

# Autorità di Certificazione

## Dichiarazione di Trasparenza

|               |                           |                      |                                |                          |
|---------------|---------------------------|----------------------|--------------------------------|--------------------------|
| Categoria     | <b>TSP CA Policy</b>      | Codice Documento     | <b>NAMTSP-PDS-IT-v1.1.docx</b> | <b>Namirial S.p.A.</b>   |
| Redatto da    | <b>Simone Baldini</b>     | Nota di riservatezza | <b>Documento Pubblico</b>      | Il Legale Rappresentante |
| Verificato da | <b>Giuseppe Benedetti</b> | Versione             | <b>1.1</b>                     | <b>Davide Ceccucci</b>   |
| Approvato da  | <b>Davide Ceccucci</b>    | Data di emissione    | <b>14/06/2018</b>              | _____                    |



### Namirial S.p.A.

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



– Questa pagina è lasciata intenzionalmente in bianco –



## INDICE

|   |           |
|---|-----------|
| <b>Indice .....</b>   | <b>3</b>  |
| <b>Storia delle modifiche apportate .....</b>                                   | <b>4</b>  |
| <b>Riferimenti .....</b>  | <b>5</b>  |
| <b>1 Introduzione .....</b>   | <b>7</b>  |
| <b>2 Informazioni di contatto .....</b>   | <b>7</b>  |
| <b>3 Tipi di certificati, relativo utilizzo e procedure di validazione.....</b> | <b>7</b>  |
| <b>4 Limitazioni di fiducia .....</b>   | <b>8</b>  |
| <b>5 Obblighi dei titolari .....</b>  | <b>8</b>  |
| <b>6 Obblighi di verifica dello stato dei certificati .....</b>                 | <b>9</b>  |
| <b>7 Limitazioni di garanzia e di responsabilità.....</b>                       | <b>9</b>  |
| <b>8 Accordi applicabili, CPS e CP.....</b>                                     | <b>9</b>  |
| <b>9 Tutela della privacy.....</b>  | <b>9</b>  |
| <b>10 Politiche di rimborso .....</b>   | <b>10</b> |
| <b>11 Norme applicabili, reclami e foro competente.....</b>                     | <b>10</b> |
| <b>12 Accreditamenti, marchi di fiducia e verifiche di conformità.....</b>      | <b>10</b> |



## STORIA DELLE MODIFICHE APPORTATE

| VERSIONE    | 1.1                                      |
|-------------|--|
| Data        | 14/06/2018                               |
| Motivazione | Revisione                                |
| Modifiche   | §9 aggiunto il Regolamento (EU) 679/2016 |

| VERSIONE    | 1.0                            |
|-------------|--------------------------------|
| Data        | 26/05/2017                     |
| Motivazione | Prima emissione del documento. |
| Modifiche   | ---                            |



## RIFERIMENTI

| NUMERO | DESCRIZIONE   |
|--------|---|
| [I]    | Decreto del Presidente della Repubblica (DPR) 28 dicembre 2000 n. 445, "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa", pubblicato sul Supplemento Ordinario alla Gazzetta Ufficiale n. 42 del 20 febbraio 2001.   |
| [II]   | Decreto del Presidente del Consiglio (DPCM) 22 febbraio 2013 "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b) , 35, comma 2, 36, comma 2, e 71."  |
| [III]  | 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) (Testo rilevante ai fini del SEE)   |
| [IV]   | Decreto Legislativo (CAD) 7 marzo 2005, n. 82 "Codice dell'Amministrazione Digitale", pubblicato nella Gazzetta Ufficiale n.112 del 16 maggio 2005 con le modifiche ed integrazioni stabilite dal decreto legislativo 26 agosto 2016, n. 179.   |
| [V]    | 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  |
| [VI]   | DECISIONE DI ESECUZIONE (UE) 2016/650 DELLA COMMISSIONE del 25 aprile 2016 - che stabilisce norme per la valutazione di sicurezza dei dispositivi per la creazione di una firma e di un sigillo qualificati a norma dell'articolo 30, paragrafo 3, e dell'articolo 39, paragrafo 2, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno |
| [VII]  | DECISIONE DI ESECUZIONE (UE) 2015/1505 DELLA COMMISSIONE dell'8 settembre 2015 - che stabilisce le specifiche tecniche e i formati relativi agli elenchi di fiducia di cui all'articolo 22, paragrafo 5, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno  |
| [VIII] | REGOLAMENTO DI ESECUZIONE (UE) 2015/1501 DELLA COMMISSIONE dell'8 settembre 2015 - relativo al quadro di interoperabilità di cui all'articolo 12, paragrafo 8, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno  |
| [IX]   | ETSI EN 319 411-1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements  |
| [X]    | 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  |
| [XI]   | ETSI EN 319 412-1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures  |
| [XII]  | ISO EN UNI 9001:2008 – Sistema Qualità  |
| [XIII] | ISO/IEC 29115:2013 Information technology - Security techniques - Entity authentication assurance framework   |
| [XIV]  | Deliberazione CNIPA n. 45/2009 e s.m.i.   |
| [XV]   | ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers   |



