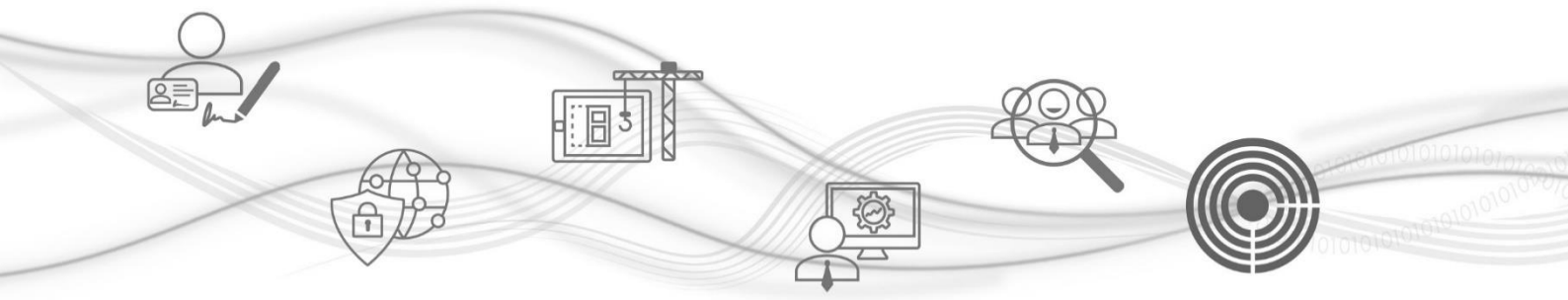
Namirial Notify

Manuale Operativo - Policy & Practice Statement per il Servizio Elettronico di Recapito Certificato Qualificato



Categoria	**Manuale operativo**	Codice Documento	**NAM-MO-QERDS**	**Namirial S.p.A.**
Redatto da	**N.Cardinaletti, F.Marti (Regulatory Compliance)**	Nota di riservatezza	**Documento Pubblico**	Il Legale Rappresentante
Verificato da	**Luigi Castaldo (Responsabile del servizio)**	Versione	**1.1**	**Massimiliano Pellegrini**
Approvato da	**Massimiliano Pellegrini**	Data di emissione	**11/03/2026**	_____

Signed by: PELLEGRINI MASSIMILIANO
Issued by: Namirial CA Firma Qualificata
Signing time: 20-03-2026 08:54:24
IP address: 185.5.246.18

Namirial
Via Caduti sul Lavoro n. 4, 60019 Senigallia (An) - Italia
Tel. +39 071 63494 | www.namirial.com

Indice

Storia delle modifiche

VERSIONE	1.1
Data	11/03/2026
Motivazione	Aggiornamento del documento
Modifiche	Aggiornamento della tabella Definizioni e Acronimi; Aggiunta del paragrafo 2.5.2 e del paragrafo 7.9; Riformulazione del paragrafo 2.6 e del paragrafo 4; Riformulazione e aggiornamento del paragrafo 9

VERSIONE	1.0
Data	14/05/2025
Motivazione	Prima emissione
Modifiche	-

Riferimenti tecnici e normativi

Namirial, nell'erogazione dei suoi servizi, è conforme alle normative e regolamenti europei e nazionali applicabili all'erogazione del servizio. Tutti i regolamenti e le leggi applicabili sono riportati nella seguente tabella.

NORMATIVA	DESCRIZIONE
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
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 e successive modifiche
Regolamento accreditamento	Regolamento recante le modalità con cui i soggetti che intendono avviare la prestazione di servizi fiduciari qualificati presentano all'AgID domanda di qualificazione ai sensi dell'art. 29 del decreto legislativo 7 marzo 2005, n. 82
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR);
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 (eIDAS)
eIDAS 2.0	Regulation (EU) 1183/2024 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework
ETSI 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI 319 521	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers
ETSI 319 522-1	Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture
ETSI 319 522-2	Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic contents
ETSI 319 522-3	Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: Formats

NORMATIVA	DESCRIZIONE
ETSI 319 522-4	Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 3: Capability/requirements bindings

Riferimenti tecnici e normativi

Definizioni ed acronimi

Sono qui riportati i significati di acronimi e di termini specifici, fatti salvi quelli di uso comune. Le definizioni sono derivate principalmente dal Regolamento eIDAS e dagli standard ETSI di riferimento, con prevalenza del primo in caso di definizioni divergenti.

TERMINE O ACRONIMO	SIGNIFICATO
Attestazione qualificata di evento	Un documento informatico avente valore probatorio, finalizzato a certificare il verificarsi di un determinato evento, che consiste in un file in formato PDF, firmato elettronicamente con Sigillo Elettronico Qualificato e dotato di marcatura temporale qualificata. Tale documento è opponibile a terzi.
AgID	Agenzia per Italia Digitale.
Appartenenti all'Organizzazione	Dipendenti e/o associati a favore dei quali l'Organizzazione richiede l'emissione di un Recapito Elettronico Certificato Qualificato.
Autorità per la marcatura temporale [Time-stamping authority]	È il sistema software/hardware, gestito dal QERDS Provider, che eroga il servizio di marcatura temporale.
Autorità di recapito qualificata [Qualified Delivery Authority]	L'Autorità di Recapito Qualificata è la terza parte fiduciaria che fornisce il Servizio elettronico di Recapito Certificato Qualificato (QERDS). Namirial è il Prestatore del Servizio di Recapito Elettronico Certificato Qualificato che agisce come autorità di recapito per i messaggi per i quali la consegna è qualificata ed è responsabile dell'identificazione di mittenti e destinatari.
Certificato digitale, Certificato Qualificato	È un documento elettronico che attesta, con una firma digitale, l'associazione tra una chiave pubblica e l'identità di un soggetto (persona fisica).

TERMINE O ACRONIMO	SIGNIFICATO
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.
Consegna	l'atto di mettere a disposizione e recapitare al destinatario il contenuto a lui destinato, entro i limiti del servizio ERDS.
CNS	Carta Nazionale dei Servizi.
Contenuto della comunicazione	Dati originari prodotti dal mittente che devono essere inviati al destinatario.
Destinatario	Persona fisica a cui è destinato il recapito della comunicazione.
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
ERDS	Electronic Registered Delivery Service. Il servizio elettronico di recapito certificato è un servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate.
ERD application	Sistema costituito da componenti software e/o hardware mediante il quale mittenti e destinatari partecipano allo scambio di dati con fornitori di servizi di recapito elettronico certificato.
LRA	È la persona fisica o giuridica delegata dal QERDS Provider allo svolgimento delle operazioni di identificazione dei destinatari delle comunicazioni qualificate, secondo le modalità individuate e descritte nel presente Manuale. L'ente deve aver preventivamente stipulato accordi di servizio con il QERDS Provider. La LRA può avvalersi di RAO per le operazioni identificazione, registrazione ed emissione.
Marca Temporale qualificata [Qualified Timestamp]	È il risultato della validazione temporale elettronica qualificata conforme al requisito di cui all'art. 44, comma 1, lettera f) del Regolamento UE n. 910/2014 come modificato dal Regolamento UE 2024/1183, che dimostra l'esistenza di un'evidenza informatica in un tempo certo,
Mittente	È la persona fisica o giuridica che procede all'invio della comunicazione qualificata.
Manuale Operativo	È il documento pubblico depositato presso AgID che definisce le procedure applicate dal QERDS Provider nello svolgimento della propria attività.

TERMINE O ACRONIMO	SIGNIFICATO
Organizzazione	È un gruppo organizzato di utenti (es. enti, aziende, società, ordini professionali, Associazioni, ecc.) che hanno stipulato accordi con il QERDS Provider per l'utilizzo di comunicazioni certificate qualificate per i 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]	Numero Identificativo Personale.
Prestatore di servizi fiduciari	Una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato.
Prestatore di servizi fiduciari qualificato	un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato.
PSD2	Payment Services Directive relativa ai servizi di pagamento nel mercato interno.
QERDS	Qualified Electronic Registered Delivery Service. È un servizio elettronico di recapito certificato qualificato che soddisfa i requisiti di cui all'articolo 44 del Regolamento eIDAS.
QERDS Practice statement	Dichiarazione delle pratiche che un prestatore di servizi QERDs impiega nella fornitura dei suoi servizi.
QERDS Provider	Prestatore di servizi fiduciari che fornisce un servizio di recapito elettronico certificato qualificato.
TSP	Trust Service Provider, si veda la definizione Prestatore di servizi fiduciari.

TERMINE O ACRONIMO	SIGNIFICATO
QTSP	Qualified Trust Service Provider, si veda la definizione Prestatore di servizi fiduciari qualificati.
RA	Registration Authority, soggetto che esegue l'identificazione dei destinatari delle comunicazioni elettroniche certificate qualificate applicando le procedure definite dal QERDS Provider.
RAO	È soggetto espressamente delegato da Namirial allo svolgimento, per conto di quest'ultima, delle Operazioni di identificazione e registrazione dei destinatari delle comunicazioni elettroniche certificate qualificate. Tale soggetto deve appartenere ad una LRA.
Referente	È la persona fisica che mantiene i contatti con il QERDS Provider.
RSA	Algoritmo di crittografia asimmetrica, basato su chiavi pubbliche e private.
SERC	Servizio elettronico di recapito certificato, si veda la definizione di ERDS.
SERCQ	Servizio elettronico di recapito certificato qualificato, si veda la definizione di QERDS.

