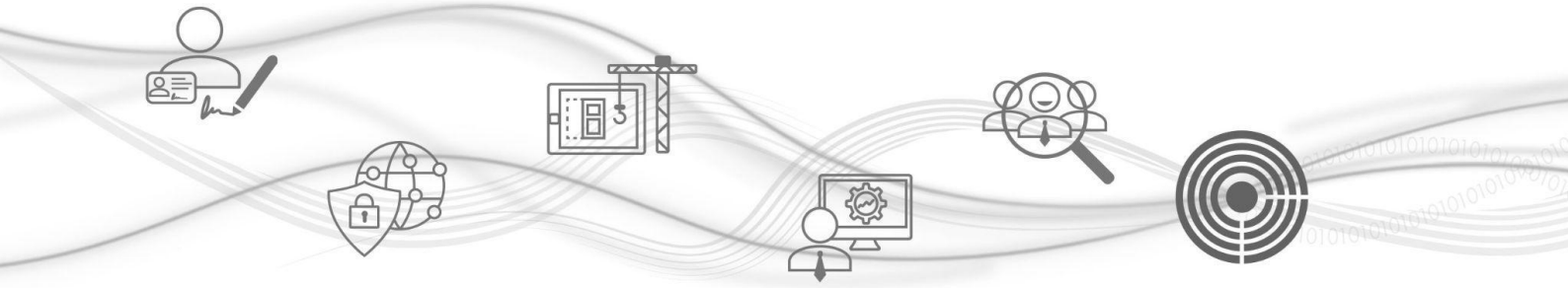
Manuale Operativo
Certificate Policy & Certificate Practice Statement
Certificati non qualificati (NQ)



Categoria	**Manuale Operativo**	Codice Documento	**NAM-MO-NQ**	**Namirial S.p.A.**
Redatto da	**Federica Gioè**	Nota di riservatezza	**Documento Pubblico**	**Il Legale Rappresentante**
Verificato da	**Luigi Enrico Tomasini**	Versione	**1**	**Massiiliano Pellegrini**
Approvato da	**Massimiliano Pellegrini**	Data di emissione	**06/05/2026**	—

Signed by: PELLEGRINI MASSIMILIANO
Issued by: Namirial CA Firma Qualificata
Signing time: 18-05-2026 16:13:59
IP address: 37.159.109.49

Namirial S.p.A.
Via Caduti sul Lavoro n. 4, 60019 Senigallia (An) - Italia | Tel. +39 071 63494
www.namirial.com | amm.namirial@sicurezzapostale.it | P.IVA IT02046570426
C.F. e iscriz. al Reg. Impr. Ancona N. 02046570426 | REA N. AN - 157295
Codice destinatario T04ZHR3 | Capitale sociale € 8.256.361,60 i.v.

Indice

Storia delle modifiche

VERSIONE	1.0
Data	06/05/2026
Motivazione	Primo rilascio
Modifiche	-

Riferimenti tecnici e normativi

Il Certificatore, nell'erogazione dei suoi servizi, è conforme alle normative e regolamenti europei e nazionali applicabili al momento dell'emissione. Tutti i regolamenti e le leggi applicabili sono riportati nella seguente tabella ed al personale del Certificatore.

NORMATIVA	DESCRIZIONE
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.
D.Lgs. 82/2005	Decreto Legislativo 7 marzo 2005, n. 82 Codice dell'Amministrazione Digitale (CAD), con le modifiche ed integrazioni stabilite dal decreto legislativo 26 agosto 2016, n. 179.
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.
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)
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
Direttiva UE 2015/2366	Direttiva (UE) 2015/2366 del Parlamento Europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE
RFC 3647	Certificate Policy and Certification Practices Framework
RFC 5280	Internet X.509 Public Key Infrastructure - Certificate and CRL Profile
ITU-T X.509 ISO/IEC 9594-8	Information Technology – Open Systems Interconnection – The Directory: Authentication Framework
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.
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 nonchè della direttiva 2006/70/CE che ne reca misure di esecuzione".
RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.
RFC 3161	Internet X.509 Public key infrastructure Time Stamp Protocol (TSP) PKIW Working Group IETF - Agosto 2001.

NORMATIVA	DESCRIZIONE
ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI EN 319 411-2	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
ETSI EN 319 411-3	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates
ETSI EN 319 412-1	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
ETSI EN 319 412-2	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
ETSI EN 319 412-3	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
ETSI EN 319 412-4	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates
ETSI EN 319 412-5	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
Regolamento (UE) 2014/910 (eIDAS)	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
QSCD	COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
TSL	COMMISSION IMPLEMENTING DECISION (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and

NORMATIVA	DESCRIZIONE
	of the Council on electronic identification and trust services for electronic transactions in the internal market
Electronic Signature Formats	COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
Regolamento (UE) 2024/1183 (eIDAS2)	amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

Tabella 1: Riferimenti tecnici e normativi

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.
Certificato digitale	documento elettronico attestante il legame tra dati di convalida della firma (chiave pubblica) e una persona fisica.
Certificato disposable o Disposable	Certificato non qualificato di firma elettronica di tipo disposable con intervallo di validità breve (eg. 30 giorni) e intervallo di utilizzo di 60 minuti
Certificatore [Certification Authority]	È l'ente, pubblico o privato, abilitato a rilasciare Certificati digitali tramite procedura di certificazione che segue standard internazionali e conforme alla normativa italiana ed europea in materia.
Chiave privata	È la chiave crittografica utilizzata in un sistema di crittografia asimmetrica; ogni chiave privata è associata ad una chiave pubblica, ed è solo in possesso dal Titolare che la utilizza per firmare digitalmente i documenti.
Chiave pubblica	È la chiave crittografica utilizzata in un sistema di crittografia asimmetrica; ogni chiave pubblica è associata ad una chiave privata, ed è utilizzata per verificare la firma digitale apposta su un documento informatico dal Titolare della chiave asimmetrica.
CIE	Carta d'Identità Elettronica, è il documento di identificazione destinato a sostituire la carta d'identità cartacea sul territorio italiano.
Cliente	È il soggetto, persona giuridica, che tramite accordi con Namirial sceglie di utilizzare i Certificati.
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione, l'Organismo di controllo istituito dal Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri.
CRL – Lista di revoca e sospensione dei Certificati	È una lista di Certificati che sono stati resi "non validi" dal Certificatore prima della loro naturale scadenza. La revoca rende i Certificati "non validi" definitivamente. La sospensione rende i Certificati "non validi" per un tempo determinato.
CUC	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 – Utente Finale	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.

TERMINE O ACRONIMO	SIGNIFICATO
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; modificato dal Regolamento (UE) N. 1183/2024
Giornale di controllo	Consiste nell'insieme delle registrazioni, effettuate automaticamente o manualmente, degli eventi previsti dalle Regole Tecniche di base.
IUT	Identificativo Univoco del Titolare, diverso per ogni Certificato emesso.
LDAP [Lightweight Directory Access Protocol]	È un protocollo standard per l'interrogazione e la modifica dei servizi di directory (segue gli standard X.500).
LRA	È il soggetto, che coincide con il Cliente, registrato all'interno del sistema del Certificatore che utilizza la soluzione di firma elettronica avanzata.
Manuale Operativo	È il documento che definisce le procedure applicate da Namirial 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.
Operatore	È soggetto delegato dal Cliente all'identificazione e registrazione del Titolare.
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 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
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.
RSA	Algoritmo di crittografia asimmetrica, basato su chiavi pubbliche e private.
SHA-256 [Secure Hash Algorithm]	Algoritmo di crittografia che genera una impronta digitale di 256 bit.

TERMINE O ACRONIMO	SIGNIFICATO
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.
Titolare	È il Firmatario, ovvero una persona fisica che crea una Firma elettronica, cui è intestato il Certificato.
X.509	È uno standard ITU-T per le infrastrutture a chiave pubblica (PKI)

Tabella 2: Definizioni e Acronimi

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.

Namirial S.p.A. è:

Autorità di Certificazione Qualificata e accreditata dal 25/07/2016 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.

