



# PKI Disclosure Statement

## Namirial Certification Authority



Categoria	<b>Manuali Operativi</b>	Codice Documento	<b>NAM-CA-MO</b>	<b>Namirial S.p.A.</b>
Redatto da	<b>Margherita Menghini</b>	Nota di riservatezza	<b>Pubblico</b>	Il Legale Rappresentante
Verificato da	<b>Franco Tafini</b>	Versione	<b>2</b>	<b>Massimiliano Pellegrini</b>
Approvato da	<b>Massimiliano Pellegrini</b>	Data di emissione	<b>28/03/2023</b>	_____



### Namirial S.p.A.

Via Caduti sul Lavoro n. 4, 60019 Senigallia (An) - Italia | Tel. +39 071 63494  
www.namirial.com | amm.namirial@sicurezza postale.it | P.IVA IT02046570426  
C.F. e iscriz. al Reg. Impr. Ancona N. 02046570426 | REA N. AN - 157295  
Codice destinatario T04ZHR3 | Capitale sociale € 8.238.145,00 i.v.



## Indice

Storico delle modifiche.....	3
1. Introduzione .....	5
2. Informazioni di contatto della CA.....	5
3. Tipologie di certificato, procedure di validazione ed utilizzo.....	5
4. Limitazioni.....	7
5. Obblighi del Titolare.....	7
5.1. Coppia di chiavi e utilizzo del Certificato.....	8
6. Obbligo di verifica dello stato del certificato.....	9
7. Limitazioni di responsabilità .....	9
8. Privacy policy .....	9
9. Politiche di rimborso.....	9
10. Licenze e repository TSP, marchi trust e audit.....	9



## Storico delle modifiche

<b>VERSIONE</b>	<b>1.0</b>
Data	26/05/2017
Motivo	Prima emissione del documento
Modifiche	

<b>VERSIONE</b>	<b>1.1</b>
Data	14/06/2018
Motivo	Revisione
Modifiche	Paragrafo 9: inserito adeguamento al Regolamento Europeo 2016/679

<b>VERSIONE</b>	<b>1.2</b>
Data	10/05/2019
Motivo	Revisione complessiva del documento
Modifiche	---

<b>VERSIONE</b>	<b>2</b>
Date	28/03/2023



Reason	Revisione complessiva del documento
Modifiche	Redazione in italiano, revisione complessiva



## 1. Introduzione

Il presente documento costituisce il PKI Disclosure Statement, in conformità a quanto richiesto dallo standard europeo ETSI EN 319 411-1, relativo al servizio di certificazione offerto dal Trust Service Provider Namirial S.p.A.

Di seguito, il servizio di certificazione è indicato anche come "Servizio CA" (Certification Authority).

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" è indicato come "Regolamento eIDAS".

Il presente documento non si pone in sostituzione delle Condizioni Generali del Servizio CA né del Manuale Operativo/Certification Practice Statement (di seguito "Manuale Operativo" pubblicato sul sito web del prestatore di servizi Namirial S.p.A., indicato d'ora in avanti come "il Certificatore").

## 2. Informazioni di contatto della CA

Di seguito si forniscono i recapiti di contatto della CA Namirial:

VIA Caduti Sul Lavoro, 4  
60019 - Senigallia (AN)

Sito web: [https:// http://www.namirial.com](https://http://www.namirial.com)

Mail: [supportoca@namirial.com](mailto:supportoca@namirial.com)

Per ogni richiesta relativa alla documentazione di servizio, incluso il presente PKI Disclosure Statement, si prega di contattare l'indirizzo:[supportoca@namirial.com](mailto:supportoca@namirial.com)

Al fine di richiedere la revoca di un certificato si invita a prendere visione della versione aggiornata del Manuale Operativo presente sul sito del Certificatore.

## 3. Tipologie di certificato, procedure di validazione ed utilizzo

Namirial emette Certificati Qualificati in conformità ai 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;
- ETSI EN 319 412-3 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons;
- ETSI EN 319 412-5 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

I Certificati riportano il valore “no- repudiation” per l'estensione keyUsage. Il campo “Subject” all'interno del certificato elenca le informazioni necessarie all'identificazione del Titolare (persona fisica o giuridica).

Nel caso di Certificato rilasciato a persona fisica, il campo “Subject” contiene almeno:

- countryName;
- givenName and surname;
- commonName;

Nel caso di Certificato rilasciato a persona giuridica, il campo “Subject” contiene almeno:

- countryName;
- organization Name
- organizationIdentifier
- commonName

I Certificati sono emessi secondo le condizioni pubblicate sul sito web del Certificatore.

Tutti i certificati sono firmati con la funzione di hash SHA-256.



I certificati delle CA emittenti di Namirial S.p.A. sono pubblicati sul sito della CA e sul sito dell'Agenzia per l'Italia Digitale (AgID) all'indirizzo [www.agid.gov.it](http://www.agid.gov.it) (si veda l'Elenco dei Trust Service Provider).

Per consentire la validazione dei certificati, la CA mette a disposizione sia la Certificate Revocation List (CRL) sia un servizio di verifica dello stato on-line basato sullo standard OCSP. Gli URL di entrambi i servizi sono inclusi in tutti i certificati, rispettivamente nelle estensioni `CRLDistributionPoints` e `AuthorityInformationAccess`.