TERMINE O ACRONIMO	SIGNIFICATO
Servizio fiduciario	Un servizio elettronico prestato normalmente dietro remunerazione e consistente in uno qualsiasi degli elementi seguenti: a) il rilascio di certificati di firma elettronica, certificati di sigilli elettronici, certificati di autenticazione di siti web o certificati di prestazione di altri servizi fiduciari; b) la convalida di certificati di firma elettronica, certificati di sigilli elettronici, certificati di autenticazione di siti web o certificati di prestazione di altri servizi fiduciari; c) la creazione di firme elettroniche o sigilli elettronici; d) la convalida di firme elettroniche o sigilli elettronici; e) la conservazione di firme elettroniche, sigilli elettronici, certificati di firme elettroniche o certificati di sigilli elettronici; f) la gestione di dispositivi per la creazione di una firma elettronica a distanza o di dispositivi per la creazione di un sigillo elettronico a distanza; g) il rilascio di attestati elettronici di attributi; h) la convalida di attestati elettronici di attributi; i) la creazione di validazioni temporali elettroniche; j) la convalida di validazioni temporali elettroniche; k) la prestazione di servizi elettronici di recapito certificato; l) la convalida dei dati trasmessi tramite servizi elettronici di recapito certificato e relative prove; m) l'archiviazione elettronica di dati elettronici e di documenti elettronici; n) la registrazione di dati elettronici in un registro elettronico;
Servizio fiduciario qualificato	È un servizio fiduciario che soddisfa i requisiti stabiliti dal Regolamento eIDAS e ne fornisce le relative garanzie in termini di sicurezza e qualità.
SHA-256 [Secure Hash Algorithm]	Algoritmo di crittografia che genera una impronta digitale di 256 bit.
Sigillo	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi

Definizioni e acronimi

Descrizione sintetica di Namirial S.p.A.

Namirial S.p.A., d'ora in poi solo **Namirial**, è l'azienda italiana di **Information Technology** specializzata nella fornitura di **servizi trust**, tra questi: firme digitali, comunicazioni certificate, conservazione a norma, fatturazione elettronica, Digital Transaction Management, servizi di Know Your Customer, onboarding e verifica dell'identità digitale.

Fondata nel 2000 ad Ancona, inizia a operare nel settore informatico offrendo soluzioni su misura per la gestione dei processi di PMI e professionisti, per poi digitalizzare velocemente l'offerta dei propri servizi e il suo ambito di competenza:

Da maggio 2020, Namirial ha portato a termine diverse acquisizioni strategiche nell'ambito dei servizi trust, tra queste:

Nel 2022 è entrata inoltre a far parte del mondo Namirial la società Bit4id, dal 2004 leader nelle tecnologie di identità digitale, Public Key Infrastructure e Digital Transaction Management.

Namirial conta oggi oltre 3 milioni di clienti distribuiti in oltre 85 paesi nel mondo, 30 sedi del gruppo e più di 170 strategic partner. Mantenendo la propria sede legale a Senigallia (AN) e con ulteriori uffici in Italia, Europa, Sud America e resto del mondo, Namirial eroga servizi per Grandi, Medie e Piccole Imprese, Pubblica Amministrazione, Strutture Cooperative ed Ordini Professionali per clienti situati in tutta Europa, Stati Uniti, Sud America, Medio Oriente, Asia e Africa.

All'ottobre 2024 il gruppo Namirial annovera un totale di oltre 900 dipendenti per un fatturato consolidato nell'anno 2023 di oltre 140 milioni di euro.

Grazie al suo impegno e all'estrema diffusione dei propri servizi, nel solo 2023 Namirial ha gestito il seguente numero di transazioni digitali:

- **3,7B** transazioni SaaS;
- **5,4B** documenti archiviati a lungo termine;
- **20,4M** processi digital onboarding;
- **12M** certificati di firma elettronica qualificata;
- **80M** di fatture elettroniche;
- **3M** di utenti Spid;
- **2.5M** di caselle PEC attive.

I numeri del digital trust service e delle soluzioni Namirial hanno avuto inoltre un positivo impatto in termini ambientali, contribuendo al risparmio di:

- **17,764 Tons** di carta;
- **11,796 m3** di rifiuti;
- **1,143,441 m3** d'acqua;
- **43,557 Tons** di emissioni CO2;
- **13,807 Toe** di energia.

Certificazioni

Si riporta di seguito un elenco delle principali qualifiche e certificazioni ottenute da Namirial in ambito nazionale ed europeo. I certificati elencati sono disponibili per consultazione all'indirizzo: https://www.namirial.com/it/company/certificazioni/.

Qualified Trust Service Provider eIDAS

Namirial è QTSP secondo la definizione eIDAS per i servizi:

- Emissione del certificato qualificato per la firma elettronica;
- Emissione del certificato qualificato per il sigillo elettronico;
- Emissione della marca temporale qualificata.

Namirial è inserito nella lista EU Trust Services Dashboard ed è accreditata dal governo italiano come prestatore di servizi fiduciari.

Certif. 910/2014 eIDAS – Prestatori Servizi Fiduciari Qualificati

- Certificato numero: T332238-3
- Rilasciato da: Bureau Veritas

Electronic Registered Delivery – Gestore PEC

Namirial è gestore di servizi accreditati da AgID per la PEC e fornisce il servizio di Sicurezza Postale dal 2007.

Long Term Archiving Provider

Namirial fornisce il servizio di Archiviazione a lungo termine dal 2014, è qualificata dal'Agid e dall'Agenzia per la cybersicurezza.

Il servizio è qualificato SaaS livello QC2 presso ACN e inserito nel Catalogo delle infrastrutture digitali e dei servizi cloud.

Identificazione Elettronica – Identity Provider SPID

Namirial fornisce servizi fiduciari di identificazione digitale SPID ed è accreditata dal governo italiano secondo gli standard europei eIDAS.

Certificazione ETSI EN 319 401

- Certificato numero: IT343163-1
- Rilasciato da: Bureau Veritas

Certificazione ISO 9001:2015

- Certificato numero: IT347262
- Rilasciato da: Bureau Veritas

Certificazione ISO/IEC 27001:2022

- Certificato numero: IT327282
- Rilasciato da: Bureau Veritas

Certificazione ISO/IEC 27017:2015

- Certificato numero: IT327283
- Rilasciato da: Bureau Veritas

Certificazione ISO/IEC 27018:2019

- Certificato numero: IT327284
- Rilasciato da: Bureau Veritas

Certificazione ISO 37001:2016

- Certificato numero: IT331400
- Rilasciato da: Bureau Veritas

Certificazione UNI PdR 125:2022

- Certificato numero: IT319923
- Rilasciato da: Bureau Veritas

AATL

Namirial fa parte dell'Adobe Approved Trust List (AATL)

AWS

Namirial ha ottenuto la certificazione Amazon Web Services

Contatti di Servizio e HelpDesk

Per ricevere informazioni sul Servizio Elettronico di Recapito Certificato Qualificato Namirial S.p.A. sono disponibili i seguenti recapiti:

telefono: (+39) 071 63494

e-mail: **info@namirial.com**

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

Per ricevere informazioni tecniche ed assistenza sul servizio è attivo il seguente recapito:

web: https://servicedesk.namirial.com/hc/it/

Il servizio è attivo nei giorni feriali con i seguenti orari:

dalle 9.00 alle 13.00 e dalle ore 14.00 alle 18.00

1. Introduzione

1.1 Scopo e campo di applicazione

Il presente documento rappresenta il **Manuale Operativo,** nonché la **Policy & Practice Statement del servizio Elettronico di Recapito Certificato Qualificato erogato da Namirial S.p.A ai sensi del Regolamento eIDAS,** ed ha come scopo la descrizione delle regole e delle procedure operative adottate da Namirial per tutte le attività inerenti alla gestione di tale servizio. All'interno del Manuale vengono, inoltre, descritte le procedure atte a garantire un adeguato livello di sicurezza e di affidabilità in conformità con la normativa vigente alla data di emissione, così come le policy e le procedure relative al personale del QTSP deputato.

La documentazione del QERDS Provider Namirial è organizzata secondo i principi degli standard ETSI EN 319 401, EN 319 521 e EN 319 522. (disponibili all'indirizzo http://www.etsi.org). Viene dunque suddivisa nel seguente modo:

a) il documento **NAMIRIAL Trust Services Practice Statement** descrive le procedure generali adottate dal QTSP Namirial nell'erogazione dei servizi qualificati;
b) parti specifiche relative al servizio Elettronico di Recapito Certificato Qualificato che sono descritte nel **Manuale Operativo** del servizio (il presente documento), in conformità alle norme nazionali;

Per casi o soggetti particolari, per i quali si rendessero necessari obblighi/regole e/o procedure operative specifiche, vengono rilasciati ulteriori documenti come "addenda".