Soggetto Conservatore, in conformità a:

- Regole Tecniche ai sensi dell'art. 71 del Codice dell'Amministrazione Digitale;
- Regolamento (UE) 910/2014 eIDAS, art. 24;

per la prestazione di servizi fiduciari di Conservazione a Norma.

Certificata ISO 9001. Namirial ha conseguito il Certificato n. IT347262 rilasciato da **Bureau Veritas Italia S.p.A.**

Certificata ISO/IEC 27001. Namirial ha conseguito il Certificato n. IT327282 rilasciato da **Bureau Veritas Italia S.p.A.**

Dal 2023 Namirial ha deciso di ampliare la propria infrastruttura PKI implementando una seconda Certification Authority root. Questa CA, che si affianca senza sostituirsi a quella esistente è stata implementata nella server farm di **Uanataca**, già Certification Authority qualificata ai sensi del regolamento eIDAS nonché azienda del gruppo **Bit4id**, parte del gruppo Namirial.

Namirial può inoltre vantare le acquisizioni strategiche di **Netheos**, azienda leader nel mercato francese specializzato in soluzioni per l'identificazione e l'onboarding digitale e di **Evicertia**, QTSP spagnolo affermato nella penisola iberica e in America Latina.
Entrambe le acquisizioni rafforzano il portafoglio di Namirial, così come la sua presenza sul mercato internazionale, determinando inoltre un ampliamento ed un improvement delle competenze dell'Azienda.

Contatti di Servizio e HelpDesk

Per ricevere informazioni sui servizi di Certificazione di Namirial S.p.A. sono disponibili i seguenti recapiti:

telefono: (+39) 071 63494
e-Mail: commercialeca@namirial.com
web: https://www.namirial.com/it/servizi-fiduciari/

Per ricevere informazioni tecniche ed assistenza sul servizio è possibile inoltrare una richiesta tramite apposita form disponibile al sito web: https://servicedesk.namirial.com/

1. Introduzione

1.1. Scopo e campo di applicazione

Il presente documento rappresenta il **Manuale Operativo** nonché la **Certificate Policy e Certification Practice Statement** della Certification Authority Namirial S.p.A per il rilascio di **certificati non qualificati di firma elettronica di tipo *disposable*** ed ha come scopo la descrizione delle regole e delle procedure operative adottate da Namirial per tutte le attività inerenti all'emissione e alla gestione dei Certificati stessi.

1.2. Nome e identificativo del documento

Il presente documento con codice "NAM-MO-NQ" è identificato attraverso il livello di revisione e la data di rilascio presente su tutte le pagine. Nel preambolo del documento è inoltre riportato un paragrafo con la storia delle modifiche apportate.
Il presente documento è consultabile, per via telematica, al seguente indirizzo https://www.namirial.com/it/documentazione/

Il documento è pubblicato in formato PDF firmato, in modo tale da assicurarne l'origine e l'integrità.
La responsabilità del presente Manuale Operativo è di Namirial, la quale ne cura la stesura, la pubblicazione e l'aggiornamento.
Le comunicazioni riguardanti il presente documento possono essere inviate all'attenzione del Certificatore ai recapiti indicati al §1.3.1

Namirial S.p.A. garantisce la compliance dei propri Certificati con la Root ASN.1 OID indicata di seguito nel documento.

L'Object Identifier (OID) che identifica Namirial S.p.A. è iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1): 36023:

OID: 1.3.6.1.4.1.36203

Tale OID è inserito nell'estensione CertificatePolicy dei Certificati, secondo le policies descritte nell'apposito paragrafo.

1.3. Partecipanti e responsabilità

Per la realizzazione ed erogazione dei certificati non qualificati, gli attori indicati nel presente documento sono:

a) **Namirial S.p.A.:** è il Certificatore (**CA**).
b) **Cliente:** è il soggetto utilizza i Certificati all'interno delle proprie procedure. Il Cliente può rivestire anche il ruolo di Local Registration Authority.

c) **Operatore della Registration Authority (RAO):** è il soggetto di cui si avvale il Cliente nei casi in cui sia prevista la verifica dell'identità al fine di rilasciare un certificato di firma nominativo.
d) **Utente:** è il soggetto che utilizza il Certificato reso disponibile dal Cliente.
e) **Destinatario** (**Relying party**): è l'eventuale soggetto interessato al contenuto del documento o ai documenti oggetto di sottoscrizione.

1.3.1. Namirial S.p.A.

Namirial S.p.A. è il Certificatore (CA).
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
Sede di erogazione del servizio:	VIA CADUTI SUL LAVORO, 4 60019 - SENIGALLIA (AN) TEL: 071.63494
Partita IVA:	IT02046570426
Iscrizione registro delle imprese:	Ancona
REA:	02046570426
Capitale sociale:	€ 8.256.361,60 i.v.
Servizio Assistenza:	https://servicedesk.namirial.com/hc/it
Sito web del Certificatore:	http://www.namirial.com
Indirizzo PEC del servizio:	firmacerta@sicurezzapostale.it

Tabella 3: Dati identificativi del Certificatore

1.3.1.1. Organizzazione del personale

Nell'ambito dei Certificati non qualificati rilasciati dalla Certification Authority Namirial S.p.A., anche se non rientrando nel perimetro qualificato, il personale preposto all'erogazione e controllo del servizio di certificazione è organizzato nel rispetto dell'art. 38 DPCM 22 febbraio 2013. In particolare, sono definite le seguenti figure organizzative:

- Responsabile della sicurezza
- Responsabile del servizio di certificazione e validazione temporale
- Responsabile della conduzione tecnica dei sistemi
- Responsabile dei servizi tecnici e logistici

- Responsabile delle verifiche e delle ispezioni (auditing)
- Responsabile della registrazione dei Titolari (RA) e dell'Help Desk;

Le responsabilità sopra descritte rientrano inoltre nei trusted roles previsti dallo standard ETSI EN 319-401, come descritto nell'apposito paragrafo.
Le figure sopra elencate possono avvalersi, per lo svolgimento delle attività di loro competenza, di addetti e collaboratori esterni.

Namirial S.p.A:

- si attiene alla normativa vigente in materia di Firma elettronica e successive modificazioni ed al regolamento eIDAS n. 910/2014 e sue successive modificazioni;
- rilascia il Certificato non qualificato esclusivamente nei casi consentiti dal Titolare del Certificato nei modi o nei casi stabiliti nell'art. 32, comma 3, lettera b) del Dlgs 82/2005 (Codice dell'Amministrazione Digitale), nel rispetto del Regolamento UE 206/679 (GDPR), e successive modificazioni;
- non copia, né duplica, le chiavi private di firma del soggetto cui il Certificatore ha fornito il servizio;
- assicura la precisa determinazione della data e dell'ora di rilascio, scadenza, revoca e sospensione dei Certificati non qualificati;
- registra sul giornale di controllo, l'emissione dei Certificati non qualificati, con la specificazione della data e dell'ora di generazione; il momento di generazione del Certificato è attestato tramite riferimento temporale;
- tiene registrazione, anche elettronica, di tutte le informazioni relative al Certificato dal momento della sua emissione almeno per 20 (venti) anni, anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
- rende accessibile, per via telematica, la copia delle liste, sottoscritte da AgID, dei Certificati relativi alle chiavi di Certificazione di cui al DPCM 22 febbraio 2013
- utilizza sistemi affidabili per la gestione del registro dei Certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i Certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal Titolare;
- adotta le misure di sicurezza per il trattamento dei dati personali, ai sensi del Regolamento UE 206/679 (GDPR).

1.3.2. Cliente

Il Cliente è il soggetto che utilizza la soluzione di firma non qualificata al fine di utilizzarla nei rapporti intrattenuti con soggetti terzi per motivi istituzionali, societari o commerciali.
Il Cliente ha l'obbligo di:

a) identificare in modo certo l'utente tramite un valido documento di riconoscimento, informarlo in merito agli esatti termini e condizioni relative all'uso del servizio, compresa ogni eventuale limitazione dell'uso, subordinare l'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente;

b) fornire liberamente e gratuitamente copia della dichiarazione e le informazioni necessarie al fine di utilizzo del certificato al firmatario, su richiesta di questo;
c) specificare le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto;

1.3.3. Operatore di registrazione (RAO)

Il Cliente può incaricare un soggetto, persona fisica, per l'adempimento degli obblighi di cui alla lettera a), affidandogli la verifica dell'identità necessaria al rilascio del certificato di firma non qualificato nominativo, questo soggetto viene identificato come Operatore di registrazione (RAO).

