Emergenza

vengono consegnati secondo le seguenti modalità:

1) **Busta cieca cartacea o scratch card** prestampata e associata al dispositivo al momento della registrazione, consegnata "a vista" al Titolare dal RAO/IR;
2) **Accesso all'area riservata del portale della CA:** In questa modalità il Richiedente riceve un'email ed un SMS contenenti le informazioni e le credenziali per l'accesso all'Area Riservata del CMS. L'email e l'SMS sono inviati ai riferimenti indicati durante la registrazione e contenuti nel modulo di richiesta del certificato.
   L'utente, tramite le credenziali, accede ad un'area in cui può stampare il pdf con i codici segreti relativi al dispositivo di firma (fisico o virtuale) ed il codice di emergenza.
3) **Ricezione credenziali via email e SMS (solo Sigillo):** In questa modalità il Titolare riceve un'email ed un SMS contenenti le informazioni e le credenziali per l'accesso al proprio Certificato Qualificato di Sigillo Elettronico

5.5.1 USO DELLA BUSTA CIECA CARTACEA

Nelle modalità di consegna 1) il certificato viene rilasciato in stato attivo.
In fase di registrazione viene quindi creato anche un account (username e password) per l'accesso all'area privata del portale di certificazione digitale (CMS):

https://cms.firmacerta.it/areaPrivata

I dati relativi a tale account vengono inviati alla casella di posta elettronica dell'utente indicata nel modulo di richiesta del certificato. L'utente, al primo accesso, sarà obbligato a cambiare la password rispettando le politiche di password enforcement.

5.5.2 RICEZIONE CREDENZIALI VIA EMAIL ED SMS (SIGILLO)

In questa modalità di consegna delle credenziali il Titolare riceve la credenziale username per email e la credenziale pin tramite SMS. Per riuscire ad utilizzare il certificato l'utente dovrà autenticarsi tramite la username ed il pin ricevuti.

5.5.3 ACCESSO ALL'AREA RISERVATA DELLA CA

Per poter accedere ai codici segreti del dispositivo di firma l'utente deve autenticarsi ad una pagina del Certificatore, accessibile, previa verifica di codici di controllo inviati ai riferimenti email e SMS indicati al momento della richiesta (doppio fattore).
La procedura di accesso ai codici del dispositivo prevede che l'utente, dopo essersi autenticato, scarichi copia del PDF contenente i codici e gli venga quindi visualizzato a video il contenuto del pdf appena scaricato.

- Successivamente all'accesso alla funzione di recupero dei codici, gli stessi vengono cancellati tramite rimozione del record da DB.

5.6 MODALITÀ DI CONSEGNA E ABILITAZIONE DEI DISPOSITIVI OTP

I dispositivi fisici OTP vengono assegnati e consegnati al Titolare dal RAO, successivamente all'identificazione e registrazione dello stesso, ovvero inviati tramite raccomandata A/R in busta chiusa all'indirizzo di residenza indicato nel documento di identificazione. La procedura di assegnazione prevede che:

1 il RAO, attraverso la propria area riservata del portale CMS, registri il numero seriale del dispositivo OTP assegnandolo al Titolare;
2 stampi il modulo di richiesta del certificato contenente il Codice Dispositivo Virtuale;
3 il Titolare sottoscriva il predetto modulo mediante firma autografa o digitale (sfruttando certificati di sottoscrizione validi eventualmente già in suo possesso).

I dispositivi vengono rilasciati non attivi e, prima del loro utilizzo, dovrà necessariamente essere effettuata la procedura di abilitazione, che prevede:

- accedere con le proprie credenziali all'URL: https://cms.firmacerta.it/areaPrivata;
- aprire la sezione "Abilitazione OTP" ed eseguire la procedura di abilitazione del dispositivo OTP seguendo le istruzioni mostrate a video.