|          |  |
|----------|--|
| [XVI]    | ISMS-DOC-A16-Security breaches reporting procedure-V1 Final  |
| [XVII]   | 20170428-NAM_CA_Struttura_Organizzativa_v3.0   |
| [XVIII]  | Manuale Operativo Servizi di Certificazione e Marcatura Temporale  |
| [XIX]    | IISMS-DOC-08-Regolamento sicurezza delle informazioni aziendali  |
| [XX]     | HR001 Job Profiles TSP   |
| [XXI]    | ISMS Governance Manual   |
| [XXII]   | ISMS-DOC-06-Information Risk Management & Control Manual   |
| [XXIII]  | ISMS-DOC-A17-Business Continuity Policy  |
| [XXIV]   | ISMS-DOC-A16-Incident Management Policy  |
| [XXV]    | ISMS-FORM-08-Risk Assessment and treatment plan Document-V1 Final  |
| [XXVI]   | Proposal for Article 19 Incident Reporting- Annex A  |
| [XXVII]  | Trust Services Practice Statement  |
| [XXVIII] | ISMS-DOC-08-Information Security Operational Policy.23.02.2017-V1  |
| [XXIX]   | Firma Elettronica Qualificata Remota - Richiesta autorizzazione all'uso di apparati Thales ai sensi dell'art. 35 comma 5 del CAD |



## 1 INTRODUZIONE

Questo documento rappresenta la Dichiarazione di Trasparenza (PKI Disclosure Statement), ai sensi della norma europea ETSI EN 319 411-1, relativa al servizio di certificazione erogato dal Prestatore di Servizi Fiduciari (Trust Service Provider) Namirial S.p.A.

Nel seguito, il servizio di certificazione è anche detto "servizio di CA" (Certification Authority).

Con "Regolamento eIDAS" si intende 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".

Questo documento non sostituisce le Condizioni Generali del servizio di CA né le previsioni del Certification Practice Statement (CPS) pubblicate sul sito web della CA (di seguito indicato).

## 2 INFORMAZIONI DI CONTATTO

La CA è contattabile ai seguenti riferimenti:

VIA CADUTI SUL LAVORO, 4  
60019 - SENIGALLIA (AN)  
TEL: 071.63494  
FAX: 071.60910

Web site: [https:// http://www.namirialtsp.com](https://http://www.namirialtsp.com)

Info mail: [firmacerta@namirial.com](mailto:firmacerta@namirial.com)

Tel. +39 071.63494

Fax +39 071.60910

Per ogni necessità di chiarimento su questo o altri documenti relativi al servizio di CA di Namirial S.p.A., si prega di inviare una mail all'indirizzo [firmacerta@sicurezza postale.it](mailto:firmacerta@sicurezza postale.it)

Per richiedere la revoca dei certificati, contattare il servizio di assistenza di Namirial S.p.A. mediante fax al numero +39.071.60910 oppure mediante posta elettronica all'indirizzo [firmacerta@namirial.com](mailto:firmacerta@namirial.com). In alternativa, se dotati delle necessarie credenziali di accesso, si può richiedere la revoca del certificato attraverso il portale dei servizi CA del Certificatore. Per maggiori informazioni si rimanda al CPS pubblicato sul sito della CA.

