Addendum Manuale Operativo

Certificati di Firma Disposable

Certificatore	**Namirial S.p.A.**	Modello Doc.	**NAM-FDMT-MO-ADD-DISP**
Redatto da	**Andrea Pace**	Nota di riservatezza	**DOCUMENTO PUBBLICO**
Revisionato da	**Giuseppe Benedetti**	Versione	**1.2**
Approvato da	**Davide Ceccucci**	Data	**28/06/2018**

Namirial S.p.A.
Il legale rappresentante
(Dott. Davide Ceccucci)

CECCUCCI DAVIDE
2018.07.02 09:07:01
CN=CECCUCCI DAVIDE
C=IT
O=NAMIRIAL S.p.A.
2.5.4.97=VATIT-02046570
RSA/2048 bits

Indice

Indice delle tabelle

Storia delle modifiche

Versione	**1.0**
Data	03/05/2016
Motivazione	Prima emissione.
Modifiche	Manuale Operativo per richiesta, emissione e uso della Firma Digitale con certificati denominati “Disposable”.

Versione	**1.1**
Data	21/01/2018
Motivazione	Seconda emissione.
Modifiche	Aggiunta nuova limitazione d’uso.

Versione	**1.2**
Data	28/06/2018
Motivazione	Terza emissione.
Modifiche	Aggiunta nuova limitazione d’uso.

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 qualificati denominati "Disposable", vale a dire "usa e getta". La caratteristica di detti certificati qualificati è quella di avere una breve durata di validità, non superiore a 60 (sessanta) minuti dal momento dell'emissione.

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]	D. Lgs. 196/2003	Decreto Legislativo 30 giugno 2003, n. 196 *Codice in materia di protezione dei dati personali.*
[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 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.
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.
Disposable	Certificato di Firma Qualificata con intervallo di validità breve (eg. 60 minuti)
Dispositivo Sicuro per la Creazione della Firma	Dispositivo hardware capace di proteggere efficacemente la segretezza della chiave privata.
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.

Termine o acronimo	Significato
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.
RA	Registration Authority, soggetto che esegue l'identificazione dei Richiedenti dei certificati qualificati applicando le procedure definite dal Certificatore.
RAO	È soggetto espressamente delegato dal Certificatore allo svolgimento, per conto di quest'ultimo, 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.
SBA – Sistema Biometrico di Autenticazione	Correlazione tra persona fisica e le sue caratteristiche fisiologiche e/o comportamentali
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.
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 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 27001:2005. Namirial ha conseguito il certificato n. IND12.2513U 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 ottenuto la certificazione UNI EN ISO 9001:2000 in data 28.11.2007. Namirial ha conseguito il certificato n. 223776 presso la Bureau Veritas Italia S.p.A. che l'ha giudicata conforme ai requisiti della norma ISO 9001:2000 con il seguente scopo:
"progettazione, elaborazione ed assistenza post vendita di software, piattaforme gestionali e siti internet. L'erogazione di servizi hosting e collocation per centri assistenza amministrativa e fiscale. L'erogazione del servizio di posta elettronica certificata. Settore/i EA di attività: 33".

2.2.2 Certificazione ISO/IEC 27001:2005

Namirial S.p.A. ha ottenuto la certificazione UNI EN ISO 27001:2005 in data 19.03.2012. Namirial ha conseguito il certificato n. IND12.2513U presso la Bureau Veritas Italia S.p.A. che l'ha giudicata conforme ai requisiti della norma ISO/IEC 27001:2005 con il seguente scopo:
"realizzazione di soluzioni di firma elettronica avanzata rivolte alle pubbliche amministrazioni ed enti privati mediante utilizzo di software di acquisizione biometrica e sistemi di cifratura a norma di legge".

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 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-DISP**" 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'Operatore della Registration Authority (RAO)
- 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.

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):

1.3.6.1.4.1.36203.1.1.6	Policy per certificati qualificati associati ad apparato sicuro per la creazione della firma mediante procedura remota di tipo Disposable.

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 almeno uno dei 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).*
- Valido solo per la sottoscrizione di polizze assicurative, escluse polizze vita caso morte/The certificate may be used only to sign insurance contract, excluded the ones for whole life insurance
- Valido solo per la sottoscrizione di contratti di telefonia mobile/ The certificate may be used only to sign mobile phone contracts

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 Disposable

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 all'indirizzo: http://crl.firmacerta.it/FirmaCertaQualificata1.crl.
All'emissione delle liste di revoca il certificatore garantisce che sia pubblicato l'insieme di tutte le CRL necessarie a coprire tutti i certificati emessi nel loro complesso fino a quel momento dal certificatore.
Certificati e CRL partizionate sono emessi nel rispetto della specifica tecnica 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 3 rilasciate da Namirial;
- attraverso il riconoscimento già effettuato da un intermediario finanziario o altro soggetto esercente l'attività finanziaria;
- attraverso le credenziali rilasciate per l'emissione di un precedente certificato Disposable.