1.3.4. Utente

L'utente è il soggetto che utilizza il Certificato di firma non qualificato fornito dal Cliente. Viene identificato anche come Titolare, in quanto persona fisica identificata all'interno del Certificato come il possessore della chiave privata associata alla chiave pubblica consegnata all'interno del Certificato.

Il Titolare del Certificato non qualificato è tenuto a:

- prendere visione del presente documento prima di richiedere il Certificato e rispettarne le prescrizioni per quanto di propria competenza;
- fornire tutte le informazioni richieste dal Cliente, garantendone l'attendibilità sotto la propria responsabilità;
- ove previsto, mantenere in modo esclusivo la conoscenza o la disponibilità dei dati per la creazione della firma (PIN e/o OTP) e il codice d'emergenza, conservandoli con la massima diligenza;
- mantenere in modo esclusivo e conservare con la massima diligenza il dispositivo OTP eventualmente fornito;
- non utilizzare la Firma per funzioni e finalità diverse da quelle per la quale è stata rilasciata;

1.3.5. Destinatario

Il Destinatario è una persona fisica o giuridica interessata al contenuto del documento o ai documenti oggetto di sottoscrizione, il cui Certificato di firma apposto è verificabile tramite il riferimento di una chiave pubblica inserita all'interno del Certificato del Titolare.
I Destinatari, al fine di verificare la validità di un Certificato, debbono sempre riferirsi alle informazioni di revoca della CA Namirial (CRL e OCSP).
Il Destinatario può inoltre verificare che il documento informatico sottoscritto con firma elettronica avanzata non abbia subito modifiche dopo l'apposizione della firma.

2. Amministrazione del Manuale Operativo

Il presente documento è definito, pubblicato ed aggiornato da Namirial S.p.A. Ogni modifica di questo documento è sottoposta ad un processo di verifica interno e approvata dall'alta direzione.
Namirial S.p.A. aggiorna periodicamente la propria documentazione pubblica disponibile al sito internet dell'organizzazione.

2.1. Pubblicazione e archiviazione

Il repository è disponibile all'indirizzo:

https://www.namirial.com/it/documentazione/

Namirial gestisce il repository in maniera indipendente e ne è direttamente responsabile.

3. Identificazione ed Autenticazione (I&A)

3.1. Naming

Namirial emette ogni Certificato in compliance con i seguenti Standard:
• ETSI EN 319 411-1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
• ETSI EN 319 411-2 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
• ETSI EN 319 412-1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
• ETSI EN 319 412-2 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

Il campo "subject" nel Certificato contiene informazioni intellegibili che permettono l'identificazione del proprietario del Certificato.
Il campo "soggetto" contiene, almeno:

- countryName;
- givenName and surname
- commonName
- DNQualifier
- SerialNumber

3.2. Significato dei nomi

L'attributo del Certificato Distinguished Name (DN) identifica in maniera univoca il soggetto a cui è rilasciato il Certificato.

3.2.1. Regole di interpretazione dei tipi di nomi

Namirial si attiene allo standard X500.

3.2.2. Univocità dei nomi

Nel Certificato vengono indicati nome, cognome ed un codice identificativo a garanzia dell'univocità del Soggetto. Per i cittadini italiani, il codice univoco del soggetto è rappresentato dal codice fiscale, mentre per i cittadini esteri può essere definito un codice univoco tratto dal documento di riconoscimento presentato durante la fase di identificazione.
Pertanto, in assenza di codice fiscale o attributo equivalente, in caso di Certificato il cui Richiedente sia estero, all'interno del Certificato potrà essere indicato:

- un codice identificativo tratto da un documento di identità valido, utilizzato nella procedura di riconoscimento;
- un identificativo univoco determinato dalla CA e codificato in base 64.

3.2.3. Anonimato e Pseudonimia dei Richiedenti

Non è previsto l'anonimato per questa tipologia di certificati.
Nel caso in cui sia richiesto dal Cliente di inserire nel certificato uno pseudonimo in luogo dei dati reali del Richiedente, Namirial si riserva di valutare caso per caso l'ammissibilità della richiesta, sulla base delle evidenze prodotte e sulla riconducibilità al soggetto.
Il Cliente conserverà, in ogni caso e senza alcuna deroga, le informazioni relative alla reale identità della persona.

3.3. Convalida iniziale dell'identità

Il processo di validazione dell'identità comporta la verifica da parte del Cliente dell'identità del Richiedente.
Le procedure per rilasciare un Certificato non qualificato sono:

- Registrazione
- Identificazione

Il processo può essere condotto dagli Operatori delegati dal Cliente.

La conservazione delle evidenze del riconoscimento può essere demandata al Cliente da Namirial.

3.3.1. Documenti di riconoscimento accettati

Il Richiedente, cittadino italiano, può identificarsi per mezzo di un documento d'identità in corso di validità, quali:

- Carta d'identità,
- Passaporto,
- Patente di guida.

Possono essere concordate tra Namirial e il Cliente altre categorie di documenti di riconoscimento, tra quelle previste dal comma 2 dell'art. 35 del DPR 445/2000.
In caso di Clienti operanti a livello internazionale o cittadini stranieri che richiedano un Certificato, i documenti che possono essere presentati sono:

- Carta d'identità,
- Passaporto,

le cui caratteristiche sono verificabili all'interno del database PRADO (https://www.consilium.europa.eu/prado/en/prado-start-page.html).
È facoltà del soggetto che effettua l'identificazione escludere l'ammissibilità del documento utilizzato dal Titolare se ritenuto non rispondente ai requisiti di autenticità e integrità.

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 di Namirial S.p.A.

3.4. Modalità di Identificazione per Persone Fisiche

L'identità del Titolare può essere accertata dal Cliente mediante le modalità pattuite con la Certification Authority, anche tramite strumenti messi a disposizione dalla Certification Authority stessa.

3.5. Identificazione ed Autenticazione per il rinnovo delle chiavi e dei Certificati

Non previsto

3.6. Identificazione ed Autenticazione per la richiesta di sospensione e revoca

I Certificati emessi secondo il presente Manuale Operativo sono di tipo *disposable* e, di conseguenza, non prevedono la possibilità di essere sospesi o revocati.

4. Requisiti operativi del ciclo di vita dei Certificati

Questa sezione descrive le modalità con le quali opera Namirial ed in particolare l'organizzazione e le funzioni del personale addetto al servizio di certificazione, le modalità di richiesta del Certificato nominale non qualificato e le modalità di comunicazione con il Richiedente il Certificato ovvero con il Titolare del Certificato.
Se non diversamente indicato nel presente documento e in accordo con lo standard ETSI 319-411, i seguenti requisiti operativi sono applicati al ciclo di vita del Certificato.

4.1. Soggetti che possono richiedere il rilascio di un Certificato

I Certificati rilasciati esclusivamente a persona fisica sono relativi a chiavi di sottoscrizione generate per l'uso attraverso applicazioni di firma remota *disposable* con limitata disponibilità temporale.

I Richiedenti sono soggetti a un processo di registrazione composto da:

- Compilazione di un apposito form;
- Accettazione delle Condizioni Generali.

4.2. Richiesta del Certificato

Le condizioni per l'identificazione e autenticazione sono descritte nel dettaglio al Capitolo 3.

4.3. Registrazione degli utenti

Le procedure per la registrazione del Richiedente e il rilascio del Certificato prevedono:

- che il Richiedente venga identificato con certezza dal Cliente
- che il Richiedente abbia preso visione dell'informativa di cui all'art. 13 del GDPR
- ove previsto, che il Richiedente abbia comunicato il proprio numero di cellulare da utilizzare per l'inoltro di OTP via SMS;
- che il Richiedente abbia preso visione delle Condizioni Generali di contratto e del presente Manuale Operativo;
- che il Richiedente abbia manifestato la volontà di ottenere il rilascio di un Certificato non qualificato di tipo *disposable* previa conferma ed accettazione della adeguata richiesta di registrazione.