1.2 Servizio Elettronico di Recapito Certificato Qualificato Namirial Notify

Namirial Notify è il **Servizio Elettronico di Recapito Certificato Qualificato** ed è la soluzione di Namirial S.p.A. dedicata al servizio oggetto del presente manuale ai sensi rispettivamente degli articoli 43 e 44 del Reg. eIDAS.

L'art. 3, n. 36 del Reg. eIDAS definisce "servizio elettronico di recapito certificato" un servizio che consente la trasmissione di dati fra terzi per via elettronica, fornisce prove relative al trattamento dei dati trasmessi, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o modifiche non autorizzate.

L'art. 3, n.37 definisce il «servizio elettronico di recapito certificato qualificato», un servizio elettronico di recapito certificato che soddisfa i requisiti di cui all'articolo 44.

La piattaforma consente l'invio di comunicazioni elettroniche qualificate che prevedono la consegna di una notifica via e-mail, WhatsApp o SMS contenete un link per accedere al

contenuto da comunicare, in cui viene certificata la ricevuta di apertura e viene consentito il rifiuto della comunicazione, nonché l'accettazione o il rifiuto del contenuto.

Inoltre, sia il mittente sia il destinatario vengono identificati in modo certo e affidabile, in conformità con il regolamento eIDAS. Tale processo è verificato dall'autorità di regolamentazione competente.

La soluzione permette di selezionare il canale per l'invio della notifica e, al tempo stesso, di indicare un canale di invio secondario per garantire che le comunicazioni vengano consegnate ai destinatari anche in caso di indisponibilità del canale di invio primario.

- Il canale di notifica viene scelto in base alla necessità di utilizzo o alla disponibilità del destinatario;
- Il monitoraggio dello stato e dell'esito degli invii avviene attraverso un'unica interfaccia web, dove è possibile consultare gli invii effettuati a un cliente attraverso qualsiasi canale.

Il servizio è disponibile via web o si può integrare in qualsiasi applicativo già esistente, grazie alle idonee API.

Per ogni azione che avviene durante la comunicazione (invio, ricezione, lettura, approvazione o rifiuto dei messaggi e dei contenuti) il mittente ha a disposizione un'attestazione qualificata di evento valida come prova informatica che certifica il verificarsi di ciascun evento.

Namirial eroga il proprio servizio avvalendosi di un fornitore principale, ovvero la propria società controllata Uanataca, la quale gestisce la componente tecnica, strutturale e infrastrutturale del servizio.

Uanataca, società del Gruppo Namirial, opera come prestatore di servizi fiduciari qualificati eIDAS in Europa e America Latina. Uanataca ha incorporato la società Evicertia (anch'essa parte del gruppo Namirial), la quale aveva sviluppato la propria soluzione di Recapito Elettronico Certificato già qualificato ai sensi eIDAS.

Uanataca ha un elevato numero di professionisti qualificati nel settore IT, diritto internazionale, infrastrutture per l'erogazione di servizi fiduciari qualificati, sistemi di rete e sistemi di gestione dei servizi, con certificazioni internazionali, che garantiscono la loro competenza nella gestione dei progetti, nei sistemi di gestione della sicurezza delle informazioni e negli audit dei sistemi informativi.

1.3 Nome e identificativo del documento

Il presente documento denominato "**NAM-MO-QERDS**" è identificato attraverso il livello di revisione e la data di rilascio presente sulla prima pagina. Nel preambolo del documento è inoltre riportato un paragrafo con la storia delle modifiche apportate.

Il QERDS Provider esegue, almeno una volta all'anno, un controllo di conformità del processo di erogazione del servizio e, ove necessario, aggiorna questo documento anche in considerazione dell'evoluzione della normativa e degli standard tecnologici.

Il presente documento e gli eventuali ulteriori documenti rilasciati per soggetti e casi particolari, come *addenda* al Manuale Operativo, sono pubblicati dal QERDS Provider e da AgID e consultabili, 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 del QERDS Provider, nella figura del "Responsabile del servizio", indicato in chiaro nel frontespizio del presente documento alla voce "Verificato da", il quale ne cura la stesura, la validazione, l'aggiornamento.

Le comunicazioni riguardanti il presente documento possono essere inviate all'attenzione del suddetto responsabile contattabile mediante i seguenti recapiti:

e-mail: **info@namirial.com**

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: 1.3.6.1.4.1.36203.8.1.0

1.4 Utilizzo dei servizi fiduciari

Le informazioni sugli utilizzi consentiti, limiti e divieti sono indicate nel presente documento.

1.5 Partecipanti e responsabilità

1.5.1 QERDS Provider

Il QERDS provider è un prestatore di servizi fiduciari che fornisce il servizio elettronico di recapito certificato qualificato.

Namirial è un QERDS provider, che opera in conformità alle disposizioni del Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 sull'identificazione elettronica e sui servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, nonché agli standard tecnici dell'ETSI applicabili ai servizi fiduciari, al fine di facilitare il rispetto dei requisiti legali e il riconoscimento internazionale dei loro servizi.

1.5.2 Registration Authority

L'Autorità di Registrazione, qui di seguito denominata "RA" (Registration Authority), è una persona fisica o giuridica incaricata da Namirial dell'identificazione e verifica dell'identità degli utenti del servizio.

Possono agire come RA di Namirial:

- Namirial stessa;
- entità esterne qualificate e che sulla base di specifici accordi si siano impegnate a svolgere le attività con adeguato impegno e diligenza.

Per agire come RA, sarà necessario formalizzare contrattualmente il rapporto esistente tra Namirial e l'entità autorizzata.

Le funzioni di queste RA, che agiscono per conto di Namirial, includono:

- Verifica dell'identità dell'utente tramite convalida dei dati del firmatario del contratto.
- Verifica delle informazioni fornite dall'utente nella formalizzazione del contratto di servizio.
- Archiviazione di tali informazioni relative all'identificazione e adesione della parte interessata, con riferimento al servizio elettronico di recapito certificato qualificato.
- Fornire agli utenti le informazioni necessarie all'utilizzo del servizio.

1.5.3 Qualified delivery authority

L'Autorità di Recapito Qualificata, qui di seguito denominata "QDA", è la terza parte fiduciaria che fornisce il servizio Elettronico di Recapito Certificato Qualificato (QERDS).

Namirial è il Prestatore del servizio QERDS che agisce come autorità di recapito per i messaggi per i quali la consegna è qualificata.

1.5.4 Delivery service subscribers

I sottoscrittori del servizio QERDS sono gli utenti finali del servizio. I Subscribers, quindi, possono essere:

- Aziende, enti, associazioni od organizzazioni che richiedono a Namirial (direttamente o tramite terzi) di utilizzare il servizio nella loro attività, contesto aziendale o associativo.
- Persone fisiche che richiedono il servizio per sé stesse.

1.5.5 Utenti

Gli utenti sono le persone e le organizzazioni che spediscono e ricevono i messaggi la cui consegna sarà certificata qualificata.

1.5.6 Mittente e Destnatario

Mittenti e destinatari sono i soggetti che interagiscono nell'ambito della comunicazione qualificata. Nell'operatività, tali soggetti agiscono tramite i propri account (credenziali di accesso alla piattaforma, e-mail etc), attraverso cui vengono inviati e ricevuti i messaggi elettronici la cui consegna è certificata qualificata.

1.6 Gestione del Manuale

1.6.1 Organizzazione che gestisce il documento

I dettagli dell'organizzazione sono I seguenti:

- Namirial S.p.A.
- P.IVA: IT02046570426.
- Indirizzo: Via Caduti sul Lavoro n. 4, 60019 Senigallia (An) - Italia.

1.6.2 Contatti dell'organizzazione

I contatti dell'organizzazione Namirial sono I seguenti:

- Web: www.namirial.com.
- E-mail: info@namirial.com
- Telefono: +39 071 63494
- PEC: amm.namirial@sicurezzapostale.it

1.6.3 Procedura di gestione dei documenti

Il sistema documentale e organizzativo di Namirial garantisce, attraverso l'esistenza e l'applicazione delle corrispondenti procedure, il corretto mantenimento di questo documento e delle specifiche del servizio correlate.

1.7 Pubblicazione e archiviazione

1.7.1 Archiviazione

Il repository Namirial è disponibile all'indirizzo:

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

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

1.7.2 Pubblicazione delle informazioni del QERDS Provider

Namirial pubblica nel proprio repository le seguenti informazioni:

- Policy e Practice Statement del servizio (Manuale Operativo);
- Service Disclosure Statement;
- Condizioni generali del servizio;
- Informativa privacy.

1.7.3 Frequenza di pubblicazione

Questo documento e i suoi allegati sono pubblicati al link di cui al precedente paragrafo ogni qualvolta vengano aggiornati. Ad ogni major change, il documento viene sottoposto alla verifica da parte di AgID.

