Addendum Manuale Operativo

Certificati di Firma Remota

Certificatore	**Namirial S.p.A.**	Modello Doc.	**NAM-FDMT-MO-ADD-FR**
Redatto da	**Simone Baldini**	Nota di riservatezza	**DOCUMENTO PUBBLICO**
Revisionato da	**Antonio Taurisano**	Revisione	**1.1**
Approvato da	**Enrico Giacomelli**	Data	**24/04/2020**

GIACOMELLI EN
2020.05.04 09:54:43
Namirial S.p.A.
Il legale rappresentante
(Dott. Enrico Giacomelli)
CN=GIACOMELLI ENRICO
2.5.4.4=GIACOMELLI
2.5.4.42=ENRICO
RSA/2048 bits

Indice

Indice delle tabelle

Storia delle modifiche

Versione	**1.1**
Data	24/04/2020
Motivazione	Prima emissione.
Modifiche	- Estensione della sezione definizioni; - Aggiornamento della sezione certificazioni; - Estensione degli obblighi per la LRA; - Estensione modalità di riconoscimento;

Versione	**1.0**
Data	06/06/2016
Motivazione	Prima emissione.
Modifiche	Manuale Operativo per richiesta, emissione e uso della Firma Digitale con certificati per firma remota.

1 Introduzione

1.1 Scopo e campo di applicazione

Il presente documento rappresenta un **Addendum al Manuale Operativo del servizio di certificazione digitale erogato da Namirial S.p.A** e ha come scopo la descrizione delle regole e delle procedure operative adottate dal Certificatore per l'emissione di certificati digitali per firma remota.

1.2 Riferimenti tecnici e normativi

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)*
[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]	REGOLAMENTO (UE) 2016/679	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
[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.*

Num	Normativa	Descrizione
[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 attività criminose e di finanziamento del terrorismo nonché' 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]	Direttiva 2005/60/CE	Direttiva 2005/60/CE del Parlamento europeo e del Consiglio, del 26 ottobre 2005, *relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo*
[24]	Direttiva 2006/70/CE	Direttiva 2006/70/CE DELLA COMMISSIONE del 1° agosto 2006 recante misure di esecuzione della direttiva 2005/60/CE del Parlamento europeo e del Consiglio *per quanto riguarda la definizione di «persone politicamente esposte» e i criteri tecnici per le procedure semplificate di adeguata verifica della clientela e per l'esenzione nel caso di un'attività finanziaria esercitata in modo occasionale o su scala molto limitata*
[25]	Direttiva (UE) 2015/849	Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, *relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione.*

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].
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
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 in possesso solo al Titolare che la utilizza per firmare digitalmente i documenti.

Termine o acronimo	Significato
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. In Italia la carta d'identità cartacea è destinata ad essere sostituito da questo documento.
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	Un dispositivo per la creazione di una Firma elettronica che soddisfi i requisiti di cui all'allegato II di eIDAS
eIDAS	Il Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;
GdC - 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.
IR	È un soggetto, appartenente ad una Società Terza, che può 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 MO per quanto concerne le fasi di identificazione della persona fisica cui è attribuita la firma digitale.
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. La 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.
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.

Termine o acronimo	Significato
RA	Registration Authority, soggetto che esegue l'identificazione dei Richiedenti dei certificati qualificati applicando le procedure definite dal Certificatore.
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.
SBA – Sistema Biometrico di Autenticazione	Correlazione tra persona fisica e le sue caratteristiche fisiologiche e/o comportamentali
SCA	Signature Creation Application. Applicazione, web o non, in grado di effettuare l'operazione di firma di documenti, gestendo opportunamente formati ed opzioni.
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.
SYK	Acronimo per Something You Know. In un processo d'autenticazione solitamente è la password.
SYH	Acronimo per Something You Have. In un processo d'autenticazione solitamente è l'OTP fornito ad esempio da un token o da una mobile application.
SYA	Acronimo per Something You Are. In un processo d'autenticazione solitamente è una informazione di tipo biometrico.
Terzo Interessato	È la persona 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	E' il Firmatario, ovvero una persona fisica che crea una Firma elettronica
X.509	È uno standard ITU-T per le infrastrutture a chiave pubblica (PKI).

Tabella 2: Definizioni e Acronimi

2 Il Certificatore

2.1 Dati identificativi del Certificatore

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 della Portale rivolto al Titolare:	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 Qualificata e accreditata presso AgID (ex DigitPA) ed è autorizzata all'emissione di certificati qualificati conformi al Regolamento (UE) n. 910/2014 del Parlamento Europeo e del consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE 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.