## 3 TIPI DI CERTIFICATI, RELATIVO UTILIZZO E PROCEDURE DI VALIDAZIONE

Namirial S.p.A. eroga certificati qualificati in conformità alla norma europea ETSI EN 319 411 e alle norme ad essa collegate. I certificati sono emessi al pubblico generale (aziende private, enti pubblici, professionisti, privati cittadini, ecc.), alle condizioni pubblicate sul sito web della CA.



Tutti i certificati sono firmati con la funzione di hashing SHA-256. Per maggiori informazioni sulle policy supportate (per es. i relativi OID ed altre caratteristiche) si rimanda alla documentazione pubblicata all'indirizzo <https://docs.namirialtsp.com/>.

I certificati delle chiavi di certificazione (CA emittenti) di Namirial S.p.A. sono pubblicati sul sito web della CA e sul sito web dell'AgID (elenco dei Prestatori di Servizi Fiduciari).

Per la validazione dei certificati, la CA rende disponibili la Lista dei Certificati Revocati (CRL) ed un servizio di interrogazione in standard OCSP. Gli indirizzi (URL) della CRL e del servizio OCSP sono contenuti nei certificati stessi, rispettivamente nelle estensioni CRLDistributionPoints e AuthorityInformationAccess.

## 4 LIMITAZIONI DI FIDUCIA

I certificati qualificati sono emessi per l'apposizione di sigilli e firme elettroniche avanzate e qualificate. Ulteriori limitazioni d'uso possono essere specificate nei singoli certificati mediante l'attributo UserNotice dell'estensione CertificatePolicies.

Eventuali limitazioni sul valore delle transazioni in cui il certificato può essere usato sono specificate all'interno dei singoli certificati attraverso l'estensione qCStatements, mediante la voce QcEuLimitValue.

Le informazioni di registrazione dei titolari ed il giornale degli eventi (event log) relativi al servizio di CA sono conservati da Namirial S.p.A. per 20 anni.

## 5 OBBLIGHI DEI TITOLARI

Il Titolare del certificato ha l'obbligo di:

- fornire alla CA informazioni complete, veritiere ed esatte nella fase di richiesta del certificato;
- utilizzare la propria chiave privata unicamente per gli scopi previsti dal CPS;
- adottare misure di sicurezza atte a prevenire l'uso non autorizzato della propria chiave privata;
- (per i certificati che richiedono l'uso di un dispositivo di firma) nel caso in cui generi da sé la propria coppia di chiavi, generarla all'interno di un dispositivo di firma approvato dalla CA;
- fino alla data di scadenza del certificato, informare prontamente la CA nel caso in cui:
  - o il proprio dispositivo di firma sia andato perso, sia stato sottratto o si sia danneggiato;
  - o abbia perso il controllo esclusivo della propria chiave privata, per es. a causa della compromissione dei dati di attivazione (es. PIN) del proprio dispositivo sicuro di firma;
  - o le informazioni contenute nel certificato siano inesatte oppure non più valide;
- nel caso di compromissione della propria chiave privata (per es. a causa dello smarrimento del PIN del dispositivo di firma o della sua rivelazione a terzi non autorizzata), cessare immediatamente l'utilizzo della stessa ed assicurarsi che non venga più utilizzata.

Per maggiori informazioni si rimanda al CPS.



## 6 OBBLIGHI DI VERIFICA DELLO STATO DEI CERTIFICATI

Tutti coloro che fanno affidamento sulle informazioni contenute nei certificati (in breve ci si riferisce a tali soggetti con "Relying Parties") hanno l'obbligo di verificare che il certificato non sia sospeso o revocato. La verifica può essere fatta mediante consultazione della Lista dei Certificati Revocati (CRL) pubblicata dalla CA o mediante interrogazione del servizio OCSP erogato dalla CA, agli indirizzi (URL) contenuti nei certificati stessi.