1.7.4 Controllo degli accessi agli archivi pubblici

Questo documento e i suoi allegati sono disponibili pubblicamente ed accessibili solo in lettura.

Namirial non limita l'accesso in lettura alle informazioni sul servizio, ma stabilisce controlli per impedire a persone non autorizzate di aggiungere, modificare o eliminare i record del Repository, per proteggere l'integrità e l'autenticità delle informazioni.

Namirial impiega sistemi affidabili per il Repository, affinché:

- solo le persone autorizzate possano fare annotazioni e modifiche;
- l'autenticità delle informazioni possa essere verificata,
- qualsiasi cambiamento tecnico che influisca sui requisiti di sicurezza possa essere rilevato.

2. Controlli e misure di sicurezza operativa

2.1 Controlli di sicurezza fisica

Namirial ha stabilito controlli di sicurezza fisica e ambientale per proteggere le risorse delle strutture in cui si trovano i sistemi, i sistemi stessi e le apparecchiature utilizzate per le operazioni per la fornitura del servizio.

In particolare, le politiche di sicurezza di Namirial applicabili al servizio stabiliscono requisiti inerenti ai seguenti temi:

- Controlli per l'accesso fisico;
- Protezione contro i disastri naturali;
- Misure di protezione contro gli incendi;
- Guasti nei sistemi di supporto (energia elettrica, telecomunicazioni, ecc.);
- Collasso della struttura;
- Inondazioni;
- Protezione contro il furto;
- Condivisione non autorizzata di apparecchiature, informazioni, supporti e applicazioni relativi ai componenti utilizzati per il servizio.

Queste misure sono applicabili alle strutture da cui viene fornito il servizio, nei loro ambienti di produzione e contingenza, che vengono periodicamente verificati in conformità con le normative applicabili e le politiche interne di Namirial a tale scopo.

Le strutture dispongono di sistemi di manutenzione preventiva e correttiva con assistenza 24 ore su 24, 365 giorni all'anno e con interventi entro 24 ore dalla segnalazione.

Si evidenzia che, in particolare in relazione agli aspetti di sicurezza fisica e logica, Namirial delega le attività al fornitore Uanataca, in quanto responsabile dell'erogazione del servizio.

2.2 Ubicazione delle strutture

La protezione fisica è ottenuta implementando perimetri di sicurezza chiaramente definiti intorno al servizio. Le strutture sono situate in un'area a basso rischio di disastri e permettono un accesso rapido.

Le strutture tramite cui viene erogato il servizio sono ridondate e sono protette da misure che impediscono accessi non autorizzati ai dati, nonché dalla loro divulgazione.

In particolare, i data center utilizzati dal fornitore Uanataca sono ubicati presso le seguenti località:

- Vodafone: Madrid, Spagna.
- Interxion: Madrid, Spagna.

2.3 Accesso fisico

L'accesso fisico alle unità in cui si svolgono le procedure di certificazione è limitato e protetto da una combinazione di misure fisiche e procedurali:

- è limitato al personale espressamente autorizzato, con identificazione al momento dell'accesso e registrazione dello stesso;
- l'accesso alle stanze è effettuato con lettori di carte ID e/o serrature elettroniche, gestiti da un sistema informatico che mantiene un registro automatico di entrata e uscita.
- per accedere al locale in cui si trovano le operazioni crittografiche, è necessaria un'autorizzazione preventiva da parte degli amministratori del servizio di colocation

2.3.1 Elettricità e aria condizionata

Le strutture principali del DC dispongono di apparecchiature di stabilizzazione della potenza e di un sistema di alimentazione duplicato con un generatore.

Le stanze che ospitano le apparecchiature informatiche sono dotate di sistemi di controllo della temperatura con sistemi di climatizzazione.

2.3.2 Esposizione all'acqua

Le strutture si trovano in un'area a basso rischio di alluvioni. Le stanze che ospitano le apparecchiature informatiche sono dotate di un sistema di rilevamento dell'umidità.

2.3.3 Prevenzione e protezione dagli incendi

Le strutture e i beni del DPC principale sono dotati di sistemi automatici di rilevamento e spegnimento degli incendi.

2.3.4 Conservazione dei supporti

Solo il personale autorizzato ha accesso ai supporti di memorizzazione. Le informazioni classificate come di livello più alto sono conservate in modalità sicure, secondo politiche di sicurezza stringenti, in una cassaforte esterna.

2.3.5 Trattamento dei supporti da eliminare

La rimozione dei supporti, sia cartacei che magnetici, viene effettuata attraverso meccanismi che garantiscono l'impossibilità di recuperare le informazioni.

Nel caso dei supporti magnetici, vengono scartati, distrutti fisicamente, o riutilizzati dopo un processo di cancellazione o formattazione permanente. Nel caso della documentazione cartacea, viene distrutta dai tritadocumenti o in appositi cestini per la successiva distruzione.

2.4 Controlli procedurali

Namirial garantisce che i suoi sistemi siano gestiti in sicurezza, per questo ha stabilito e implementato procedure per le funzioni che influenzano la fornitura dei suoi servizi.

Il personale al servizio di Namirial e Uanataca esegue le procedure amministrative e gestionali in conformità con le politiche di sicurezza applicate.

2.4.1 Trusted roles

Il personale è nominato secondo i trusted roles previsti dalla normativa AgID e dallo standard ETSI EN 319-401. Tutto il personale cui è assegnato un ruolo di fiducia è libero da conflitti di interesse che possano essere pregiudizievoli a livello di imparzialità nelle operazioni svolte da ciascuno nell'esercizio delle proprie funzioni.

I trusted roles sono nominati dal management. L' elenco del personale nominato per tali ruoli è inserito in un apposito documento di Struttura organizzativa, che viene mantenuto e rivisto da Namirial, nonché inviato ad ogni aggiornamento all'Organismo di Vigilanza.

2.4.2 Numero delle persone coinvolte nelle attività

In relazione a compiti inerenti a funzioni critiche, Namirial richiede l'assegnazione di un ruolo di fiducia (*trusted role*) ad almeno due soggetti. Ove tale meccanismo sia previsto, esso deve essere applicato, secondo necessità, da due soggetti debitamente autorizzati.

2.4.3 Identificazione ed autenticazione per ciascun ruolo

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

2.5 Controlli sul personale

Tali figure possiedono adeguata esperienza nella definizione, sviluppo e gestione del servizio e ricevono, con cadenza regolare, il 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.

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.

2.5.1 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 e indicati in precedenza.

2.5.2 Check delle esperienze in itinere

La funzione aziendale delle Risorse umane, con il supporto dei Responsabili dei servizi, implementa un processo di monitoraggio continuo delle competenze e delle performance del personale. Il processo prevede l'assegnazione di specifici obiettivi definiti in base al ruolo ricoperto, nonché il monitoraggio periodico dello stato di avanzamento e della percentuale di raggiungimento degli stessi.

A supporto di tale monitoraggio, i Responsabili di servizio organizzano incontri periodici one-to-one con le risorse del proprio team, finalizzati a verificare l'adeguatezza delle competenze rispetto al ruolo assegnato e intervenire tempestivamente in caso di scostamenti o necessità di rafforzamento.

L'analisi continua delle competenze consente, inoltre, di valutare la corretta allocazione delle risorse e di definire programmi di formazione annuale, volti a colmare eventuali gap emersi e a rafforzare la consapevolezza del personale sulle politiche e procedure rilevanti.

Attraverso tali presidi, Namirial assicura che le risorse coinvolte nell'erogazione dei servizi siano costantemente monitorate nel tempo e mantengano un livello di competenza adeguato.

2.5.3 Requisiti di formazione

Il personale Namirial riceve una formazione di base in materia di sicurezza delle informazioni e consapevolezza sulla protezione dei dati fin dalle prime fasi del processo di onboarding aziendale. Tale formazione viene successivamente riproposta con cadenza regolare (almeno annuale) attraverso la somministrazione di video-lezioni, corredate da appositi test di verifica dell'apprendimento.

I corsi obbligatori comprendono, in particolare, i seguenti ambiti tematici:

- GDPR e Data Protection (selezionati dal DPO)
- Security Awareness (selezionati dal CISO)

Le funzioni responsabili della verifica della formazione (Risorse umane, DPO, CISO e Responsabili delle Business unit) dispongono di strumenti di analisi e monitoraggio dello stato di completamento dei percorsi formativi, sopra citati, da parte del personale.

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.

2.5.4 Frequenza di aggiornamento della formazione e requisiti

Il personale è tenuto a mantenere un adeguato livello di competenza professionale mediante la partecipazione a percorsi formativi pertinenti al proprio ambito di attività, al fine di garantire il costante rispetto dei requisiti previsti dal ruolo ricoperto.

È adottato un approccio strutturato alla formazione e all'aggiornamento professionale del personale, con iniziative pianificate almeno su base annuale, in coerenza con i requisiti dei ruoli e delle responsabilità assegnate.