Gestore SPID, dal 13/04/2017, accreditato presso AgID (ex DigitPA) e certificato (IT273825) ai sensi del:

- DPCM 24/10/2014;
- Regolamento di attuazione UE 2015/1502 della Commissione
- Regolamento (UE) 910/2014 eIDAS, art. 24

per la prestazione di servizi fiduciari di Identificazione Digitale.

Conservatore, dal 13/03/2015, accreditato presso AgID (ex DigitPA) e certificato (IT 277150) ai sensi del:

- DPCM 3 dicembre 2013;
- Regolamento (UE) 910/2014 eIDAS, art. 24;

per la prestazione di servizi fiduciari di Conservazione a Norma.

Certificata ISO 9001:2015. 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).

2.3 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 dalle 9.00 alle 13.00 e dalle ore 14.00 alle 19.00.

2.4 Versione del documento

Il presente documento denominato "**NAM-FDMT-MO-ADD-FR**" è identificato attraverso il livello di revisione e la data di rilascio presente su tutte le pagine. Nel preambolo del documento è inoltre riportata 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 il Manuale Operativo, sono custoditi presso la sede del Certificatore ma sono depositati presso 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 URL è altresì 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

La responsabilità del presente Addendum al 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:

- telefono: (+39) 071 63494
- e-mail: firmacerta@namirial.com
- fax: (+39) 071 60910

3 Regole Generali

3.1 Attori coinvolti nei processi

Gli attori indicati nel presente documento sono:

- il Certificatore
- la Registration Authority (RA)
- la Local Registration Authority (LRA)
- l'Incaricato della Registrazione (IR)
- il Titolare
- il Terzo Interessato

3.2 Obblighi del Certificatore, del Titolare e dei Richiedenti la verifica delle firme

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;
2. provvede con certezza all'identificazione della persona che fa richiesta della certificazione;
3. si accerta dell'autenticità della richiesta di certificazione;
4. 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;
5. 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;
6. 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;
7. non si rende depositario, nella loro interezza, dei dati per la creazione della firma del Titolare;
8. non copia, né duplica, le chiavi private di firma del soggetto cui il certificatore ha fornito il servizio di certificazione;
9. assicura la precisa determinazione della data e dell'ora di rilascio, scadenza, revoca e sospensione dei certificati qualificati;
10. 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;
11. 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;
12. rende accessibile, per via telematica, la copia delle liste, sottoscritte da AgID, dei certificati relativi alle chiavi di Certificazione di cui al [05];
13. fornisce almeno un sistema che consenta al Titolare di effettuare la verifica della firma qualificata;
14. 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. mantenere in modo esclusivo e conservare con la massima diligenza il dispositivo OTP eventualmente fornito;
4. non utilizzare la firma qualificata per funzioni e finalità diverse da quelle per la quale è stata rilasciata;
5. 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;
6. 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.

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).

3.2.4 Obblighi della Registration Authority Locale (LRA)

La LRA 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 il dispositivo OTP eventualmente fornito;
3. richiedere, quando previsto e prima di rilasciare il certificato, la prova del possesso della chiave privata e verificare la correttezza della coppia di chiavi;
4. informare il titolare delle misure di sicurezza adottate per il trattamento dei dati personali, ai sensi del [06];
5. provvedere con certezza all'identificazione della persona che fa richiesta della certificazione;
6. accertare l'autenticità della richiesta di certificazione;
7. comunicare al Certificatore tutti i dati e documenti acquisiti durante l'identificazione del Titolare e previsti dalle procedure del Certificatore al fine di attivare tempestivamente la procedura di emissione del certificato;
8. verificare ed inoltrare al Certificatore le richieste di revoca/sospensione richieste dal Titolare presso LRA;
9. attenersi scrupolosamente alle regole impartite dal Certificatore e presenti su questo documento e, se del caso, nel Manuale Operativo;
10. assicurarsi che il Richiedente e Titolare abbiano preso visione delle Condizioni Generali di contratto;
11. consegnare al Richiedente e Titolare copia della documentazione di richiesta di emissione del Certificato dagli stessi sottoscritta.

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 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

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 non si assume la 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

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 fornito dal Titolare.