4.4. Processo di registrazione

I partecipanti al processo di registrazione (Titolari, Richiedenti, LRA, RAO) concorrono al buon esito dell'emissione del Certificato, ciascuno assolvendo alle proprie responsabilità.

Il Certificatore, terminata la fase di identificazione, effettua l'operazione di registrazione del Richiedente/Titolare attraverso il portale web messo a disposizione della Certification Authority, ovvero attraverso i web-service previsti, i quali registrano i dati forniti all'interno dei propri database.
Le attività di registrazione, oltre che essere svolte direttamente dal personale autorizzato del Certificatore, possono essere svolte dal personale delle LRA.

4.5. Elaborazione della richiesta

Gli attributi acquisiti dalla CA funzionali all'emissione dei Certificati e riferiti al Titolare sono:

- Nome e cognome
- Data di nascita
- Luogo di Nascita
- Codice Fiscale se il Titolare è cittadino italiano. Nel caso in cui il Titolare sia cittadino estero, vengono acquisiti i dati specificati nell'apposita sezione *3.1.3 Univocità dei nomi*
- Estremi del documento di riconoscimento
- Indirizzo fisico di residenza e/o indirizzo e-mail
- Recapito mobile

4.6. Emissione del Certificato

Qualora l'esito delle verifiche degli attributi di cui ai precedenti paragrafi sia positivo, viene inviata alla CA la richiesta di emissione del Certificato.
In caso contrario, la Certification Authority può rifiutarsi di portare a termine l'emissione del Certificato, ad esempio se le informazioni sono assenti, incomplete o inconsistenti, se sussistono dubbi sull'identità del Titolare o del Richiedente o se la documentazione fornita non è conforme a quanto disposto dal Certificatore.

4.7. Procedura di generazione delle chiavi

La procedura di generazione delle chiavi prevede i seguenti step:

- assegnazione al Titolare di un codice identificativo univoco nell'ambito degli utenti del Certificatore (CUC), diverso per ogni Certificato emesso;
- generazione del Certificato contenente la chiave pubblica e i dati previsti mediante la firma con la chiave di certificazione della CA;
- inserimento del Certificato nel registro dei Certificati;
- registrazione sul giornale di controllo dell'avvenuta generazione;
- trasmissione del Certificato dalla CA alla LRA;
- registrazione sul giornale di controllo dell'avvenuta emissione del certificato.

4.8. Accettazione del Certificato

Il Certificatore non prevede alcun comportamento concludente al momento del rilascio del Certificato. Quest'ultimo si intende accettato alla sua emissione.

4.9. Coppia di chiavi e utilizzo del Certificato

Il Certificato rilasciato ai sensi del presente manuale operativo è un certificato non qualificato contraddistinto dall'OID: **1.3.6.1.4.1.36203.10.1**

Questo certificato riporta la seguente Notice: "IT:Certificato emesso ai fini della creazione di firme elettroniche non qualificate. Non è un certificato qualificato ai sensi del Regolamento (UE) n. 910/2014 (eIDAS)" / "EN:Certificate issued for the purpose of creating non-qualified electronic signatures. It is not a qualified certificate within the meaning of Regulation (EU) No. 910/2014 (eIDAS)."

I Certificati emessi sono finalizzati esclusivamente alla sottoscrizione di documenti informatici che non prevedono l'utilizzo di una firma elettronica qualificata (Key Usage: non ripudio).
Il proprietario del Certificato deve salvaguardare la propria chiave privata, facendo attenzione ad evitarne la divulgazione a terzi.

I Certificati devono essere usati solo come prescritto dalla Certificate Policy e dalle Condizioni Generali. Qualsiasi uso diverso è proibito.

4.10. Limitazioni d'uso

I Certificati emessi sono finalizzati esclusivamente alla sottoscrizione di documenti che non prevedono l'utilizzo di una firma elettronica qualificata (key usage: non ripudio).

Nel caso specifico dei Certificati di tipo *disposable*, il certificato emesso, utilizzabile esclusivamente in flussi concordati dal Certificatore con il Cliente, riporta il seguente limite d'uso:

"*L'utilizzo del certificato è limitato esclusivamente alla sottoscrizione dei documenti indicati dal soggetto che ne ha richiesto il rilascio*".

4.11. Rinnovo del Certificato

Non previsto.

4.12. Modifica del Certificato

Un Certificato firmato dalla CA emittente non può essere modificato. Al fine di rimediare a potenziali imprecisioni subite durante il processo di generazione, è necessario emettere un nuovo Certificato.

4.13. Revoca e sospensione del Certificato

La sospensione o revoca del Certificato 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.
La sospensione del Certificato comporta la non validità delle firme generate durante il periodo di sospensione.
Sospensione e revoca non si applicano ai Certificati di tipo *disposable*.

4.14. Servizio di verifica dello stato del Certificato

La CA Namirial fornisce servizi di controllo per verificare lo stato del Certificato, come CRL e OCSP. Lo stato del Certificato (che potrebbe essere attivo, sospeso o revocato) è reso disponibile a tutte le entità coinvolte pubblicando la Certificate Revocation List (CRL). La CA rende anche disponibile un OCSP (On-line Certificate Status Provider) al seguente link: http://ocsp.namiriatsp.com/ocsp/certstatus. La CRL è firmata al momento della sua emissione, con il Certificato della CA.
Sia la CRL che l'OCSP sono disponibili 24 ore per 7 giorni la settimana.

4.15. Modalità di sostituzione delle chiavi

4.15.1. Sostituzione delle chiavi di sottoscrizione degli utenti

Qualora si rendesse necessaria la sostituzione del Certificato, a causa di variazioni delle informazioni in esso contenute, si procederà con la revoca di tale Certificato e con una nuova emissione.

4.15.2. Sostituzione delle chiavi di certificazione

Avviene nel rispetto dell'art. 30 del DPCM 22 febbraio 2013. Il Certificato "Root" della CA utilizzato dal Certificatore per sottoscrivere i Certificati del Titolare ha durata 20 anni e viene sostituito all'occorrenza per garantire la fruibilità di tutti i Certificati emessi fino alla naturale scadenza degli stessi.

4.16. Risoluzione della sottoscrizione

Il contratto di servizio si considera terminato alle seguenti date:

- data di scadenza del Certificato;
- data di revoca del Certificato.

4.17. Key escrow e recupero delle chiavi

Non previsto.

5. Controlli e misure di sicurezza

Il sito primario di produzione (Data4) è localizzato a Milano, con sito di Disaster Recovery collocato presso Adam Ecotech S.L, situato nel Parco tecnologico Vallés, precisamente in Carrer dels Artesans, 7, 08290 Cerdanyola del Vallès, Barcellona, Spagna.
Sono definite politiche, responsabilità e procedure operative per l'accesso alle aree protette di Data4. In queste aree sono implementati dispositivi di protezione fisica per minimizzare i rischi legati ad accessi non autorizzati. La protezione è implementata da sistemi di controllo degli accessi e da sistemi di videosorveglianza posizionati nei punti più critici e segnalati da apposita cartellonistica. Il sito di Disaster Recovery è collocato in un Datacenter certificato, dotato di tutte le misure di sicurezza.

5.1. Controlli fisici

Le aree di lavoro sono sottoposte a diverse misure di controllo, in relazione ai rischi, al valore degli asset e alle informazioni da proteggere. Un processo di autorizzazione organizzato, relativo al tipo di area, gestisce tutti gli accessi.

5.1.1. Collocazione del sito

Namirial esegue le sue operazioni CA da data center sicuri e dotati di controlli logici e fisici che rendono le operazioni CA Namirial inaccessibili a personale non autorizzato.
Il data center primario è collocato presso il Campus di Data4 (Cornaredo, MI), mentre il sito di ADAM, viene attivato in caso di disastro.
Namirial opera, per ciascuno dei siti di erogazione, in conformità ad una politica di sicurezza progettata per rilevare, scoraggiare e prevenire l'accesso non autorizzato alle operazioni dell'Organizzazione.