## 7 LIMITAZIONI DI GARANZIA E DI RESPONSABILITÀ

Per quanto riguarda le limitazioni di garanzia e di responsabilità, si rimanda alle condizioni generali del servizio CA pubblicate sul sito web di Namirial S.p.A. all'indirizzo: <https://docs.namirialtsp.com/>.

## 8 ACCORDI APPLICABILI, CPS E CP

Gli accordi e condizioni che si applicano al servizio di CA sono contenuti nei seguenti documenti pubblicati sul sito web di Namirial S.p.A. all'indirizzo: <https://docs.namirialtsp.com/>:

- Certification Practice Statement (CPS) ovvero "Manuale Operativo" del servizio di CA
- Condizioni Generali del servizio di CA

Le policy dei certificati (CP) sono indicate nel CPS, oltre che nel presente documento.

## 9 TUTELA DELLA PRIVACY

Namirial S.p.A. rispetta il Regolamento (UE) 679/2016 in tema di privacy, nonché le raccomandazioni e disposizioni del Garante per la Protezione dei Dati Personali. Per ulteriori informazioni si rimanda alle condizioni generali del servizio CA pubblicate sul sito web di Namirial S.p.A. all'indirizzo: <https://docs.namirialtsp.com/>.

Tutte le informazioni relative ai certificati qualificati emessi da Namirial S.p.A. (le evidenze dell'identificazione dei titolari e della loro accettazione delle condizioni generali, i dati di registrazione dei titolari, le richieste di revoca, ecc.) sono conservate da Namirial S.p.A. per 20 anni.



## **10 POLITICHE DI RIMBORSO**

Per quanto riguarda la politica sui risarcimenti, si rimanda alle condizioni generali del servizio CA pubblicate sul sito web di Namirial S.p.A. all'indirizzo: <https://docs.namirialtsp.com/>.

## **11 NORME APPLICABILI, RECLAMI E FORO COMPETENTE**

Il servizio di CA erogato da Namirial S.p.A. è assoggettato alle leggi dell'ordinamento italiano ed europeo. L'applicabilità, l'esecuzione, l'interpretazione e la validità del CPS sono regolate dalle leggi italiane e dalle leggi europee direttamente applicabili, indipendentemente dal contratto o altre scelte di disposizioni di legge e senza la necessità di stabilire un punto di contatto commerciale in Italia. Questa scelta è volta a garantire a tutti gli utenti un'uniformità di procedure e interpretazioni, indipendentemente dal luogo in cui essi risiedono o utilizzano il servizio.

Per tutte le eventuali controversie giudiziarie nelle quali risulti attrice o convenuta Namirial S.p.A. e relative al servizio di CA erogato da Namirial S.p.A. sarà competente esclusivamente il Foro di Ancona, con esclusione di qualsiasi altro foro competente e con esclusione delle ipotesi in cui la legge preveda la competenza del foro del consumatore.

## **12 ACCREDITAMENTI, MARCHI DI FIDUCIA E VERIFICHE DI CONFORMITÀ**

Dal 3 novembre 2010, Namirial S.p.A. è un Certificatore (Certification Service Provider) iscritto nell'elenco pubblico dei certificatori accreditati tenuto dall'Agenzia per l'Italia Digitale (AgID).

Dal 1° luglio 2016, Namirial S.p.A. è un Prestatore di Servizi Fiduciari (Trust Service Provider) di Certificazione e di Validazione Temporale Elettronica ai sensi del Regolamento eIDAS e pertanto iscritto nell'Elenco dei Prestatori di Servizi Fiduciari stabiliti in Italia pubblicato dall'AgID.

Il servizio di CA erogato da Namirial S.p.A. è sottoposto ogni due anni ad una verifica di conformità alle norme ETSI EN 319 411-1 e ETSI EN 319 411-2 da parte di un auditor esterno indipendente, qualificato ed accreditato, come richiesto dal Regolamento eIDAS.