3.5 Tariffe

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

4 Policy, limiti d'uso e gestione dei certificati

4.1 Certificate Policy

Il Certificatore utilizza i seguenti Object Identifier, (OID):

1.3.6.1.4.1.36203	Namirial S.p.A.
1.3.6.1.4.1.36203.1	CA FirmaQualificata
1.3.6.1.4.1.36203.1.1	Policy CA FirmaQualificata

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

1.3.6.1.4.1.36203.1.1.5	Policy per certificati qualificati associati ad apparato sicuro per la creazione della firma mediante procedura remota.

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

4.2 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.
- 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).*

Si precisa che il soggetto indicato nella limitazione di cui sopra è da intendersi la persona giuridica che funge da terzo interessato e/o LRA.

4.3 Informazioni contenute nei certificati per la firma remota

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.

4.4 Registro dei certificati

Il registro dei certificati contiene:

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

4.4.1 Accesso al registro dei certificati

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.
Le CRL relative ai certificati qualificati e di autenticazione sono distinte da un numero progressivo, posizionato prima dell'estensione del file.
I certificati sospesi e revocati sono inseriti e pubblicati nella stessa CRL già descritta nel Manuale Operativo ed è pubblicata agli indirizzi:

- http://crl.firmacerta.it/FirmaCertaQualificata1.crl (per i certificati emessi con Issuer CN=Name Namirial CA Firma Qualificata)
- http://crl.namirialtsp.com/QES.crl (per i certificati emessi con Issuer CN=Namirial Qualified e-Signature

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

4.4.2 Gestione del registro dei certificati

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.

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 Modalità di identificazione e registrazione

Il Titolare richiedente può essere identificato:

- dal personale autorizzato del Certificatore o dagli uffici di registrazione LRA;
- dal Referente del Terzo Interessato che ha sottoscritto una Convenzione;
- attraverso la propria identità elettronica associata ad un certificato di firma digitale, ad una CNS o CIE, ovvero a credenziali SPID di livello pari almeno a 2;
- attraverso il riconoscimento già effettuato da un intermediario finanziario o altro soggetto esercente l'attività finanziaria;
- attraverso il riconoscimento effettuato da un pubblico ufficiale.
-

Nei successivi paragrafi si riportano i dettagli delle suddette modalità.

5.1.1 Identificazione tramite personale autorizzato del Certificatore o dagli uffici di registrazione LRA

Il Titolare richiedente può 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 può altresì essere identificato per via telematica attraverso il sistema di identificazione remota "ViSI" del Certificatore o sistema equivalente; 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 oppure uno smartphone, tablet, o altri dispositivi informatici con caratteristiche equivalenti.
Per garantire la tutela e la gestione dei propri dati personali in piena aderenza al Regolamento (UE) 2016/679 (GDPR), ad ogni richiedente verrà preventivamente fornita l'informativa sulla privacy e richiesto il consenso alla videoregistrazione ed al trattamento dei dati da parte degli incaricati del Certificatore. Ciascun richiedente sarà altresì informato circa il fatto che per ragioni di sicurezza la videochiamata (video/voce) sarà registrata e conservata - senza soluzione di continuità - 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 videoconferenza 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, il certificatore conserva per una durata almeno ventennale i dati di registrazione, costituiti da file audio video e metadati strutturati in formato elettronico. Tale procedura in uso soddisfa quanto richiesto dall'art. 32, comma 3, lettera a) del CAD. Il file audio/video è costituito dall'intera sessione audio video utilizzata per la registrazione utente.
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 o da Esso riconosciuto. 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 non idoneo all'identificazione certa.
Detto soggetto conclude il processo registrando gli estremi del documento presentato. Sono quindi raccolte informazioni quali il periodo di validità, l'Ente emettitore, il tipo del documento etc.

5.1.2 Identificazione da parte del Referente del Terzo Interessato che ha sottoscritto una convenzione

Il Terzo Interessato, nella persona del Referente:

- Struttura l'elenco dei Titolari oggetto di certificazione accludendo le informazioni necessarie per la registrazione (anagrafica, estremi del documento di riconoscimento, tipo prodotto richiesto, eventuale ruolo ricoperto, eventuali limitazioni d'uso, etc).
- Comunica detto elenco al Certificatore utilizzando modalità che diano garanzie di autenticità, provenienza e integrità;
- S'incarica di ottenere accettazione e conferma da parte dei Titolari di voler procedere con l'emissione del certificato.