5.1.2. Accessi fisici

Le attrezzature Namirial sono protette da accessi non autorizzati su cui sono implementati controlli fisici per ridurre il rischio di manomissione delle attrezzature. Le parti sicure delle strutture di hosting sono protette mediante controlli di accesso fisici che le rendono accessibili solo a persone debitamente autorizzate. Gli edifici sono sotto costante sorveglianza video.
L'accesso alla sala del Datacenter Data4 è regolamentato dalle procedure di quest'ultimo.

5.1.3. Energia elettrica e condizionamento

I Data Center hanno alimentatori primari e secondari che assicurano un accesso continuo e ininterrotto all'energia elettrica. Gli alimentatori ininterrotti (UPS) e i generatori elettrici forniscono un'alimentazione di backup ridondante. Le strutture dei Data Center

utilizzano sistemi multipli per il riscaldamento, il raffreddamento e la ventilazione dell'aria.

5.1.4. Esposizione all'acqua

Un sistema di rilevamento rileva la presenza di liquido attraverso dei sensori e determina lo scatto dell'allarme in caso di allagamento.

5.1.5. Prevenzione degli incendi

I Data Center sono dotati di meccanismi di soppressione degli incendi.

5.1.6. Media storage

Gli asset sono protetti dai danni accidentali e dall'accesso fisico non autorizzato.

5.2. Controlli procedurali

5.2.1. Trusted roles

Il personale nominato secondo i trusted roles previsti dallo standard ETSI EN 319-401 include gli operatori addetti all'amministrazione del sistema CA e RA. Le funzioni e i compiti svolti dai trusted roles sono distribuiti per permettere che una sola persona autonomamente non possa aggirare le misure di sicurezza o sovvertire la sicurezza e l'affidabilità delle operazioni della PKI. Tutto il personale nominato secondo trusted roles deve essere libero da conflitti di interesse che possano essere pregiudizievoli a livello di imparzialità nelle operazioni della PKI Namirial.
I trusted roles sono nominati dal management. Un elenco del personale nominato in tali ruoli viene mantenuto e rivisto dall'Organizzazione. Le responsabilità previste dai trusted roles sono le seguenti:

- Responsabili della sicurezza (Security Officers): Responsabilità della definizione delle policy di sicurezza.
- Amministratori di sistema: Autorizzati a installare, configurare e mantenere i sistemi trust Namirial per la gestione del servizio
- Operatori di sistema: Responsabili del funzionamento quotidiano dei sistemi trust Namirial. Sono autorizzati ad eseguire il backup del sistema.
- Auditor di sistema: Autorizzati a visualizzare gli archivi e i log di audit dei sistemi trust Namirial.

5.2.2. Numero delle persone coinvolte nelle attività

In caso di compiti relativi a funzioni critiche, Namirial richiede che almeno due persone agiscano in un trusted role per evitare che una persona possa agire in autonomia. Quando questo meccanismo è attivo, due persone autorizzate sono tenute ad applicarlo ove opportuno.

5.2.3. Identificazione ed autenticazione per ciascun ruolo

Il personale preposto a questi servizi è tenuto ad autenticarsi ai sistemi CA e RA prima di accedere agli ambienti necessari per svolgere i propri ruoli di fiducia.

5.2.4. Attività che richiedono il dual control

Le attività che richiedono la segregation of duties sono le seguenti:

- La verifica delle informazioni nella generazione di Certificati CA (root e intermedi, ove applicabile);
- L'approvazione delle richieste di Certificati CA;
- La maggior parte dei compiti relativi alla gestione delle chiavi CA o all'amministrazione CA.

Namirial, per queste attività individua tra i propri dipendenti delle figure adeguate ai trusted roles definiti in precedenza, cui può essere assegnato solo un ruolo tra amministratore o auditor, ma entrambi possono ricoprire anche il ruolo di operatore.

5.3. Controlli sul personale

Le figure identificate da Namirial per ricoprire i trusteed roles possiedono adeguata esperienza nella definizione, sviluppo e gestione di servizi PKI ed hanno ricevuto un necessario livello di formazione su procedure e strumenti che possono essere utilizzati in varie fasi operative.
Il personale Namirial incaricato a queste attività deve:

- possedere la competenza, l'affidabilità, l'esperienza e le qualifiche necessarie e aver ricevuto formazione relativa alle norme di sicurezza e di protezione dei dati personali adeguata ai servizi offerti e alla loro funzione lavorativa;
- essere in grado di soddisfare il requisito di "conoscenza, esperienza e qualifiche" attraverso formazione o esperienza effettiva, o una combinazione di entrambe;
- essere aggiornato circa le nuove minacce e sulle più recenti pratiche di sicurezza applicabili.

5.3.1. Qualifiche, esperienza e requisiti di autorizzazione

Namirial assume personale con i più alti livelli di integrità e competenza. Non esiste alcun requisito di cittadinanza per il personale che svolge i trusted roles associati all'emissione di altri tipi di Certificati.

5.3.2. Check delle esperienze pregresse

Namirial verifica l’identità ed esegue un controllo delle esperienze pregresse di ogni dipendente al fine di affidare uno dei trusted roles previsti ed indicati in precedenza.

5.3.3. Requisiti di formazione

Tutto il nuovo personale Namirial riceve una formazione di base sulla security awareness durante il processo di onboarding a livello aziendale. Oltre a ciò, una formazione on-the-job dedicata viene fornita a tutto il personale Namirial coinvolto in compiti specifici, come descritto nel presente documento.

5.3.4. Frequenza di aggiornamento della formazione e requisiti

Il personale è tenuto a mantenere alti livelli di competenza attraverso sessioni di formazione pertinenti al settore per poter continuare ad agire in conformità ai requisiti richiesti dai trusted roles. Namirial mette al corrente di eventuali modifiche circa la normale operatività tutti coloro che ricoprono tali ruoli. La formazione al personale avviene con cadenza almeno annuale.

5.3.5. Frequenza della job rotation

In caso di job rotation, Namirial esegue un controllo di sicurezza, compresa una verifica delle credenziali a livello di reti, sistemi, applicazioni o altre risorse utilizzate, nonché le autorizzazioni di accesso alle strutture e alle aree.

5.3.6. Sanzioni in caso di azioni non autorizzate

Il personale Namirial che non segue le politiche e le disposizioni interne all'Organizzazione, sia per negligenza che per dolo, è soggetto a sanzioni disciplinari, compresa la cessazione del rapporto di lavoro o di collaborazione e, nei casi più gravi a sanzioni penali da parte dell'autorità competente.

5.3.7. Requisiti del personale non dipendente

Il personale non dipendente, che sia stato incaricato di un trusted role, è soggetto ai requisiti ed ai doveri specifici di tale ruolo nonché alle eventuali sanzioni.

5.3.8. Documentazione fornita al personale

Al personale, in fase di onboarding, sono fornite le informazioni necessarie per svolgere i propri compiti, compresa una copia del presente documento e la documentazione operativa necessaria per mantenere l'integrità delle operazioni della CA Namirial.

5.4. Procedure di gestione del giornale di controllo

Namirial registra tutte le informazioni rilevanti relative ai dati emessi e ricevuti dalla stessa e mantiene le registrazioni accessibili per un periodo di 20 anni, allo scopo di fornire prove adeguate in procedimenti legali e garantire la continuità del servizio.

5.4.1. Frequenza di salvataggio del giornale di controllo

La frequenza di salvataggio del giornale di controllo è giornaliera.
L'ora esatta di significativi eventi ambientali, di gestione delle chiavi e di sincronizzazione dell'orologio di Namirial sono registrati. L'ora utilizzata per registrare gli eventi come richiesto nel giornale di controllo deve essere sincronizzata con UTC almeno una volta al giorno.

5.4.2. Conservazione delle registrazioni del giornale di controllo

La procedura messa in atto dal Certificatore prevede che gli eventi rilevati e disponibili sul database vengano estratti ed inseriti all'interno di file di testo gestiti in maniera tale da garantirne l'integrità e la disponibilità.
Le registrazioni relative al funzionamento dei servizi sono a disposizione dell'Autorità Giudiziaria nel caso di procedimenti legali ed internamente ai fini di audit e verifiche periodiche del sistema.