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 D.lgs. 196/2003, 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 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, 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 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 3

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 SPID di livello 3

Questa modalità prevede che il richiedente sia in possesso di credenziali SPID di livello 3 e si colleghi su di un portale del Certificatore o di una sua LRA, che funge da Service Provider SPID. L'accesso alla funzionalità di richiesta del certificato, o all'area riservata che ne permette la fruizione avviene mediante autenticazione di livello 3 previa l'utilizzo di credenziali SPID rilasciate dal Certificatore.
In questo modo il portale di registrazione ottiene le informazioni necessarie sotto forma di messaggi SAML provenienti dall'Identity Provider SPID che ha rilasciato le credenziali usate per l'autenticazione.

5.1.3.3 Autenticazione mediante CNS o CIE

Questa modalità prevede che il richiedente sia in possesso e possa utilizzare una tra le seguenti carte:

- CNS;
- CRS;
- CIE o documento equivalente nel paese di provenienza del richiedente.

Previa inserimento del PIN della carta, il Richiedente effettua l'autenticazione sul portale del Certificatore. Il sistema recupera le informazioni anagrafiche inserite nel certificato digitale e le associa a quelle relative al certificato di sottoscrizione in oggetto di richiesta.

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 tramite le credenziali rilasciate per l'emissione di un precedente certificato Disposable

In questa modalità il Certificatore si basa sull'identificazione già effettuata durante l'emissione di un precedente certificato Disposable. Il Richiedente già in possesso di credenziali, si autentica al portale del Certificatore o della LRA e chiede l'emissione di un nuovo certificato Disposable, previa la conferma o l'aggiornamento dei dati di registrazione. Per il rilascio del certificato è necessario che il Titolare inserisca una One-Time-Password inviata al suo dispositivo OTP e che sia data l'autorizzazione a procedere dalla LRA o dal Terzo Interessato.

5.1.6 Registrazione del Richiedente e rilascio del certificato

I certificati Disposable vengono rilasciati per essere utilizzati contestualmente da applicazioni di firma remota.
Il rilascio di Certificati Disposable a persone fisiche avviene previa l'identificazione del Richiedente da parte di uno dei soggetti elencati al paragrafo 5.1. Le procedure per la registrazione del Richiedente e il rilascio del certificato prevedono:

a) che il Richiedente venga identificato con certezza con una delle modalità descritte ai precedenti paragrafi.
b) che il Richiedente abbia 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 abbia comunicato il proprio numero di cellulare da utilizzare per l'inoltro di OTP via SMS.
e) che il Richiedente abbia preso visione delle Condizioni Generali di contratto e del presente Addendum del Manuale Operativo;
f) che il Richiedente abbia manifestato la volontà di ottenere il rilascio di un certificato Disposable previa conferma ed accettazione della richiesta di registrazione, attestata da opportune evidenze informatiche che ne comprovino la veridicità e disponibili presso il Certificatore o la LRA.

Il Certificatore o la LRA, terminata la fase di identificazione, effettua l'operazione di registrazione del Richiedente attraverso il portale web del servizio di certificazione digitale, ovvero attraverso i previsti web-service. Il Certificatore provvede successivamente al rilascio del certificato qualificato di tipo Disposable.
Il Certificatore si riserva di effettuare delle verifiche sull'autenticità della documentazione fornita.
Il Richiedente con il rilascio del certificato assume la qualifica di Titolare.

5.2 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.

5.2.1 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);
- le chiavi usate dal Certificatore per firmari certificati hanno lunghezza pari a 2048 bit;

5.2.2 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.

5.2.3 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.

5.2.4 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.

5.2.5 Emissione di certificati Disposable

L'emissione dei certificati per applicazioni di firma qualificata remota di tipo Disposable (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. I certificati di firma Disposable vengono emessi in stato attivo.

5.3 Revoca e sospensione del certificato qualificato

Nonostante l'esiguo periodo di validità del certificato Disposable, ove applicabili restano valide le procedure già descritte nel Manuale Operativo del Certificatore.

5.3.1 Modalità per la sospensione del certificato Disposable

La sospensione di un certificato può essere effettuata direttamente dal Titolare mediante le apposite funzionalità accessibili on-line nel portale del Certificatore.
La funzionalità di sospensione, funzionante con i medesimi meccanismi, potrà essere resa disponibile al Titolare anche su portali di terzi, quali quelli della LRA o del Terzo Interessato.

5.4 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.
La richiesta di firma proveniente dall'utente, vista la breve durata dei certificati Disposable, può essere autenticata sia attraverso la componente delle credenziali nota al Titolare (OTP), sia attraverso un Sistema Biometrico di Autenticazione (SBA)
Nel caso ci si avvalga di un SBA, al momento della registrazione, viene associato al Titolare un insieme di una o più 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.