2.5.5 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.

2.5.6 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 amministrative o disciplinari, compresa la cessazione del rapporto di lavoro o di collaborazione e, nei casi più gravi a sanzioni penali.

2.5.7 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.

2.5.8 Documentazione fornita al personale

Al personale, in fase di onboarding, vengono 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.

2.6 Procedure di sicurezza per file di log e registrazione degli eventi

Gli eventi generati dal sistema durante le fasi del processo del servizio elettronico di recapito certificato qualificato producono dei log, che consentono di tracciare le diverse operazioni che si verificano durante i processi automatici e di interazione con l'utente, facilitando la diagnosi di eventuali anomalie e/o incident.

2.6.1 Tipi di log mantenuti

Namirial produce e conserva registrazioni almeno dei seguenti eventi relativi alla sicurezza del sistema:

- Attivazione e spegnimento del sistema;
- Manutenzione e modifiche delle impostazioni di sistema;
- Tentativi di creare, eliminare, impostare password o modificare privilegi;
- Modifiche relative alla gestione degli account con privilegi;
- Tentativi di accesso non autorizzato ai sistemi attraverso la rete;
- Tentativi di accesso non autorizzato al file system;
- Accesso ai log;
- Attivazione e spegnimento dei sistemi utilizzati per l'erogazione dei servizi di fiducia;
- Manutenzione e modifiche delle impostazioni dei sistemi utilizzati per l'erogazione dei servizi di fiducia;
- Registrazioni della distruzione dei supporti, compresi quelli contenenti le chiavi e i dati di attivazione;
- Eventi relativi al ciclo di vita del modulo crittografico, come ricezione, utilizzo o disinstallazione di esso;
- La cerimonia di generazione delle chiavi e i database di gestione delle stesse;
- Registri di accesso fisico;
- Rapporti completi dei tentativi di intrusione fisica nelle infrastrutture che supportano il servizio;
- Rapporti di compromissioni e discrepanze;
- Eventi relativi alla sincronizzazione e ricalibrazione dell'orologio.

In riferimento alla sicurezza del servizio, invece, Namirial produce e conserva registrazioni almeno dei seguenti eventi:

- Eventi relativi alla gestione del ciclo di vita dei certificati utilizzati nelle attestazioni qualificate di evento;
- Accessi al sistema di emissione e gestione dei suddetti certificati;
- Eventi relativi alle attività di timestamping.
- I dati di attivazione o informazioni personali del sottoscrittore;
- I log di identificazione degli utenti coinvolti nell'erogazione del servizio, che vengono registrati nelle attestazioni qualificate di evento

I log includono i seguenti elementi:

- Data e ora dell'evento.
- Numero di serie o sequenza dell'evento, nei registri automatici.
- utente che esegue l'evento.
- Tipo di evento.

2.6.2 Frequenza di elaborazione dei log

Namirial controlla i propri log quando riceve un alert di sistema relativo a un'anomalia.

L'elaborazione dei log di audit consiste nella loro revisione periodica, finalizzata a verificarne l'integrità e ad analizzare le registrazioni presenti, con particolare attenzione

ad alert o anomalie. Eventuali approfondimenti e le azioni conseguenti sono formalmente documentati.

Namirial mantiene un sistema che permette di garantire:

- spazio sufficiente per la memorizzazione dei log;
- che i file di log non siano sovrascritti;
- che le informazioni salvate includano almeno: tipo di evento, data e ora, utente che esegue l'evento e risultato dell'operazione.

I file di log verranno archiviati in file strutturati che possono essere incorporati in un database per esplorazioni successive.

2.6.3 Periodo di conservazione dei file di log

Namirial conserva le informazioni per un periodo massimo di 20 anni, a seconda del tipo di informazioni registrate, o per il periodo stabilito dalla legislazione vigente.

I file di log saranno disponibili per l'ispezione da parte delle Autorità di vigilanza in base alla conformità con la legislazione vigente.

I log relativi all'identificazione degli utenti vengono salvati nel giornale di controllo, che conserva le informazioni salvate per 20 anni, si veda a riguardo il paragrafo 10.5 del presente documento.

2.6.4 Protezione dei fil di log

Namirial protegge, controlli fisici e logici di accesso, i file di log in modo che solo persone debitamente qualificate e autorizzate possano accedervi. I file sono protetti contro la visualizzazione, modifica, cancellazione o qualsiasi altra manipolazione non autorizzata, essendo archiviati in un sistema di strutture sicure.

Esiste una procedura interna che dettaglia le procedure di gestione dei dispositivi che contengono i dati dei log di audit.

2.6.5 Procedure di backup

Namirial dispone di una procedura di backup adeguata, che stabilisce che in caso di perdita o distruzione dei file pertinenti, le copie di backup corrispondenti dei log siano disponibili in breve tempo.

2.6.6 Sistema di archiviazione dei log

Le informazioni relative ai log vengono raccolte internamente e automaticamente dal sistema, dalle comunicazioni di rete e dal software di servizio, oltre ad eventuali dati generati manualmente, che verranno archiviati dal personale debitamente autorizzato.

2.6.7 Notifica dell'evento di audit al causatore dell'evento

Quando il sistema di archiviazione dei log registra un evento, non è necessario inviare una notifica alla persona, organizzazione, dispositivo o applicazione che ha causato l'evento.

2.6.8 Data e ora

I log sono datati con una fonte affidabile tramite NTP. Non è necessario che queste informazioni siano firmate digitalmente.

2.6.9 Procedure per ottenere e verificare le informazioni sui file di log

Namirial ha implementato una procedura che descrive il processo per verificare che le informazioni archiviate siano corrette e accessibili nel tempo, prevedendo verifiche periodiche dell'integrità dei supporti e la migrazione dei dati su nuovi supporti prima che quelli in uso diventino inaffidabili o obsoleti.

2.7 Procedure di gestione degli incidenti

Namirial ha sviluppato politiche di sicurezza e continuità aziendale che consentono la gestione e il recupero dei sistemi in caso di incidenti e compromissione delle sue operazioni.

La procedura apposita per la gestione e la risposta agli incidenti, applicata anche attraverso un sistema di allerta e la generazione di rapporti periodici, è descritta in dettaglio nell'idonea documentazione interna a Namirial.

2.7.1 Corruzione di risorse, applicazioni o dati

Quando si verifica un evento di corruzione delle risorse, applicazioni o dati, vengono seguite le procedure di gestione appropriate in conformità con le politiche di sicurezza e gestione degli incidenti di Namirial, che includono escalation, indagine e risposta all'incidente. Se necessario, vengono attivate le procedure di compromissione delle chiavi o di recupero dai disastri di Namirial.

2.7.2 Continuità aziendale dopo un disastro

Namirial ripristinerà i servizi critici in conformità con il piano di continuità aziendale relativo al servizio, ripristinando il normale funzionamento dei servizi precedenti entro un massimo di 24 ore dal disastro.

3. Cessazione del servizio

Namirial ha redatto un apposito Piano di Cessazione per il servizio QERDS, che verrà implementato qualora si presenti la necessità di terminare il servizio. Il documento contiene le seguenti disposizioni:

- disposizione dei fondi necessari, inclusa l'assicurazione di responsabilità civile, per eseguire l'attività di cessazione;
- comunicazione all'Autorità di vigilanza, a tutti i sottoscrittori del servizio, alle Terze Parti e in generale ogni terza parte con cui si hanno accordi o altro tipo di rapporto con un anticipo minimo di 2 (due) mesi;
- distruzione o dismissione delle chiavi private utilizzate nell'ambito del servizio;
- esecuzione delle attività necessarie per trasferire gli obblighi di manutenzione delle informazioni dei log e delle evidenze per i rispettivi periodi di tempo.

4. Controlli di sicurezza tecnica

Namirial utilizza sistemi e prodotti affidabili, protetti contro qualsiasi alterazione e che garantiscono la sicurezza tecnica e crittografica dei processi di certificazione che supportano.

4.1 Utilizzo della crittografia per la sottoscrizione degli attestati qualificati di evento

Nel servizio di recapito elettronico certificato qualificato, le attestazioni qualificate di evento (prove di accettazione, invio, consegna o mancata consegna) sono generati e protetti mediante meccanismi crittografici che ne garantiscono autenticità, integrità e immodificabilità nel tempo.

A tal fine, ogni attestazione è sottoscritta con sigillo elettronico qualificato del prestatore del servizio fiduciario qualificato, in conformità al Regolamento eIDAS. Il sigillo elettronico qualificato è basato su un certificato qualificato e su una coppia di chiavi crittografiche (chiave privata e chiave pubblica):

- la **chiave privata**, custodita in modo sicuro dal prestatore, è utilizzata per generare la firma o il sigillo;
- la **chiave pubblica**, resa disponibile tramite il certificato qualificato, consente a chiunque di verificare la validità della sottoscrizione.