5.4.3. Backup del giornale di controllo

La sincronizzazione degli eventi con il repository presente sul sito di Disaster Recovery avviene con frequenza almeno giornaliera.

5.5. Archiviazione dei record

Namirial produce e conserva registri accessibili che comprendono tutte le attività e tutte le informazioni rilevanti relative ai dati emessi e ricevuti da Namirial.
La CA mantiene i registri accessibili per un periodo di 20 anni, allo scopo di fornire prove adeguate in procedimenti legali e garantire la continuità del servizio. Questi registri restano accessibili anche nel caso in cui Namirial abbia cessato le proprie attività.
Le principali evidenze raccolte sono:

- Richieste di emissione;
- Documentazione fornita dai Richiedenti;
- CSR (Certificate Signing Request) fornite dai Richiedenti;
- Dati personali del Titolare;
- Richieste di revoca o sospensione;
- Tutti i Certificati emessi;
- Giornale di controllo per 20 anni.

5.6. Sostituzione della chiave

Nel caso in cui l'utente finale (Titolare) decida di utilizzare una nuova chiave, deve necessariamente richiedere un nuovo Certificato.

5.7. Compromissione della chiave e disaster recovery

La compromissione della chiave di certificazione rappresenta un evento critico, che innescherebbe l'attivazione del Piano di Cessazione della Certification Authority.
La continuità operativa è garantita anche in situazioni di elevata criticità o disastro.

5.8. Piano di cessazione

Namirial ha definito un piano di cessazione aggiornato. In particolare, secondo tale procedura interna, Namirial dovrà:

- informare almeno 90 giorni prima della cessazione i seguenti soggetti: tutti i Richiedenti e gli altri soggetti con i quali Narmirial ha accordi o relazioni, tra cui i Destinatari e le autorità competenti (AgID e l'organismo di certificazione). Inoltre, queste informazioni devono essere messe a disposizione di altre parti facenti affidamento;
- porre fine all'autorizzazione di tutti i subappaltatori ad agire per conto di Namirial nello svolgimento di qualsiasi funzione relativa al processo di emissione di Certificati;
- trasferire gli obblighi a una parte affidabile per il mantenimento di tutte le informazioni necessarie a fornire la prova del funzionamento di Namirial per un periodo ragionevole, a meno che non sia possibile dimostrare che Namirial non detenga alcuna informazione;
- le chiavi private devono essere distrutte, o ritirate, per assicurare che non possano essere recuperate;
- prendere accordi per trasferire la fornitura di servizi fiduciari per i suoi clienti esistenti ad un altro Trust Service Provider.

La Certification Authority ha redatto il proprio "Piano di Cessazione" ad uso esclusivo del Certificatore ed in conformità all'art. 24 eIDAS.

6. Controlli di sicurezza tecnica

6.1. Generazione della coppia di chiavi

La CA emette i Certificati non qualificati in conformità con il regolamento (UE) n. 910/2014 e successive modifiche introdotte dal Regolamento (UE) n.1183/2024. Le chiavi di certificazione utilizzate per la firma dei Certificati sono generate per mezzo di dispositivi e procedure che garantiscono l'unicità, la segretezza e la resilienza della chiave privata.
La CA utilizza una coppia di chiavi crittografiche di almeno 4096 bit generate all'interno di HSM (Hardware Secure Module).

Gli HSM e le procedure assicurano che:

- le coppie di chiavi siano generate individualmente, sempre in copia unica;
- le coppie di chiavi soddisfino i requisiti imposti dagli algoritmi di generazione e dalle verifiche RSA perché gli HSM possiedono un motore interno di generazione di coppie di chiavi RSA e DSA;
- la generazione di tutte le coppie di chiavi possibili è equiprobabile;
- la persona che attiva le procedure di generazione è sempre identificata;
- la generazione delle coppie di chiavi avviene esclusivamente all'interno dell'HSM;
- se i dispositivi sono preparati o gestiti da una terza parte, Namirial verifica che questa terza parte abbia i requisiti adeguati.

Nelle attività di certificazione, Namirial utilizza l'algoritmo RSA.
La generazione di coppie di chiavi di certificazione da parte della CA è sotto doppio controllo, secondo la procedura della Key Ceremony.

6.2. Modalità di generazione delle chiavi

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 DPCM 22 febbraio 2013 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 DPCM di cui in precedenza.
La generazione delle chiavi avviene all'interno del dispositivo sicuro per la generazione delle firme.

Nel caso in cui la generazione avvenga al di fuori di tale dispositivo, il sistema di generazione è conforme alle disposizioni di cui all'art. 9 del DPCM 22 febbraio 2013.

6.2.1. Modalità di generazione delle chiavi di certificazione

La generazione delle chiavi asimmetriche avviene all'interno dei moduli crittografici dedicati e certificati in presenza del Responsabile del servizio di Certificazione, come previsto dall'art. 7 del DPCM 22 febbraio 2013 ed è generata solo con la presenza contemporanea di due operatori incaricati all'uopo.

6.2.2. Modalità di generazione delle chiavi di sottoscrizione degli utenti

Completata la fase di registrazione, durante la quale i dati del Richiedente vengono memorizzati nel database del Certificatore, è possibile procedere alla generazione delle chiavi di sottoscrizione. Nel caso dei certificati non qualificati la generazione delle chiavi avviene da parte della Certification Authority su HSM.

6.2.3. Consegna della chiave privata al Richiedente

La chiave privata è contenuta all'interno del dispositivo HSM. Il titolare accede alla chiave privata mediante procedura stabilita dal Certificatore e dal Cliente (es. tramite OTP o eID)

6.3. Protezione della chiave privata e controlli ingegneristici sul modulo crittografico

Le coppie di chiavi utilizzate dalla CA per firmare i Certificati e le CRL sono memorizzate in un HSM (Hardware Security Module) di alta qualità.
L'HSM utilizzato da Namirial è Certificato al livello EAL4+ Common Criteria e qualificato ANSSI al massimo livello.

6.3.1. Algoritmi crittografici e lunghezza delle chiavi

Le chiavi usate dal Certificatore per firmare i Certificati hanno lunghezza almeno pari a 4096 bit; la lunghezza della chiave di sottoscrizione dei Titolari è pari almeno a 3072 bit in caso di algoritmo RSA, in caso ECDSA con lunghezza delle chiavi minima di 256 bit.

6.3.2. Funzioni di HASH

Per la generazione dell'impronta viene utilizzata la funzione di hash SHA-256.

6.4. Altri aspetti relativi alla gestione della coppia di chiavi

Namirial usa in modo appropriato le chiavi private di firma della CA e non le utilizza oltre la fine del loro ciclo di vita.

In particolare:

- La chiave di firma della CA utilizzata per la generazione di Certificati e/o l'emissione di informazioni sullo stato di revoca, non viene utilizzata per nessun altro scopo;
- Le chiavi di firma della CA sono utilizzate solo all'interno di locali fisicamente sicuri;
- L'uso della chiave privata della CA è compatibile con l'algoritmo di hash, l'algoritmo di firma e la lunghezza della chiave di firma utilizzata per generare i Certificati;
- Tutte le copie delle chiavi private di firma della CA saranno distrutte alla fine del loro ciclo di vita.

6.5. Dati di attivazione

I dati di attivazione consistono nel set necessario all'attivazione del processo di consegna del Certificato di sottoscrizione.

6.6. Controlli di sicurezza informatica

I sistemi operativi utilizzati dalla CA per gestire i Certificati possiedono un elevato livello di sicurezza e seguono le procedure di hardening stabilite da Namirial. I compiti e le aree di responsabilità sono segregati al fine di minimizzare la possibilità di apportare modifiche non autorizzate o involontarie o abusare degli asset Namirial.
Gli eventi di accesso ai sistemi sono registrati, come descritto nella sezione relativa ai controlli fisici.
I componenti della rete locale, sia fisici che logici, sono mantenuti in un ambiente sicuro e le configurazioni sono periodicamente controllate per verificarne la conformità ai requisiti specificati da Namirial.
Sono implementati dei job che verificano il controllo dell'integrità del software della CA e della sua configurazione.
Sono previste strutture di monitoraggio continuo e alert per consentire a Namirial di rilevare, registrare e reagire tempestivamente a qualsiasi tentativo non autorizzato e/o irregolare di accesso alle proprie risorse.