5.1.3 Identificazione attraverso la propria identità elettronica associata ad un certificato di firma digitale, ad una cns o cie, ovvero a credenziali spid di livello 2 o superiore

In tale modalità il Certificatore si basa su riconoscimento già effettuato da Namirial o da altri soggetti accreditati. Il Titolare deve essere in possesso di credenziali o di strumenti elettronici atti all'identificazione forte.

5.1.3.1 Autenticazione mediante firma digitale

Questa modalità prevede che il Richiedente compili il modulo di richiesta previsto per il rilascio della firma digitale (NAM_CA02 o derivati), che lo sottoscriva mediante firma elettronica qualificata e che sottometta a sistema il documento firmato. Una procedura automatizzata effettua i seguenti controlli:

- Validità della firma;
- Coincidenza del firmatario del modulo con il Richiedente;
- Che una copia dello stesso documento di richiesta non sia già stata utilizzata per ottenere un altro certificato di firma digitale.

5.1.3.2 Autenticazione mediante strumenti di identificazione elettronica

Questa modalità prevede che il richiedente sia in possesso di un mezzo di identificazione elettronica preesistente:

- Notificato dallo Stato Membro ai sensi dell'articolo 9 del Regolamento eIDAS, di livello elevato;
- Notificato dallo Stato Membro ai sensi dell'articolo 9 del Regolamento eIDAS, di livello significativo, a patto che fornisca una garanzia equivalente sotto il profilo dell'affidabilità alla presenza fisica;
- Non notificato ed emesso da una autorità pubblica o un soggetto privato, a condizione che fornisca una garanzia equivalente alla presenza fisica sotto il profilo dell'affidabilità, e questa sia confermata da un organismo di valutazione della conformità.

Nello specifico, relativamente allo Stato Italia vengono riconosciuti come mezzi di identificazione elettronica adatti al riconoscimento:

a. la tessera CNS (Carta nazionale dei Servizi);
b. la TS-CNS (Tessera Sanitaria – Carta Nazionale dei Servizi);
c. la CIE (Carta di Identità Elettronica)
d. la CRS (Carta Regionale dei Servizi)
e. Le identità digitali rilasciate nel contesto del sistema SPID di livello 2 o superiore.

Nei casi a,b,c,d di cui sopra il Richiedente, previo inserimento del PIN, effettua l'autenticazione sul portale del Certificatore o del CIE ID Server (caso CIE). Il sistema recupera le informazioni anagrafiche inserite nel certificato digitale e le associa a quelle relative al certificato di sottoscrizione in oggetto di richiesta.

Nel caso e, il Richiedente, utilizzando le credenziali SPID di livello 2 o superiore, è chiamato ad effettuare un'autenticazione su di un portale del Certificatore o di una sua LRA attraverso meccanismi del circuito SPID.
L'accesso alla funzionalità di richiesta del certificato avviene mediante autenticazione di livello 2 o superiore previa l'utilizzo di credenziali SPID rilasciate dal Gestore dell'Identità.
Qualora l'identità digitale utilizzata sia stata emessa da un Gestore dell'identità diverso da Namirial, la richiesta e rilascio del certificato avvengono in conformità Avviso n. 17 di AgID del 24 gennaio 2019 recante *"Utilizzo identità digitali SPID*

al fine di rilasciare certificati qualificati". In particolare, il certificato conterrà l'OID 1.3.76.16.5, registrato dall'Agenzia, con la seguente descrizione: "Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity".

I dati di registrazione sono conservati, in questi casi, esclusivamente in formato elettronico.

5.1.4 Identificazione attraverso il riconoscimento già effettuato da un intermediario finanziario o altro soggetto esercente l'attività finanziaria

In tale modalità il Certificatore si avvale del riconoscimento già effettuato da un intermediario finanziario o altro soggetto esercente attività finanziaria, che, ai sensi della normativa antiriciclaggio tempo per tempo vigente, è obbligato all'identificazione dei propri clienti.
I dati utilizzati per il riconoscimento del Richiedente, sono rilasciati dal soggetto finanziario ai sensi delle specifiche normative nazionali che recepiscono le direttive [23], [24] e [25].

5.1.5 Identificazione da parte di un pubblico ufficiale

Il Richiedente 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:

- il modulo di richiesta di emissione certificato;
- la dichiarazione sostitutiva dell'atto di notorietà (in originale).

5.2 Registrazione del Richiedente e rilascio del certificato

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 5.1.1, 5.1.2 e 5.1.3;
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".