5.7 MODALITÀ DI GENERAZIONE DELL'ACCOUNT DI FIRMA REMOTA

Per l'utilizzo del servizio di firma remota è necessario eseguire la procedura di generazione dell'account di firma, che prevede:

- di accedere con le proprie credenziali all'URL: https://cms.firmacerta.it/areaPrivata;

- se non già fatto in precedenza, che il Titolare debba cambiare la password d'accesso all'Area Privata assegnata automaticamente con una scelta autonomamente;
- l'effettuazione della procedura di abilitazione dell'OTP (in caso di dispositivi fisici) come descritto al Paragrafo 5.6;
- l'utilizzo della sezione denominata *"Prima Attivazione"*;
- di selezionare il tipo di dispositivo da attivare (Disp. Firma Remota) ed inserire i seguenti dati:
    - PIN della chiave (arbitrariamente scelto);
    - codice di emergenza (arbitrariamente scelto rispettando le politiche di enforcement definite dall'applicazione);
    - codice OTP.

Se tutti i codici sono corretti il sistema avvia la generazione delle chiavi e rilascio del certificato (§ 5.4.7) comunicando l'esito dell'operazione all'utente con un messaggio di avvenuta attivazione.

5.7.1 MODIFICA DEI CODICI DEL TITOLARE

In qualsiasi momento successivo alla generazione del certificato, il Titolare potrà modificare il *Codice Emergenza* e il *PIN*. Il *Codice Dispositivo Virtuale* non potrà in nessun modo essere modificato.

5.7.1.1 MODIFICA CODICE EMERGENZA

La procedura di modifica del *Codice Emergenza* necessita che il Titolare esegua le operazioni seguenti:

- Accedere alla propria Area Privata;
- Selezionare la funzione di modifica Codice Emergenza;
- Digitare due volte il nuovo Codice Emergenza;
- Digitare l'OTP.

5.7.1.2 MODIFICA PIN

La procedura di modifica del *PIN* necessita che il titolare esegua le operazioni seguenti.:

- Accedere alla propria *Area Privata;*
- Selezionare la funzione di modifica *PIN;*
- Digitare il vecchio *PIN;*
- Digitare due volte il nuovo *PIN;*
- Digitare l'OTP.

5.8 REVOCA E SOSPENSIONE DEL CERTIFICATO QUALIFICATO(L)

La sospensione o revoca del certificato avviene nel rispetto degli articoli da 22 a 29 del [05], determina la fine della validità prima della scadenza naturale e invalida 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 dall'art. 18, comma 4, della [08] e successive modificazioni.
Il Certificatore può anticipare l'emissione della CRL in circostanze particolari.
La data della pubblicazione della lista, 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 dispositivo di firma.
La sospensione del certificato comporta la **non validità** delle firme generate durante il periodo di 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.

5.8.1 MOTIVI PER LA REVOCA O SOSPENSIONE DEL CERTIFICATO

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. [03];
- 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.

La sospensione può avvenire in seguito alle seguenti circostanze:

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

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

5.8.2 MODALITÀ PER LA REVOCA O SOSPENSIONE DEL CERTIFICATO

La richiesta di revoca o sospensione del certificato qualificato viene inoltrata per iscritto al Certificatore compilando in tutte le sue parti l'apposito modulo messo a disposizione sul sito del Certificatore.
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[1] della stessa.
Il Certificatore verifica l'autenticità della richiesta e procede alla revoca del certificato inserendo lo stesso nella lista dei certificati revocati e sospesi (CRL) da lui gestita.

[1] La data di fine non deve essere successiva alla data di scadenza del certificato.

5.8.3 SOSPENSIONE IN EMERGENZA

Il Titolare, in caso di smarrimento/compromissione della chiave privata o dei codici che ne consentono l'utilizzo, richiede tempestivamente al Certificatore la sospensione del certificato.
La richiesta può essere inoltrata:

- telefonicamente[1] al servizio di Help Desk (§ 2.3);
- via Web[2] inserendo il codice di emergenza o OTP.

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

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.

5.8.4 MODALITÀ PER L'INOLTRO DELLE RICHIESTE

La revoca, la sospensione o la riattivazione del certificato può essere richiesta 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 (fisico o virtuale),
    - codice d'emergenza o OTP.
- **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.