L'applicazione di un sigillo elettronico qualificato garantisce che:

- l'attestazione qualificata di evento proviene effettivamente dal prestatore del servizio qualificato;
- il contenuto non è stato alterato dopo la sua generazione;
- l'evento certificato è opponibile a terzi nei limiti previsti dalla normativa vigente.

L'uso della crittografia costituisce quindi un elemento tecnico fondamentale per garantire il valore probatorio delle attestazioni qualificate di evento e la loro affidabilità nel tempo.

4.1.1 Generazione e installazione della coppia di chiavi

Le informazioni sulla generazione e installazione della coppia di chiavi di ciascun profilo di certificato o servizi fidati di Namirial sono indicate nella normativa e nella dichiarazione di prassi corrispondenti a ciascun profilo di certificato.

4.1.2 Protezione della chiave privata

4.1.2.1 Norme sui moduli crittografici

Le chiavi private sono gestite tramite HSM certificati Common Criteria EAL4+, che garantiscono adeguati livelli di sicurezza logica e fisica. Le chiavi sono generate direttamente all'interno dei moduli crittografici di produzione e non vengono mai esportate in chiaro. Sono conservate in forma cifrata.

La chiave privata di Namirial viene attivata e/o disattivata eseguendo la procedura di avvio sicuro corrispondente del modulo crittografico.

I moduli crittografici sono sottoposti ai controlli di sicurezza previsti dagli standard adottati dal provider. Gli algoritmi di generazione delle chiavi utilizzati sono riconosciuti e adeguati alla destinazione d'uso delle chiavi stesse.

4.1.2.2 Controllo della chiave privata

La gestione dell'accesso alla chiave privata dei certificati dei servizi fidati viene effettuata secondo i controlli stabiliti dall'HSM dove vengono conservati. Inoltre, i dispositivi crittografici sono fisicamente protetti come definito in questo documento.

4.1.2.3 Backup della chiave privata

Namirial effettua una copia di backup delle chiavi private dei certificati, per rendere possibile il loro recupero in caso di disastro, perdita o deterioramento delle stesse. Sia la generazione del backup che il suo recupero necessitano della partecipazione di almeno due persone.

4.1.2.4 Cifratura delle chiavi a riposo

Tutte le chiavi memorizzate sono cifrate con algoritmi robusti (AES-256), sia nei repository che nei backup.

4.1.3 Compromissione della chiave privata

In caso di sospetto o conoscenza di una compromissione, verranno attivate le procedure di compromissione delle chiavi, in conformità con le politiche di sicurezza, gestione degli incidenti e continuità aziendale, che consentono il recupero dei sistemi critici, se necessario, in un centro dati alternativo.

4.1.4 Metodo di revoca e distruzione delle chiavi private

Per disattivare la chiave privata, verranno seguiti i passaggi descritti nell'apposita documentazione interna a Namirial.

Prima della distruzione della chiave privata, viene revocato il certificato associato. La distruzione avviene secondo procedure documentate e comprende la cancellazione sicura dei dispositivi e dei backup, al fine di impedirne qualsiasi recupero.

4.1.5 Rinnovo delle chiavi

Le chiavi e i certificati utilizzati nei servizi fiduciari di Namirial sono associati solo al sistema che fornisce il servizio stesso. Prima dell'uso di nuove chiavi private, viene effettuata una sostituzione di chiavi, nonché la revoca di quelle attuali.

4.2 Controlli di sicurezza informatica

Namirial utilizza sistemi affidabili per offrire i propri servizi qualificati ed effettua controlli e verifiche al fine di stabilire una gestione adeguata dei propri asset informatici, aderendo al livello di sicurezza richiesto nella gestione dei sistemi di recapito e certificazione.

Per quanto riguarda la sicurezza delle informazioni, Namirial applica i controlli dello schema di certificazione dei sistemi di gestione delle informazioni ISO 27001. Allo stesso modo, il fornitore principale del servizio di recapito qualificato Uanataca applica i controlli del medesimo standard.

La strumentazione utilizzata viene configurata con i profili di sicurezza appropriati, dal personale dei sistemi di Namirial, nei seguenti aspetti:

- configurazione di sicurezza del sistema operativo;
- impostazioni di sicurezza delle applicazioni;
- dimensionamento corretto del sistema;
- configurazione degli utenti e dei permessi;
- configurazione degli eventi di registro;
- piano di backup e recupero;
- requisiti del traffico di rete;
- le funzionalità sopra menzionate vengono svolte mediante una combinazione di sistema operativo, software PKI, protezione fisica e procedure;
- controlli del ciclo di vita tecnico;
- controlli sullo Sviluppo del Sistema.

4.2.1 Controlli sulla gestione dello sviluppo

Le applicazioni vengono sviluppate e implementate da Namirial in conformità con gli standard di sviluppo e controllo delle modifiche.

Le applicazioni dispongono di metodi per verificare l'integrità e l'autenticità, nonché per correggere la versione da utilizzare.

4.2.2 Ulteriori controlli di sicurezza

Namirial richiede misure di sicurezza equivalenti per qualsiasi fornitore esterno coinvolto nell'erogazione dei servizi fiduciari qualificati.

I sistemi operativi utilizzati dal QERDS Provider possiedono un elevato livello di sicurezza e seguono specifiche procedure di hardening. 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 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.

4.2.2.1 Classificazione e gestione delle informazioni e degli asset

Namirial mantiene un inventario degli asset e della documentazione e una procedura per la gestione e l'utilizzo di tali asset.

La politica di sicurezza di Namirial dettaglia le procedure di gestione delle informazioni, dove vengono classificate in base al loro livello di riservatezza.

I documenti sono catalogati su tre livelli: uso pubblico, interno e riservato.

4.2.2.2 Elaborazione e sicurezza dei supporti

Tutti i supporti vengono elaborati in modo sicuro in conformità con i requisiti della classificazione delle informazioni. I supporti contenenti dati sensibili vengono distrutti in modo sicuro se non saranno più necessari.

4.2.2.3 Gestione dell'accesso al sistema

Namirial prevede che l'accesso ai sistemi relativi al servizio elettronico di recapito certificato qualificato sia limitato alle persone autorizzate.

In particolare:

- il controllo dei firewall è implementato con un'alta disponibilità;
- i dati sensibili sono protetti tramite tecniche di crittografia e controlli di accesso con autenticazione forte;
- Namirial dispone di una procedura documentata per la gestione delle registrazioni e cancellazioni degli utenti, nonché di una politica di controllo degli accessi inclusa nella politica di sicurezza;
- sono incluse procedure per garantire che le operazioni siano eseguite in conformità con le politiche dei ruoli;
- il personale di Namirial è vincolato al rispetto delle proprie responsabilità tramite un accordo di riservatezza firmato con l'azienda.

4.2.2.4 Gestione del ciclo di vita dell'hardware crittografico

Namirial assicura che l'hardware crittografico impiegato per la firma dei certificati o per i servizi fiduciari non venga manomesso.

In particolare:

- l'hardware crittografico viene trasportato su supporti specializzati per prevenire qualsiasi manipolazione;
- Namirial registra tutte le informazioni pertinenti sui dispositivi, aggiungendole all'inventario degli asset;
- l'uso dell'hardware crittografico richiede la presenza di personale di fiducia, almeno due dipendenti;
- Namirial esegue test periodici per garantire il corretto funzionamento dei dispositivi;
- la chiave privata dei certificati conservata nell'hardware crittografico viene eliminata una volta che il dispositivo è dismesso.

Le impostazioni del sistema, così come le relative modifiche e aggiornamenti, sono documentate e controllate. Le modifiche o gli aggiornamenti sono autorizzati dal responsabile della sicurezza e debitamente registrati nei registri di lavoro corrispondenti.

4.3 Controlli di sicurezza della rete

Namirial protegge l'accesso fisico ai dispositivi di gestione della rete e implementa un'architettura che ordina il traffico generato, creando sezioni di rete chiaramente definite. Questa divisione avviene tramite l'uso di firewall.

Il trasferimento di informazioni riservate su reti non sicure avviene tramite crittografia utilizzando protocolli TLS o il sistema VPN con doppio fattore di autenticazione.

4.4 Riferimenti temporali

Tutti i dispositivi utilizzati da Namirial sono sincronizzati tramite protocollo NTP (Network Time Protocol) tramite internet (RFC 1305 Network Time Protocol). L'accuratezza del

sistema di riferimento temporale è pari a 1 secondo e la tolleranza, come richiesto dalla normativa vigente, non è mai superiore al minuto secondo rispetto alla scala di tempo UTC (IEN).

Il riferimento temporale utilizzato nelle evidenze prodotte dal servizio QERDS (le attestazioni qualificate di evento), che ne consente la validazione temporale in conformità all'art. 42 del Regolamento eIDAS, garantisce anch'esso uno scarto non superiore a un secondo rispetto alla scala UTC.

5. Profili e revoca dei certificati

Le informazioni sui profili dei certificati emessi o utilizzati da Namirial sono indicate nella corrispondente documentazione del Certificatore Namirial.