5.3 Dispositivi OTP supportati

Sono supportate le seguenti tipologie di dispositivi OTP:

- Token fisico;
- Token virtuale o mobile;
- SMS;
- Sistemi biometrici d'autenticazione o altri sistemi d'autenticazione presso terzi.

5.4 Modalità di consegna e abilitazione dei dispositivi OTP

I dispositivi OTP di tipo fisico vengono assegnati e consegnati al Titolare dall'operatore della LRA, 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. Il tipo e numero seriale del dispositivo OTP di tipo fisico sono registrati dall'operatore ed associati al Titolare.
I dispositivi fisici vengono rilasciati non attivi e, prima del loro utilizzo, il Titolare dovrà necessariamente effettuare la procedura di abilitazione, accedendo all'apposita area e seguendo le istruzioni mostrate a video. La procedura provvederà ad eseguire un allineamento della sequenza di codici attesa.
Per i dispositivi OTP di tipo virtuale (mobile) le procedura d'attivazione sono documentate all'interno dell'email che il Titolare riceve a seguito della registrazione.
L'utilizzo di OTP mediante SMS rende obbligatorio al Titolare di comunicare un suo numero di telefono cellulare. Il sistema provvede a verificare che detto numero non sia già utilizzato da altri soggetti.

5.5 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 5.3;
- 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 (si veda par. 5.6) comunicando l'esito dell'operazione all'utente con un messaggio di avvenuta attivazione.

5.6 Modalità di generazione delle chiavi, di emissione dei certificati e di utilizzo delle chiavi di sottoscrizione

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 di un HSM dotato di certificazione OCSI o equipollente.

5.6.1 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);
- sia le chiavi di certificazione che quelle di sottoscrizione hanno lunghezza pari a 2048 bit. Future chiavi di certificazione potranno usare avere lunghezza superiore.

5.6.2 Modalità di generazione e protezione delle chiavi di sottoscrizione

Completata la fase di registrazione, durante la quale i dati dei Titolari vengono memorizzati negli archivi del Certificatore (o LRA), è possibile procedere alla generazione delle chiavi di sottoscrizione che vengono generate dal Certificatore. 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.

5.6.3 Sostituzione delle chiavi di certificazione

La sostituzione delle chiavi di certificazione 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 almeno ogni 13 anni per garantire la fruibilità di tutti i certificati emessi fino alla naturale scadenza degli stessi.

5.6.4 Funzioni di HASH

Per la generazione delle impronte 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. Per il futuro il Certificatore si riserva la possibilità di utilizzare anche le funzioni hash SHA-348 e SHA-512.

5.7 Revoca e sospensione del certificato qualificato

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 salvo che lo stato di sospensione non sia stato annullato come previsto dall'art.24 comma 4bis del CAD. Nel caso in cui si proceda alla revoca di un certificato in stato di sospensione, la revoca decorre dalla data di inizio della sospensione.

5.7.1 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.

5.7.2 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[2] al servizio di Help Desk (§ 2.3);

[1] La data di fine non deve essere successiva alla data di scadenza del certificato.
[2] Al cliente verranno richiesti alcuni dati personali per assicurare la liceità della richiesta.

- via Web[3] 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 Strumenti e modalità per l'apposizione della firma