[1] Al cliente verranno richiesti alcuni dati personali per assicurare la leicità della richiesta.
[2] Il sito web è accessibile in modalità 24h x 7gg.

5.8.5 TEMPI PER LA GESTIONE DELLE RICHIESTE

Le richieste di revoca, sospensione e riattivazione dei certificati qualificati, saranno gestiti entro un giorno lavorativo dal ricevimento della richiesta, 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.

5.8.6 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 via e-mail, al Terzo Interessato, l'avvenuta revoca o sospensione;
- se la richiesta è su iniziativa del Terzo Interessato, il Certificatore comunica via e-mail, al Titolare e al Terzo Interessato, l'avvenuta revoca o sospensione del suo Certificato;
- se la richiesta è su iniziativa del Certificatore, il Certificatore comunica via e-mail, al Titolare, l'intenzione di revocare o sospendere il Certificato, indicando la motivazione nonché la data e l'ora di decorrenza; 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.

5.9 MODALITÀ DI SOSTITUZIONE DELLE CHIAVI(M)

5.9.1 SOSTITUZIONE DELLE CHIAVI DI SOTTOSCRIZIONE DEGLI UTENTI

La durata massima di un Certificato qualificato è di 6 (sei) anni. La richiesta di rinnovo delle chiavi deve essere effettuata prima della scadenza del Certificato (dal 45° giorno prima della data di scadenza).
Il rinnovo del Certificato può essere fatto solo dal Certificatore qualificato che l'ha emesso ed il Titolare può procedere a tale operazione mediante la procedura remota disponibile nel software "FirmaCerta", messo a disposizione dal Certificatore.

La procedura di rinnovo prevede:

- l'eventuale aggiornamento dei dati relativi al Titolare con le informazioni fornite dal Terzo Interessato;
- la verifica del possesso del dispositivo di firma contenente il certificato in scadenza, mediante procedura remota (§ 5.3.2.2);
- la generazione di una nuova coppia di chiavi sul dispositivo sicuro di firma ed emissione di un nuovo certificato, mediante procedura remota (§ 5.3.2.2);
- la registrazione sul Giornale di Controllo dell'avvenuta operazione.

Se nel Certificato qualificato sono presenti anche informazioni relative al Ruolo e all'Organizzazione, il Certificatore provvederà ad inserirle nel nuovo certificato verificando, al momento del rinnovo, che non sia pervenuta la revoca del certificato dal Terzo Interessato.

Qualora le informazioni relative al Ruolo e all'Organizzazione contenute nel certificato da rinnovare non siano più valide al momento del rinnovo, al Titolare che intenda effettuare il rinnovo attraverso la procedura remota verrà rilasciato un certificato privo di tali informazioni.
Nel caso di richiesta effettuata dopo la scadenza del certificato si procederà ad una nuova registrazione ed emissione.
Qualora si rendesse necessaria la sostituzione del Certificato qualificato, a causa di variazioni delle informazioni in esso contenute, si procederà con la revoca di tale certificato e/o con una nuova emissione.

5.9.2 SOSTITUZIONE DELLE CHIAVI DI MARCATURA TEMPORALE(ART. 49)

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. 49, comma 2 del [05].
I certificati relativi alle chiavi di marcatura temporale hanno durata massima pari a 11 (undici) anni.

5.9.3 SOSTITUZIONE DELLE CHIAVI DI CERTIFICAZIONE(ART. 30)

Avviene nel rispetto dell'art. 30 del [05].
Il Certificato "Root" della CA utilizzata dal Certificatore per sottoscrivere i Certificati qualificati del Titolare ha durata 20 anni e viene sostituito ogni 8 anni per garantire la fruibilità di tutti i certificati emessi fino alla naturale scadenza degli stessi.

5.10 STRUMENTI E MODALITÀ PER L'APPOSIZIONE E LA VERIFICA DELLA FIRMA DIGITALE(R, S)

Gli strumenti messi a disposizione dal Certificatore consentono di effettuare firme di tipo PAdES, CAdES e XAdES. Maggiori informazioni sulle tipologie di firme utilizzabili possono essere reperite sul sito http://www.agid.gov.it/.