6. Audit e conformità

Namirial è un Qualified Trust Service Provider deputato alla fornitura del servizio elettronico di recapito certificato qualificato, soggetto ad attività periodica di valutazione della conformità del servizio da parte di un Organismo di Valutazione della Conformità (CAB), riconosciuto in ambito UE.

Namirial è anche soggetta ad una valutazione di conformità ("sorveglianza") da parte dell'Organismo di Vigilanza AgID

6.1 Frequenza e circostanze della valutazione di conformità

La funzione di audit di Namirial è responsabile degli audit interni sul servizio elettronico di recapito certificato qualificato, che si occupa di verificare che i processi siano conformi ai requisiti di legge, al Regolamento eIDAS nonché agli standard tecnici che regolano l'erogazione del servizio. L'audit interno viene effettuato almeno una volta all'anno.

L'audit di terza parte, allo stesso modo, viene eseguito da un Organismo di Valutazione della Conformità con periodicità almeno annuale.

6.2 Azioni derivanti da non conformità

In caso di non conformità, Namirial adotta le azioni correttive necessarie stabilendo un termine di risoluzione congruo rispetto alla natura e alla criticità della stessa. L'avanzamento delle attività correttive è monitorato fino alla completa chiusura.

Qualora l'Organismo di Vigilanza rilevi eventuali non conformità rispetto ai requisiti previsti dal Regolamento (UE) eIDAS, Namirial provvederà ad adottare tutte le misure correttive necessarie entro i termini indicati dall'Autorità competente.

6.3 Comunicazione dei risultati

I risultati degli audit sono condivisi con Namirial attraverso un rapporto di valutazione della conformità. Il risultato dell'audit interno, invece, viene comunicato alla Direzione e al Responsabile del Servizio, incaricato della fornitura del servizio stesso.

7. Requisiti legali e commerciali

7.1 Tariffe dei servizi fiduciari

Le tariffe del servizio sono pubblicate sullo Shop del QERDS Provider.

Condizioni diverse possono essere negoziate su base personalizzata, a seconda dei volumi richiesti.

7.2 Responsabilità finanziaria

Namirial possiede mezzi finanziari sufficienti per mantenere le sue operazioni e adempiere ai suoi obblighi, oltre che per affrontare il rischio di responsabilità per danni, come stabilito nella ETSI EN 319 401, in relazione alla gestione del piano di cessazione dei servizi e della dismissione.

7.3 Copertura assicurativa

Namirial ha stipulato un'assicurazione di responsabilità civile professionale che comprende i servizi fiduciari qualificati descritti nel presente documento. La polizza è pubblicamente disponibile sul sito web Namirial al seguente link https://www.namirial.com/it/documentazione/

7.4 Riservatezza

7.4.1 Informazioni riservate

Le seguenti informazioni sono mantenute riservate da Namirial:

- le richieste di servizio, così come tutte le altre informazioni personali ottenute per la loro fornitura;
- registrazioni delle transazioni, inclusi i log;
- evidenze di audit interne ed esterne;
- piani di continuità aziendale e di emergenza;
- piani di sicurezza;
- documentazione delle operazioni, archiviazione, monitoraggio e altre simili;
- tutte le altre informazioni identificate come "Riservate."

7.4.2 Divulgazione legale delle informazioni

Namirial non divulgherà informazioni riservate eccetto nei casi previsti dalla legge.

7.5 Protezione dei dati personali

Di seguito vengono descritte le procedure e le modalità operative che Namirial , in qualità di Titolare del trattamento dei dati personali, adotta nello svolgimento della propria attività. Le informazioni personali concernenti i clienti e gli utenti 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.

Namirial garantisce la tutela degli interessati, in ottemperanza al Regolamento europeo 679/2016 in materia di protezione dei dati personali. In particolare, fornisce agli interessati tutte le informazioni necessarie, in relazione al diritto di accesso ai dati personali ed agli usi degli stessi, consentiti dalla legge.

7.5.1 Titolare del trattamento

Il titolare del trattamento dei dati personali è:

- Namirial S.p.A.
- P.IVA: IT02046570426.
- Indirizzo: Via Caduti sul Lavoro n. 4, 60019 Senigallia (An) - Italia.

7.5.2 Dettagli di contatto dell'organizzazione responsabile della protezione dei dati

I dettagli di contatto del Responsabile della Protezione dei Dati sono:

- Website: https://www.namirial.com/it/privacy-policy/
- E-mail: dpo@namirial.com
- PEC: dpo.namirial@sicurezzapostale.it

7.5.3 Finalità del trattamento

I dati personali vengono acquisiti in osservanza alle finalità esplicitate nell'informativa fornita all'utente. L'informativa è anche pubblicata su https://www.namirial.com/it/documentazione/ , nella sezione specifica Informativa Privacy.

Namirial ha il dovere di informare gli utenti che tutti i dati personali forniti vengono trattati per le seguenti finalità:

- Fornitura del servizio: i dati vengono raccolti tramite un contratto appropriato e vengono trattati al fine di erogare i servizi elettronici richiesti dagli utenti, in base a quanto descritto nel presente documento;
    - Certificazione dei processi di comunicazione, tra cui (i) certificazione del contenuto comunicato (che può includere dati personali) mediante meccanismi di verifica dell'integrità crittografica, (ii) certificazione degli

indirizzi di posta elettronica o numeri di telefono del mittente e del destinatario e (iii) certificazione del processo di consegna e/o apertura.
    - Certificazione dei processi di consenso: servizi per la visualizzazione sicura del contenuto (che può includere dati personali) e/o la firma dello stesso mediante il meccanismo di identificazione e autenticazione.
    - Archiviazione delle evidenze: (i) conservazione a lungo termine del contenuto, nonché delle prove relative ai processi di certificazione (attestazione qualificata di evento e cronologia degli eventi) e (ii) fornitura di servizi di ricerca e interrogazione, inclusa la possibilità di ricerca per indirizzo del destinatario o firmatario (quando applicabile).
- Namirial agisce come titolare del trattamento dei dati, il responsabile è l'entità che invia la comunicazione. La finalità è la gestione della comunicazione inviata;
- Supporto per la fornitura del servizio: mantenimento dei dati di contatto per facilitare la gestione delle richieste di assistenza, degli incidenti o reclami relativi alla fornitura del servizio;
- Relazione commerciale: mantenimento dei dati di contatto per facilitare la gestione commerciale, fatturazione, monitoraggio e gestione del servizio.

7.5.4 Altre forme di utilizzo dei dati

I dati personali possono essere usati con finalità diverse rispetto alla fornitura del servizio descritto nel presente manuale e possono essere comunicati a soggetti pubblici, quali forze dell'ordine, autorità pubbliche e autorità giudiziarie, qualora gli stessi soggetti ne facciano richiesta per motivi di ordine pubblico e nel rispetto delle disposizioni di legge per la sicurezza e difesa dello Stato, la prevenzione, l'accertamento e/o la repressione dei reati.

7.5.5 Legittimità del trattamento

Secondo le finalità dichiarate del trattamento, la base giuridica per il trattamento dei dati personali degli utenti è:

- La legittimità del trattamento per la Fornitura di Servizi di Fiducia Elettronici consistente nell'esecuzione del contratto dei servizi richiesti, stipulato con l'utente, il quale fornisce espressamente e inequivocabilmente, attraverso un'azione positiva e prima dell'utilizzo del servizio, l'accettazione delle Condizioni Generali di Servizio;
- La legittimità del trattamento per rispondere alle domande e alle richieste si basa sull'interesse legittimo: una casistica può essere, ad esempio, la risposta al destinatario a una comunicazione risultante dalla fornitura del servizio.

Il consenso al trattamento può essere revocato in qualsiasi momento inviando una richiesta indirizzi specificati nella sezione Dettagli di contatto dell'organizzazione responsabile della protezione dei dati.

L'utente garantisce che i dati forniti siano veritieri, accurati, completi e aggiornati, essendo responsabile per eventuali danni o pregiudizi, diretti o indiretti, che possono essere causati a seguito della violazione di tale obbligo.

7.5.6 Dati trattati e mantenimento

Le categorie di dati trattati da Namirial includono, ma non sono limitate a, dati identificativi (nome, cognome e identità) e informazioni di contatto (indirizzo di posta ordinaria e numero di telefono), e alcune informazioni aggiuntive come l'indirizzo IP, dati del browser e dati di tracciabilità.

I dati personali saranno conservati finché necessari per rispondere a eventuali richieste, fino alla fine del rapporto contrattuale e, successivamente, secondo i termini definiti nel presente documento. In caso di obbligo legale, rimarranno esclusivamente a disposizione di autorità e tribunali.

Maggiori informazioni sono consultabili all'indirizzo https://www.namirial.com/it/privacy-policy/

7.5.7 Trasferimento di dati

I dati personali non saranno divulgati o trasferiti a terzi eccetto per:

- Obbligo legale;
- Interesse legittimo sui dati, come il destinatario delle comunicazioni;
- Per adempiere ad una richiesta giudiziaria o qualsiasi autorità amministrativa competente che lo richieda;
- Cessazione dei servizi.