Per l'apposizione della firma in modalità remota, sarà possibile utilizzare applicazioni di tipo on-line e funzionanti mediante i servizi erogati dal Certificatore o dalla LRA. In quest'ultimo caso il Certificatore provvede ad assicurarsi che il sistema gestito dalla LRA garantisca la conoscenza esclusiva del dato per la creazione della firma da parte del Titolare grazie ad opportuni requisiti di sicurezza.
Il Certificatore mette a disposizione web services per permettere l'integrazione con le applicazioni richiedenti i servizi di firma. Si intende che i documenti oggetto di firma siano normalmente formati da dette applicazioni in dipendenza dalle specifiche necessità. Per poter firmare un documento è necessario che la SCA sia collegata al sistema di firma remota attraverso un canale di comunicazione sicuro (es TLS). Attraverso tale canale viene veicolata l'impronta del documento alla firma unitamente alle credenziali che consentono l'utilizzo delle chiavi di sottoscrizione.
Oltre all'identificativo univoco delle chiavi di sottoscrizione, dette credenziali utilizzano un doppio fattore d'autenticazione composto dalla coppia SYK+SYH oppure dalla coppia SYK+SYA. In quest'ultimo caso la componente SYA è validata da un Sistema Biometrico di Autenticazione (SBA).
Laddove sussistano particolari condizioni d'utilizzo, previa approvazione da parte dell'Agenzia per l'Italia digitale (AgID) ai sensi dell'art.35 comma 5 del CAD, potranno essere adottate soluzioni d'autenticazione che utilizzano un solo fattore.
Nel caso ci si avvalga di un SBA, al momento della registrazione, fermo restando il rispetto delle norme volte a garantire la tutela dei propri dati personali in piena aderenza al REGOLAMENTO (UE) 2016/679 (GDPR) , viene associato al Titolare un insieme di diverse caratteristiche fisiologiche e/o comportamentali unicamente riconducibili al titolare stesso, quali ad esempio: le caratteristiche delle firma autografa, la forma dell'orecchio, la fisionomia del volto, le impronte digitali, il colore e la dimensione dell'iride, la sagoma della mano, il palmo della mano, la vascolarizzazione, l'impronta vocale, lo stile di battitura sulla tastiera o i movimenti del corpo.
Nella fase di autenticazione verrà verificata la corrispondenza con i parametri rilevati durante la fase di registrazione per poter procedere nell'operazione di firma.

5.8.1 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. La richiesta di firma proveniente dall'utente è 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

In alternativa, nel caso di applicazioni di Firma destinate ad un gruppo chiuso di utenti, è possibile autenticare la richiesta di firma attraverso un Sistema Biometrico di Autenticazione (SBA)[4].
A titolo esemplificativo, ma non esaustivo, il certificatore detiene, attraverso la controllata Namirial Gmbh (conosciuta precedentemente come XYZmo Gmbh) un SBA che si avvale delle caratteristiche della firma autografa.
Questo tipo di procedura è utilizzabile in contesti presidiati, cioè dove si hanno ragionevoli garanzie che terzi non possano recuperare e/o riutilizzare informazioni biometriche del titolare[5].
Nella realizzazione di progetti in cui vengano utilizzati SBA, potrà essere necessario, qualora i dati biometrici vengano storicizzati, richiedere la preventiva approvazione dell'organismo preposto alla protezione dei dati personali.
Modalità alternative di autenticazione forte possono essere implementate, a fronte di situazioni specifiche che lo giustifichino e sempre con l'esplicita approvazione preventiva da parte dell'Organismo di Vigilanza sui Certificatori.

[3] Il sito web è accessibile in modalità 24h x 7gg.
[4, 5] Previa approvazione da parte dell'Agenzia per l'Italia digitale (AgID) ai sensi dell'art.35 comma 5 del CAD ai fini della valutazione di conformità del sistema e degli strumenti di autenticazione nella generazione della firma elettronica.

Le applicazioni di Firma Remota fornite dal Certificatore sono descritte nei paragrafi seguenti.

5.8.1.1 FirmaCerta

E' 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 nel documento "Software FirmaCerta - Guida rapida all'utilizzo", disponibile al seguente URL:

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

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

5.8.1.2 FirmaCertaMobile

E' un'applicazione mobile, sviluppata dal Certificatore, installabile su dispositivi dotati di sistema operativo Android e IOS.

5.8.1.3 FirmaCertaWeb

E' 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[6]
- PIN[7]
- OTP

5.8.1.4 eSignAnyWhere

E' un'applicazione web fruibile sia in modalità cloud che on-premises sviluppata dalla società Rumena Namirial Srl, posseduta al 100% da Namirial SpA. La versione cloud è disponibile su alla URL www.significant.com
L'apposizione della firma richiederà che l'utente inserisca i seguenti codici:

- Codice Dispositivo Virtuale o Nome Utente area riservata Namirial SpA[8]
- PIN
- OTP

Per questioni di usabilità, nei soli casi delle applicazioni *FirmaCerta*, *FirmaCertaMobile* e *eSIgnAnyWhere*, il Titolare potrà memorizzare al loro interno il *Codice Dispositivo Virtuale* o il Nome Utente 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 adotta dei sistemi che non gli consentono 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 5.7.1.
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.

[6] Tale informazione è presente all'interno del modulo sottoscritto dal Titolare.
[7] Può essere impostato dal Titolare in fase di generazione delle chiavi.
[8] Tale informazioni sono presenti all'interno del modulo sottoscritto dal Titolare e possono essere pre-impostati dall'utente o dall'applicazione che forma il documento da sottoscrivere.