Per l'apposizione della firma digitale sono previste due modalità:

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

Nei paragrafi che seguono si riportano le modalità operative per entrambi i casi.

5.10.1 FIRMA CON DISPOSITIVO DI FIRMA PERSONALE

Namirial mette gratuitamente a disposizione degli utenti un software denominato "FirmaCerta" che consente, con facilità d'uso, di eseguire tutte le operazioni relative alla firma digitale. Nello specifico il software consente, per ogni singolo file:

- La Firma Digitale;
- La Marcatura Temporale;
- La Verifica della Firma e della Marca Temporale;
- La Controfirma di un file (validazione);
- La Firma Grafometrica.

Tra le funzionalità offerte dal prodotto "FirmaCerta" vi è inoltre la possibilità di:

- firmare contemporaneamente grandi volumi di documenti digitali, come fatture, polizze, ricevute di pagamenti, bonifici e qualsiasi altro documento digitale;
- firmare i documenti PDF mantenendo il formato originale;
- scegliere il dispositivo hardware col quale si desidera apporre la firma (Smart Card, Token);
- apporre/associare una marca temporale ad un documento o ad una firma (Grafometrica);
- selezionare i file con il drag & drop di uno o più file all'interno della stessa finestra di firma;
- firmare i documenti PDF protetti da password, previa conoscenza della stessa.

I prerequisiti hardware e software nonché tutte le indicazioni per l'installazione del prodotto "FirmaCerta" sono riportate nella "Guida rapida all'utilizzo" del software, reperibile al seguente URL:

- http://www.firmacerta.it/manuali.php

Nel documento, che è parte integrante del presente Manuale Operativo, sono riportate le modalità operative per effettuare la generazione e la verifica della firma digitale.
Alcuni formati di documenti permettono di inserire del codice eseguibile (macro o comandi) all'interno del documento senza che questo ne alteri la struttura binaria e tali da attivare funzionalità che possono modificare gli atti, i fatti o i dati rappresentati nel documento medesimo. Si ricorda che i file firmati digitalmente che contengono tali strutture non producono gli effetti di cui all'articolo 21, comma 2 del CAD ed è cura del Titolare assicurarsi, tramite le funzionalità tipiche di ciascun prodotto, dell'assenza di tali codici eseguibili.
In Appendice A sono riportate le modalità operative, in riferimento ad alcuni formati di larga diffusione, per accertarsi che il documento non contenga macroistruzioni o codici eseguibili.

5.10.2 FIRMA CON APPLICAZIONI DI FIRMA AUTOMATICA

L'utente utilizza un'applicazione "client" di firma fornita dal Certificatore o dal Cliente (es. impresa, banca, ente pubblico, ecc.) che eroga servizi applicativi ad utenti interni o esterni. Le specifiche modalità per l'esecuzione della firma dipendono quindi dalla particolare applicazione client usata dagli utenti e vengono all'occorrenza descritte caso per caso dagli addendum al manuale operativo.
La soluzione fornita dal Certificatore è composta da due componenti:

- **HSM ed il server SignEngine (di seguito SE) che lo controlla e lo pilota.** SE è responsabile della firma a basso livello degli hash dei documenti.
- **Il server SignWebServices (di seguito SWS).** È la componente capace di apporre e verificare le firme ad un alto livello di astrazione. Si integra con i sistemi del cliente (custom o legacy). Necessita di comunicare con la componente SE, ma può essere dislocata altrove. SWS esegue l'imbustamento nei vari formati supportati e calcola gli hash da far firmare a SE.