## 4. Limitazioni

I Certificati sono emessi per firme elettroniche avanzate e qualificate, nonché per sigilli elettronici.

Le limitazioni all'uso dei certificati possono essere specificate all'interno degli stessi, nell'attributo `UserNotice` dell'estensione `CertificatePolicies`.

Le limitazioni sul valore delle transazioni in cui il certificato può essere utilizzato possono essere specificate all'interno dello stesso nell'estensione `qCStatements`, mediante l'elemento `QcEuLimitValue`.

Tutte le registrazioni relative al ciclo di vita dei certificati, così come tutti i log di audit del servizio di CA, sono conservati da Namirial S.p.A. per 20 anni.

## 5. Obblighi del Titolare

Il Richiedente o Titolare del certificato ha l'obbligo di:



- fornire al Certificatore informazioni complete, accurate e veritiere in fase di registrazione;
- utilizzare le proprie chiavi private solo per gli scopi e con le modalità consentite dal paragrafo successivo;
- adottare misure idonee a prevenire la compromissione e qualsiasi uso non autorizzato delle proprie chiavi private;
- (per i certificati che richiedono l'uso di un dispositivo di firma) se genera autonomamente la propria chiave privata, generarla all'interno di un dispositivo di firma approvato dal Certificatore;
- fino alla data di scadenza del certificato, informare tempestivamente la CA nei seguenti casi:
  - i) il dispositivo di firma viene smarrito, rubato o danneggiato;
  - ii) ha perso il controllo esclusivo della sua chiave privata, ad esempio a causa della compromissione dei dati di attivazione (ad esempio il PIN) del suo dispositivo di firma;
  - iii) alcune informazioni contenute nel suo certificato sono imprecise o non più valide:
- in caso di compromissione della propria chiave privata (ad esempio perché il PIN del proprio dispositivo di firma viene smarrito o divulgato a persone non autorizzate), cessare immediatamente l'utilizzo di tale chiave privata e assicurarsi che non venga più utilizzata.

## 5.1. Coppia di chiavi e utilizzo del Certificato

Il Titolare del Certificato deve salvaguardare la propria chiave privata, facendo attenzione ad evitarne la divulgazione a terzi. Namirial fornirà un apposito contratto di sottoscrizione, che evidenzia gli obblighi del proprietario in merito alla protezione della chiave privata. Le chiavi private devono essere utilizzate solo come specificato nei campi "keyUsage" ed "extendedkeyUsage", come riportato all'interno del Certificato.

Le responsabilità relative all'uso delle chiavi e dei Certificati includono quelle adeguatamente affrontate nell'apposita sezione del Manuale Operativo. I Certificati devono essere usati solo come prescritto dal suddetto Manuale e dalle Condizioni Generali. Qualsiasi uso differente è proibito.



## **6. Obbligo di verifica dello stato del certificato**

Tutti gli utilizzatori ("Relying Parties") devono verificare che i certificati non siano sospesi o revocati. Tale verifica può essere effettuata consultando l'elenco dei certificati revocati (CRL) pubblicato dal Certificatore o interrogando il servizio OCSP fornito dalla CA, agli indirizzi (URL) contenuti nel certificato stesso.

## **7. Limitazioni di responsabilità**

Per le limitazioni di garanzia e di responsabilità, consultare le Condizioni Generali del servizio pubblicate sul sito web del Certificatore.

## **8. Privacy policy**

Namirial è conforme al Regolamento UE n. 679/2016 e alle raccomandazioni e disposizioni del Garante per la protezione dei dati personali italiano.

Per ulteriori informazioni, si faccia riferimento alle Condizioni Generali del servizio disponibili sul sito web del Certificatore.

Tutte le registrazioni relative ai Certificati Qualificati emessi da Namirial S.p.A. (ad esempio, le prove dell'identità dei Richiedenti; le richieste di emissione dei Certificati, l'accettazione delle Condizioni Generali; le richieste di revoca dei certificati; ecc.) sono conservate da Namirial S.p.A. per 20 anni.

## **9. Politiche di rimborso**

Per le politiche di rimborso si faccia riferimento alle Condizioni Generali pubblicate sul sito del Certificatore.

## **10. Licenze e repository TSP, marchi trust e audit**

Dal 3 novembre 2010, Namirial S.p.A. è un Certification Service Provider (Certification Authority) iscritto nel registro pubblico delle CA accreditate mantenuto dall'Agenzia per l'Italia Digitale (AgID).

Dal 1° luglio 2016, Namirial S.p.A. è un Trust Service Provider di servizi di certificazione e marcatura temporale ai sensi del Regolamento eIDAS iscritto nell'elenco italiano dei Trust Service Provider (TSL) pubblicato da AgID.



Il servizio CA di Namirial S.p.A. è soggetto a valutazione di conformità ogni due anni, secondo le norme europee ETSI EN 319 411-1 e ETSI 319 411-2, da parte di un Conformity Assessment Body, qualificato e accreditato, come richiesto dal Regolamento eIDAS.