6.7. Controlli di sicurezza sul ciclo di vita del processo

6.7.1. Controlli sugli asset

Namirial utilizza sistemi e prodotti affidabili protetti da modifiche e che garantiscono la sicurezza tecnica e l'affidabilità dei processi da essi supportati.

In particolare:

- Un'analisi dei requisiti di sicurezza viene effettuata durante la fase di progettazione e identificazione dei requisiti di qualsiasi progetto di sviluppo di sistemi intrapreso da Namirial;

- Le procedure di change management sono applicate a rilasci, modifiche e patch di emergenza di qualsiasi software operativo nonché a changes a livello di configurazione cui si applica la politica di sicurezza delle informazioni.
- L'integrità dei sistemi e degli asset Namirial è protetta da virus, software maligni e non autorizzati.
- Le procedure di gestione dei media sono definite e implementate al fine di proteggere questi da danni, furti, accessi non autorizzati, obsolescenza e deterioramento nel periodo di tempo in cui i record devono essere conservati.
- Le procedure organizzative sono definite e implementate al fine di gestire tutti i ruoli di fiducia e amministrativi che hanno un impatto sulla fornitura dei servizi.

6.7.2. Controlli sulla chiave privata

Al fine di emettere e gestire le chiavi CA in modo sicuro, Namirial utilizza HSM (Hardware Security Module), che:

- Garantiscono la protezione delle chiavi secondo i livelli di sicurezza previsti dalla normativa e l'elevato standard tecnologico;
- impediscono qualsiasi tentativo non autorizzato di lettura, duplicazione, estrazione della chiave privata
- conserva la Chiave Privata per garantirne l'integrità per l'intero ciclo di vita;

6.8. Controlli di network security

L'architettura di rete di Namirial è strutturata su più livelli in modo da creare ambienti di rete separati, indirizzati a host relativi a funzioni diverse e caratterizzati da diversi livelli di criticità.
La sicurezza degli accessi e del traffico di rete è garantita mediante l'applicazione di politiche di protezione implementate sui sistemi firewall dislocati su diversi livelli di rete.
Le richieste di implementazione di nuove regole sul firewall sono gestite attraverso una change request.
L'attivazione di regole che causano un alto livello di impatto, viene trattata con il Security Officer. La sicurezza della rete privata CA è realizzata non solo dai sistemi di protezione perimetrale descritti in precedenza, ma anche da una configurazione specifica che mantiene gli indirizzi interni come riservati. Le comunicazioni tra le stazioni di gestione e i sistemi sono protette per mezzo di strumenti che assicurano l'autenticazione tra le parti e la loro privacy.
I potenziali collegamenti remoti avvengono su un canale VPN criptato e richiedono l'autenticazione tramite Username, Password e un token di autenticazione (OTP).
La comunicazione tra i moduli applicativi della piattaforma PKI di Namirial avviene attraverso canali crittografici.
La comunicazione tra gli utenti che accedono ai servizi online avviene attraverso connessioni TLS/SSL con algoritmo SHA -256.

Il sistema implementato per gestire gli accessi degli utenti fornisce sia meccanismi AAA (autenticazione, autorizzazione, accesso) e di profilazione che la crittografia del canale di comunicazione con protocollo TLS/SSL.
Il sistema dovrebbe anche gestire gli accessi che provengono dai consulenti che lavorano sulla rete interna di Namirial.

7. Policy, limiti d'uso e gestione dei Certificati

7.1. Profili dei Certificati

I Certificati sono conformi ai seguenti requisiti normativi:

- international standard ISO/IEC 9594-8:2005 [X.509 versione 3];
- specifiche pubbliche IETF RFC 5280 Management of Reliable Public Certificates;
- ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles (Part 1, 2).

La CA compila i campi dell'emittente e del soggetto di ogni Certificato emesso in seguito all'adozione dei requisiti, definiti sopra, in conformità con quanto dichiarato nel presente documento. Con l'emissione del Certificato, la CA dichiara di aver seguito la procedura descritta nel documento per dimostrare che, alla data di emissione del Certificato, tutte le informazioni relative al soggetto erano accurate.
Le sezioni seguenti descrivono i principali attributi normalmente inclusi in ogni Certificato non qualificato emesso da Namirial. Qualora il Richiedente richieda un nuovo tipo di attributi, non inclusi di seguito, Namirial li imposterà di conseguenza, a condizione che il nuovo set di attributi sia conforme alle specifiche di cui sopra.
L'emissione di Certificati avviene utilizzando il seguente Certificato CA root:

Nome CA Root	Scopo	Note
Namirial EU Qualified CA	Emissione certificati per firma digitale	Certificato CA Root

Tabella 4: Certificate profile

7.1.1. Namirial EU Qualified CA

Version	Version 3
Serial Number	39 61 62 D9 E5 04 83 A3
Signature	sha256, RSA
Issuer (ETSI 319 412-2 par. 4.2.3.1)	Issuer DN: **countryName**: "IT" **organizationName**: "Namirial S.p.A." organizationalUnit: "Trust Service Provider" **commonName**: " Namirial EU Qualified CA"
Validity Period	20 Years (expire 20 years from the date of issue)
Subject	Equal to Issuer
SubjectPublicKeyInfo	Public Key 4096 bit Algorithm: RSA

Extentions	
Subject Key Identifier	63 B8 CD B8 49 52 E5 E7 09 7B 57 8C FB 7A 41 0E 41 AA 78 59
Authority Key Identifier	63 B8 CD B8 49 52 E5 E7 09 7B 57 8C FB 7A 41 0E 41 AA 78 59
Certificate Policies	Not critical Policy OID 1.3.6.1.4.1.36203.1.1
crlDistributionPoint	Not critical http://crl.namirialtsp.com/CA4K.crl
Basic Constraint (critical)	Critical Subject Type: CA Path Length Constraint: no constraint
KeyUsage (critical)	CertSign, cRLSign

Il certificato radice e le CRL emesse dal Certificatore sono pubblicate sul sito Namirial alla pagina Documentazione | Namirial.com

7.2. Registro dei Certificati

Il registro dei Certificati contiene:

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

7.3. Accesso al registro dei Certificati

È consentito l'accesso libero alle liste dei certificati sospesi e revocati. I registri contenenti le informazioni sul ciclo di vita dei certificati sono accessibili esclusivamente alla CA.

7.4. 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 non 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 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.

7.5. Archiviazione dei Certificati

I Certificati sono archiviati e conservati per 20 (venti) anni dalla emissione.
Le chiavi private di firma di cui sia scaduto il Certificato non possono più essere utilizzate.

8. Altri aspetti legali

8.1. Responsabilità finanziaria

Namirial ha sottoscritto un'assicurazione adeguata a coprire i rischi dell'attività e gli eventuali danni derivanti dal servizio di certificazione.

8.2. Responsabilità del Titolare

Il Titolare ha la responsabilità di fornire informazioni certe, veritiere e riconducibili alla propria identità. È chiamato altresì al rispetto delle modalità previste per l'emissione e la custodia delle credenziali, nonché all'attenta lettura del materiale informativo messo a disposizione della CA, di cui il presente manuale è parte. Tale soggetto è inoltre tenuto a seguire in maniera scrupolosa le indicazioni fornite dal Certificatore.

8.3. Responsabilità della CA e limitazioni agli indennizzi

8.3.1. Limitazioni di responsabilità del Certificatore

Il Certificatore è responsabile, verso i Titolari, per l'adempimento degli obblighi di legge derivanti dalle attività previste dal D.Lgs. 82/2005, dal DPCM 22 febbraio 2013, dal Regolamento eIDAS, dal DPR 445/2000, e successive modifiche ed integrazioni.