Si configurano pertanto due differenti scenari di utilizzo:

- **HSM presso il CED del cliente.** Tale configurazione è preferibile nel caso si debba produrre un numero considerevole di firme e garantisce maggiori risultati in termini di performance poiché l'HSM è dedicato e non ci sono ritardi di rete apprezzabili in quanto tutte le comunicazioni avvengono su LAN. In questo scenario sia la componente SE che SWS sono istallate presso il cliente.
- **HSM presso Namirial.** Con questa configurazione il cliente si limita ad effettuare l'integrazione tra i suoi sistemi e la componente SWS, disinteressandosi dell'acquisto e dell'esercizio dell'HSM. In questo scenario il cliente necessita della sola componente SWS o dell'applicazione di firma remota fornita dal Certificatore.

Il sistema di firma automatica, basato su HSM, può essere quindi ospitato presso il data center del Certificatore oppure presso il data center del Cliente; nel secondo caso, il Cliente deve rispettare i requisiti di sicurezza fisica, logica, operativa e gestionale indicati dal Certificatore, il quale svolgerà verifiche periodiche sul rispetto di tali requisiti in conformità all'articolo 3, comma 5 del [05].
Le componenti *SE* e *SWS* stabiliscono autonomamente connessioni sicure sempre protette tramite i protocolli TLS/SSL, con autenticazione del server e cifratura della sessione con chiavi simmetriche di almeno 128 bit e, in conformità all'art. 42 comma 6 del [05], non consentono al Certificatore di conoscere gli atti o fatti rappresentati nel documento informatico oggetto del processo di sottoscrizione o verifica.
La richiesta di firma proveniente dal client è autenticata con username e password. Gli utenti accedono al server esclusivamente attraverso una rete locale (LAN) non raggiungibile da Internet e il certificato di firma contiene le opportune limitazioni d'uso.

5.10.3 FIRMA CON APPLICAZIONI DI FIRMA REMOTA

Per l'apposizione della firma in modalità remota, sarà possibile utilizzare applicazioni distribuite dal Certificatore o dal Cliente (es. impresa, banca, ente pubblico, ecc) che eroga servizi applicativi ad utenti interni o esterni. Le specifiche modalità per l'esecuzione della firma dipendono quindi dalla particolare applicazione usata dagli utenti e vengono all'occorrenza descritte caso per caso dagli addendum al manuale operativo. La richiesta di firma proveniente dall'utente è sempre autenticata con due fattori. La modalità standard si basa sull'uso di un PIN statico (primo fattore) accompagnato da una password dinamica OTP (One-Time Password) che può essere, a seconda dei casi:

- token fisico
- token mobile
- token SMS

Modalità alternative di autenticazione forte possono essere implementate, a fronte di situazioni specifiche che lo giustifichino e sempre con l'esplicita approvazione preventiva dell'Agenzia per l'Italia Digitale.

Gli strumenti forniti dal Certificatore sono i seguenti:

- FirmaCerta
- FirmaCertaMobile
- FirmaCertaWeb

FirmaCerta è un'applicazione desktop installabile su postazioni di lavoro dotate di sistema operativo Microsoft Windows. I prerequisiti hardware e software nonché tutte le indicazioni per l'installazione del prodotto "FirmaCerta" sono riportate nella "Guida rapida all'utilizzo" del software, reperibile al seguente URL:

- http://www.firmacerta.it/manuali.php

Nel documento, che è parte integrante del presente Manuale Operativo, sono riportate le modalità operative per effettuare la generazione e la verifica della firma digitale.

FirmaCertaMobile è un'applicazione mobile, sviluppata dal Certificatore, installabile su dispositivi dotati di sistema operativo Android e IOS;

FirmaCertaWeb è un'applicazione web utilizzabile per la firma e la verifica delle firme mediante i browser comunemente usati ed è disponibile al seguente URL:

- https://sws.firmacerta.it/SignEngineWeb/

In ogni caso l'apposizione della firma richiederà che l'utente inserisca i seguenti codici:

- Codice Dispositivo Virtuale[1]
- PIN[2]
- OTP

Per questioni di usabilità, nei soli casi delle applicazioni *FirmaCerta* e *FirmaCertaMobile*, il Titolare potrà memorizzare al loro interno il *Codice Dispositivo Virtuale* per non doverlo digitare tutte le volte. Gli altri codici quali PIN e OTP saranno comunque sempre indispensabili e da digitare ogni volta.

Il Certificatore addotta dei sistemi che gli rendono impossibile la conoscenza o la modifica del codice PIN, sarà cura del Titolare gestire detto codice, senza il quale il certificato associato non potrà essere utilizzato per l'apposizione di nuove firme.
In caso non si disponga più del codice *PIN* al Titolare è consigliato di procedere immediatamente alla sospensione del certificato associato, secondo la procedura descritta al Paragrafo 5.8.2.

Si precisa inoltre che le applicazioni server utilizzate nell'ambito del servizio di firma remota adottano specifiche misure di sicurezza, in conformità all'art. 42 comma 6 del [05], e non consentono al Certificatore di conoscere gli atti o fatti rappresentati nel documento informatico oggetto del processo di sottoscrizione o verifica.

5.11 MODALITÀ PER L'APPOSIZIONE E LA DEFINIZIONE DEL RIFERIMENTO TEMPORALE (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 che coincide con il momento della sua generazione, con una differenza non superiore ad un minuto secondo rispetto alla scala di tempo UTC (IEN), del [09],
- la marcatura viene consegnata al Titolare, in modalità sicura, per l'utilizzo.

L'impronta dell'evidenza informatica è calcolata utilizzando la funzione 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.

Per ulteriori informazioni di dettaglio sul servizio di emissione delle marche temporali si fa riferimento al documento specifico del servizio, ovvero il documento "Time-Stamping Authority Practice Statement" (NAMIRIAL TSA PS).

[1] Tale informazione è presente all'interno del modulo sottoscritto dal Titolare.
[2] Impostato dal Titolare in fase di generazione delle chiavi.

5.11.1 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.

5.11.2 PRECISONE DEL RIFERIMENTO TEMPORALE(ART. 51)

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 due sistemi di sincronizzazione:

- una sonda esterna connessa al sistema della rete satellitare GPS,
- il servizio NTP messo a disposizione da INRIM.

L'accuratezza del sistema di riferimento temporale è pari a 1 secondo. La tolleranza, come richiesto dalla normativa vigente, non è mai superiore al minuto secondo rispetto alla scala di tempo UTC (IEN) del [09].

6 PROTEZIONE DEI DATI PERSONALI(K)

Di seguito vengono descritte le procedure e le modalità operative che Namirial S.p.A., in qualità di titolare del trattamento dei dati personali, adotta nello svolgimento della propria attività. Le informazioni personali, concernenti i titolari dei certificati e, più in generale i clienti del servizio erogato vengono trattate, conservate e protette in conformità a quanto previsto nel Regolamento europeo 679/2016 in materia di protezione dei dati personali

6.1 STRUTTURA ORGANIZZATIVA DI NAMIRIAL S.P.A.

Namirial S.p.A. è il **Titolare del trattamento dei dati personali**, secondo quanto previsto dal Regolamento europeo 679/2016 in materia di protezione dei dati personali. Il responsabile della protezione dei dati, DPO, è Serena Donegani.
Namirial S.p.A. individua e nomina gli incaricati al trattamento che operano sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle istruzioni dagli stessi impartite.

6.2 TUTELA E DIRITTI DEGLI INTERESSATI

Namirial S.p.A. garantisce la tutela degli interessati, in ottemperanza al Regolamento europeo 679/2016 in materia di protezione dei dati personali. In particolare, fornisce agli interessati tutte le informazioni necessarie, in relazione al diritto di accesso ai dati personali ed agli usi degli stessi, consentiti dalla legge.
L'accesso ai propri dati da parte degli interessati è consentito tramite richiesta scritta, a mezzo del format scaricabile dal sito web di Namirial ww.namirial.com da far pervenire al responsabile per la protezione dei dati anche tramite e-mail all'indirizzo s.donegani.dpo@namirial.com che provvederà ad evadere la richiesta senza ingiustificato ritardo.
Gli interessati devono prestare consenso scritto al trattamento dei propri dati da parte di Namirial S.p.A.