Il Certificatore non assume responsabilità:

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

8.4. Confidenzialità e trattamento dei dati personali

8.4.1. Protezione dei dati personali

Le procedure e le modalità operative che Namirial S.p.A., in qualità di Titolare del trattamento dei dati personali, adotta nello svolgimento della propria attività, sono descritte interamente nell'Informativa Privacy consegnata al Titolare in fase di emissione del Certificato e disponibile sul sito di Namirial https://www.namirial.com/it/documentazione/. Le informazioni personali, concernenti i Titolari dei Certificati e, più in generale i clienti del servizio erogato vengono trattate, conservate e protette in conformità a quanto previsto nel Regolamento europeo 679/2016 in materia di protezione dei dati personali.

8.4.2. Tutela e diritti degli interessati

L'accesso ai propri dati da parte degli interessati è consentito tramite richiesta scritta da far pervenire al responsabile per la protezione dei dati tramite e-mail all'indirizzo dpo@namirial.com che provvederà ad evadere la richiesta senza ingiustificato ritardo. Il DPO valuta richieste d'accesso pervenute unicamente dall'interessato, o in alternativa di terzi con apposita procura, di cui verifica l'attendibilità.

Gli interessati devono prestare consenso scritto al trattamento dei propri dati da parte di Namirial S.p.A. in caso di attività che lo richiedano, in conformità all'informativa sul trattamento dei dati personali.

8.4.3. Modalità del trattamento

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

8.4.4. Finalità del trattamento

I dati personali vengono acquisiti in osservanza alle finalità esplicitate nell'informativa fornita al Richiedente durante le fasi di richiesta del Certificato. L'informativa è anche pubblicata su https://www.namirial.com/it/documentazione/

8.4.5. Sicurezza dei dati

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

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

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

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

8.5. Archivi contenenti dati personali

L'archivio contenente i dati personali è il database di registrazione.
Gli archivi sopra elencati sono gestiti dal responsabile della registrazione e sono adeguatamente protetti da accessi non autorizzati, in conformità a quanto previsto dal GDPR e successivi aggiornamenti.

8.6. Diritti di proprietà intellettuale

Questo documento è di proprietà di Namirial, che si riserva tutti i diritti relativi ad esso. Il proprietario del Certificato mantiene tutti i diritti sul proprio marchio (brand name) e sul suo nome di dominio. In relazione alle proprietà di altri dati e informazioni si applica la legge in vigore.

8.7. Obblighi e garanzie

8.7.1. Certification Authority

La CA è obbligata a:

- Operare in conformità con questo documento;
- Identificare Richiedenti/Titolari come descritto in questo documento;
- Emettere e gestire i Certificati come descritto in questo documento;
- Fornire un servizio efficiente di sospensione o revoca dei Certificati;
- Assicurarsi che il proprietario possieda, al momento dell'emissione del Certificato, la chiave privata corrispondente;
- Segnalare tempestivamente l'eventuale compromissione della chiave privata;
- Fornire informazioni chiare e complete sulle procedure e sui requisiti del servizio;
- Fornire una copia di questo documento a chiunque ne faccia richiesta;
- Garantire che la fornitura di servizi di firma digitale sia accessibile alle persone con disabilità;
- Garantire un trattamento dei dati personali conforme alla normativa vigente;
- Garantire la disponibilità del servizio, salvo in caso di attività di manutenzione programmata, preventivamente comunicata;
- Fornire un servizio di informazione efficiente e affidabile sullo stato dei Certificati.

8.7.2. Local Registration Authority

La Local Registration Authority, identificata nel Cliente, tratta i dati personali dell'interessato con la massima riservatezza e in conformità a quanto previsto dal GDPR.

8.7.3. Richiedenti o Titolari

Il Richiedente o il Titolare ha l'obbligo di:

- Leggere, comprendere e accettare completamente questo documento;
- Richiedere il Certificato fornito da questo documento;

- Fornire alla CA informazioni accurate e veritiere nella fase di registrazione;
- Garantire la privacy dei codici riservati ricevuti dalla CA;
- In seguito all'emissione e fino alla scadenza o alla revoca del Certificato, comunicare tempestivamente alla CA ogni modifica delle informazioni fornite in fase di richiesta.

8.7.4. Utenti finali

Gli utenti finali, quindi tutte le entità (diverse dal Richiedente o dal Titolare) che fanno affidamento sui Certificati emessi ai sensi del presente documento, hanno l'obbligo di:

- Fare in modo di ottenere informazioni sufficienti sul funzionamento dei Certificati e della PKI;
- controllare lo stato dei Certificati emessi da Namirial sulla base del presente documento;
- fare affidamento su un Certificato solo se non è scaduto, sospeso o revocato.

9.9 Limitazioni di garanzia

Si applica quanto descritto all'interno del documento NAM CA01D_NQ_ITA "Emissione di certificati non qualificati di firma elettronica di tipo disposable - CONDIZIONI GENERALI DI CONTRATTO" pubblicato sul sito https://www.namirial.com/it/documentazione/.

9.10 Limitazioni di indennizzo

Si applica quanto descritto all'interno del documento NAM CA01D_NQ_ITA "Emissione di certificati non qualificati di firma elettronica di tipo disposable - CONDIZIONI GENERALI DI CONTRATTO" pubblicato sul sito https://www.namirial.com/it/documentazione/.

9.11 Indennizzi

Si applica quanto descritto all'interno del documento NAM CA01D_NQ_ITA "Emissione di certificati non qualificati di firma elettronica di tipo disposable - CONDIZIONI GENERALI DI CONTRATTO" pubblicato sul sito https://www.namirial.com/it/documentazione/.

9.12 Termini e risoluzione

Si applica quanto descritto all'interno del documento NAM CA01D_NQ_ITA "Emissione di certificati non qualificati di firma elettronica di tipo disposable - CONDIZIONI GENERALI DI CONTRATTO" pubblicato sul sito https://www.namirial.com/it/documentazione/.

9.13 Comunicazioni

Si applica quanto descritto all'interno del documento NAM CA01D_NQ_ITA "Emissione di certificati non qualificati di firma elettronica di tipo disposable - CONDIZIONI GENERALI DI CONTRATTO" pubblicato sul sito https://www.namirial.com/it/documentazione/.

9.14 Procedure di risoluzione delle controversie

Si applica quanto descritto all'interno del documento NAM CA01D_NQ_ITA "Emissione di certificati non qualificati di firma elettronica di tipo disposable - CONDIZIONI GENERALI DI CONTRATTO" pubblicato sul sito https://www.namirial.com/it/documentazione/.

9.15 Foro competente

Si applica quanto descritto all'interno del documento NAM CA01D_NQ_ITA "Emissione di certificati non qualificati di firma elettronica di tipo disposable - CONDIZIONI GENERALI DI CONTRATTO" pubblicato sul sito https://www.namirial.com/it/documentazione/.

9.16 Legge applicabile

Si applica quanto descritto all'interno del documento NAM CA01D_NQ_ITA "Emissione di certificati non qualificati di firma elettronica di tipo disposable - CONDIZIONI GENERALI DI CONTRATTO" pubblicato sul sito https://www.namirial.com/it/documentazione/.

Appendice A – Namirial Certificate Policy

Certificate Policies

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

1.3.6.1.4.1.36203	Namirial S.p.A.
1.3.6.1.4.1.36203.1	CA FirmaQualificata
1.3.6.1.4.1.36203.1.1	Policy CA FirmaQualificata
1.3.6.1.4.1.36203.2	CA TSA
1.3.6.1.4.1.36203.2.1	Policy CA TSA
1.3.6.1.4.1.36203.4	CA Autenticazione
1.3.6.1.4.1.36203.4.1	Policy CA Autenticazione
1.3.6.1.4.1.36203.10.1	Policy CA Firma non Qualificata

Tabella 5: Namirial CA Object Identifier

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

1.3.6.1.4.1.36203.10.1	Policy per certificati non qualificati associati ad apparato sicuro per la creazione della firma mediante procedura remota di tipo *disposable*.

Tabella 6: Object Identifier dei Certificati non qualificati emessi da Namirial CA

In relazione ai Certificati qualificati emessi da Namirial, si rimanda totalmente al documento *NAM-MO-FDMT Manuale Operativo dei Servizi di Certificazione e Marcatura Temporale* pubblicato sul https://www.namirial.com/it/documentazione.