6.3 MODALITÀ DEL TRATTAMENTO

Tutte le informazioni personali, acquisite durante l'erogazione dei servizi , vengono trattate da Namirial che adotta le misure di sicurezza, descritte all'interno del presente manuale allo scopo di prevenirne la perdita, evitarne usi illeciti o accessi da parte di personale non espressamente autorizzato.
I dati in formato elettronico vengono conservati in appositi data server adibiti allo scopo e su supporti ottici all'interno di armadi protetti.

Namirial S.p.A. si riserva l'opportunità di conservare i dati cartacei presso la propria sede centrale, all'interno di archivi cartacei cui hanno accesso solo gli incaricati espressamente autorizzati.

6.4 FINALITÀ DEL TRATTAMENTO

I dati personali vengono acquisiti in osservanza alle finalità esplicitate nell'informativa fornita al richiedente durante le fasi di richiesta del certificato. L'informativa è anche pubblicata su https://docs.namirialtsp.com/privacy/.
Di seguito, elencate, le finalità del trattamento.

- gestione del rapporto contrattuale;
- eventuali controlli sulla qualità del servizio e sulla sicurezza del sistema;
- attività di natura commerciale, effettuata tramite invio di informative legate alla emissione di prodotti e/o servizi analoghi o direttamente connessi ai servizi di certificazione e marca temporale.

L'interessato ha la possibilità di opporsi al trattamento dei dati personali, avente ad oggetto tale tipologia di comunicazioni.

6.5 ALTRE FORME DI UTILIZZO DEI DATI

I dati personali possono essere usati con finalità diverse rispetto alla fornitura dei servizi descritti dal presente manuale e possono essere comunicati a soggetti pubblici, quali forze dell'ordine, autorità pubbliche e autorità giudiziarie, qualora gli stessi soggetti ne facciano richiesta per motivi di ordine pubblico e nel rispetto delle disposizioni di legge per la sicurezza e difesa dello Stato, la prevenzione, l'accertamento e/o la repressione dei reati.

6.6 SICUREZZA DEI DATI

In ottemperanza normativa vigente, Namirial S.p.A. adotta tutte le misure di sicurezza necessarie al fine di ridurre al minimo:

- i rischi di distruzione o perdita, anche accidentale, dei dati;
- i rischi di danneggiamento di risorse hardware sulle quali siano memorizzati i dati;
- i rischi di danneggiamento ai locali nei quali siano custoditi i dati;
- l'accesso non autorizzato ai dati;
- le attività di trattamento non consentite dalla legge o dai regolamenti aziendali

Attraverso le misure di sicurezza adottate da Namirial vengono inoltre garantite:

- l'integrità e la salvaguardia dei dati, contro manomissioni o modifiche da parte di soggetti non autorizzati
- la disponibilità dei dati e la loro conseguente fruibilità;
- la riservatezza dei dati ovvero la garanzia che alle informazioni abbiano accesso le sole persone autorizzate.

7 APPENDICE A: MACRO E COMANDI(ART. 44)

Istruzioni macro o codici eseguibili presenti all'interno del documento che modifichino gli atti ed i fatti rappresentati nel documento stesso invalidano la firma (art. 4, comma 3 del [05]). È cura del Titolare assicurarsi, tramite le funzionalità tipiche di ogni prodotto, dell'assenza di tali codici eseguibili.
Di seguito si riportano i passaggi utili a disabilitare le istruzioni macro o codici eseguibili per i prodotti maggiormente diffusi. Per i dettagli si rimanda 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 su Opzioni,
- cliccare su Centro protezione,
- posizionarsi su Impostazioni Centro protezione,
- cliccare su Disattiva tutte le macro con notifica.

MS Word® 2010/2013 e MS Excel® 2010/2013
Per disattivare le macro seguire i seguenti passi:

- cliccare sul pulsante File,
- cliccare su Opzioni,
- cliccare su Centro protezione,
- posizionarsi su pulsante 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,
- rimuovere il flag di abilitazione del JavaScript.