Non saranno effettuati trasferimenti internazionali al di fuori dell'Unione Europea o dello Spazio Economico Europeo (SEE).

7.5.8 Diritti degli utenti

L'Utente può esercitare tutti i diritti previsti dagli artt. 15-21 del GDPR in qualunque momento e senza limitazioni ingiustificate, contattando il Titolare tramite i riferimenti indicati nella sezione Dettagli di contatto dell'organizzazione responsabile della protezione dei dati.

In particolare, l'Utente può:

- Ottenere conferma che sia in corso un trattamento (Art.15);
- Ottenere la rettifica dei dati inesatti o incompleti (Art. 16);
- Ottenere la cancellazione dei dati senza ingiustificato ritardo (Art. 17);
- Limitare il trattamento solo a parte dei dati personali (Art. 18);

- Ricevere copia dei dati personali in possesso del titolare, in formato d'uso comune e leggibile da dispositivo automatico; ottenere trasferimento senza ostacoli ad un altro Titolare (Art. 20);
- Opporsi in qualsiasi momento al trattamento dei dati personali. (Art. 21);

Con riguardo alle finalità del trattamento che si fondano sul consenso, revocarlo in qualsiasi momento.

7.6 Diritti di proprietà intellettuale

Namirial possiede diritti di proprietà intellettuale sul presente documento.

7.7 Obblighi e Garanzie

7.7.1 Obblighi di Namirial

Namirial è obbligata a:

- operare in conformità con questo documento;
- identificare mittenti e destinatari come descritto in questo documento;
- gestire le comunicazioni certificate qualificate come descritto in questo documento;
- fornire un servizio efficiente di supporto;
- 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 del servizio sia accessibile alle persone con disabilità;
- garantire il trattamento dei dati 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 del servizio.

7.7.2 Registration Authority

La Registration Authority è obbligata a:

- trattare i dati personali dell'interessato con la massima riservatezza e in conformità a quanto previsto dal GDPR;
- svolgere la propria attività di autorità di registrazione in conformità alle indicazioni fornite dal QTSP Namirial, il quale esercita un monitoraggio operativo e sistemico sul relativo operato

7.7.3 Obblighi di terzi nei servizi di supporto

Gli obblighi in carico a soggetti terzi a che operano a supporto del servizio sono i seguenti:

- rispettare e facilitare il rispetto di tutto ciò che è stabilito in questo documento;
- i servizi la cui infrastruttura è distribuita in terzi devono offrire gli stessi livelli di sicurezza e affidabilità dell'infrastruttura utilizzata dal QERDS Provider;
- il terzo deve conoscere e seguire quanto stabilito in questo documento;
- nel caso in cui il terzo debba anche archiviare informazioni e dati, lo farà alle stesse condizioni e scadenze stabilite nel presente documento;
- il terzo deve informare il QERDS Provider di eventuali modifiche che verranno effettuate nell'infrastruttura o nelle procedure per sottoporle a valutazione da parte del Provider stesso. In ogni caso, queste modifiche devono garantire le disposizioni del presente documento.

7.7.4 Obblighi dei sottoscrittori

Gli obblighi dei sottoscrittori rispetto al servizio elettronico di recapito certificato qualificato sono i seguenti:

- rispettare le disposizioni del presente documento, nonché le relative procedure e le politiche di Namirial;
- evitare l'utilizzo dei servizi fiduciari di Namirial per scopi illegali, in contrasto con le disposizioni del presente documento
- sottoscrivere un contratto con Namirial per la fornitura di servizi fiduciari;
- fornire tutte le informazioni richieste, garantendone la veridicità, completezza e correttezza in merito alla propria identità e ai dati comunicati, assumendo la piena responsabilità in caso di dichiarazioni non veritiere e astenendosi dall'utilizzo di documenti personali non veritieri ai sensi dell'art. 76 del DPR445/2000;utilizzare i servizi fiduciari di Namirial in conformità con le procedure e, se necessario, i componenti tecnici forniti da Namirial, come stabilito nel presente documento e nella documentazione di Namirial;
- verificare le firme elettroniche qualificate e le marche temporali qualificate, inclusa la validità dei certificato utilizzati nel servizio di recapito certificato qualificato di Namirial;
- notificare qualsiasi incidente o evento che influisca sui servizi fiduciari di Namirial.

7.7.5 Garanzie

Namirial, nella documentazione che la vincola ai sottoscrittori e alle terze parti, stabilisce e declina le garanzie e le limitazioni di responsabilità applicabili.

Namirial garantisce al sottoscrittore che i servizi fiduciari rispettino tutti i requisiti materiali stabiliti in questo documento, nonché gli standard di riferimento.

7.7.6 Rifiuto di altre garanzie

Namirial rifiuta qualsiasi altra garanzia che non sia legalmente esigibile, salvo quelle contemplate in questo documento e nelle Condizioni Generali di Servizio.

7.7.7 Limiti di responsabilità

Namirial limita la sua responsabilità alla fornitura di servizi fiduciari, che sarà regolata dal contratto appropriato.

Namirial non sarà responsabile per eventuali danni diretti e/o di terze parti derivanti dall'uso improprio dei servizi fiduciari, salvo sia dimostrato che il danno è riconducibile a dolo o negligenza imputabile a Namirial.

7.7.8 Giurisdizione applicabile

Namirial stabilisce nel contratto di sottoscrizione, le procedure di mediazione e risoluzione delle controversie applicabili.

Namirial dichiara nel contratto con il sottoscrittore che la legge applicabile alla fornitura dei servizi è la legge italiana.

7.7.9 Risoluzione delle controversie

Namirial stabilisce nel contratto di sottoscrizione, le procedure di mediazione e risoluzione delle controversie applicabili.

7.8 Utilizzo del servizio elettronico di Recapito Certificato Qualificato Namirial Notify

7.8.1 Utilizzi consentiti

Namirial Notify genera e rilascia delle attestazioni qualificate di evento, ovvero documenti a valore legale che costituiscono prova o dichiarazione idonea all'esibizione in ambito processuale o garanzia di sicurezza in altri casi. Tale evidenza attesta che vi sia stato uno scambio di dati relativi alla comunicazione tra un mittente e un destinatario e che tali dati non siano stati alterati in nessun modo. Il suo utilizzo è riservato alle app e/o ai sistemi dei clienti (persone fisiche o giuridiche) che hanno ingaggiato tale servizio.

7.8.2 Restrizioni e divieti di utilizzo

Namirial Notify non deve essere utilizzato per scopi diversi da quelli specificati in questo documento. Allo stesso modo, il servizio deve essere utilizzato solo in conformità con la legge applicabile.

7.9 Modalità di sospensione e revoca del servizio

Prima di descrivere le modalità operative per sospensione o la revoca del servizio si precisa che:

- la sospensione causa una disattivazione temporanea delle credenziali associate all'utilizzo del servizio;
- la revoca rende inutilizzabili, in maniera irreversibile, le credenziali associate all'utilizzo del servizio.

La sospensione può avvenire in seguito alle seguenti circostanze:

- esecuzione di interventi tecnici finalizzati a garantire o migliorare l'erogazione del servizio stesso;
- presenza di rischi per la sicurezza, violazioni di legge o uso non conforme
- esecuzione di un provvedimento dell'autorità;
- inadempimento degli obblighi previsti nel presente documento, al paragrafo 7.7.

La revoca può avvenire in seguito alle seguenti circostanze:

- cessazione dell'attività del QERDS Provider;
- presenza di rischi per la sicurezza, violazioni di legge o uso non conforme;
- esecuzione di un provvedimento dell'autorità;
- accertamento di abusi o falsificazioni;
- termine del rapporto tra titolare del servizio e QERDS Provider;
- nel caso di persona giuridica, estinzione della stessa;
- inadempimento degli obblighi previsti nel presente documento, al paragrafo 7.7.

Sospensioni e revoche saranno comunicate alle parti interessate a mezzo posta elettronica ordinaria o certificata.

Mittenti e Destinatari hanno la facoltà di richiedere la revoca o sospensione del servizio per un qualunque motivo ritenuti valido dagli stessi ed in qualsiasi momento, attraverso richiesta scritta a mezzo PEC, o tramite gli appositi canali predisposti da Namirial.

8. Identificazione e autenticazione

8.1 Identificazione

Per utilizzare il servizio Namirial Notify, è necessario che sia il mittente sia il destinatario delle comunicazioni abbiano superato il processo di verifica dell'identità e che entrambe le parti abbiano accettato le condizioni di servizio.

Il processo di verifica dell'identità degli utenti si svolge mediante i metodi di identificazione consentiti dal Regolamento eIDAS, a condizione che Namirial li abbia inclusi nel presente documento. In generale, sono consentiti i seguenti:

- presenza fisica presso una delle sedi delle Autorità di Registrazione di Namirial;
- da remoto, utilizzando mezzi di identificazione elettronica per i quali è stata garantita la presenza della persona fisica o di un rappresentante autorizzato della persona giuridica;
- mediante un certificato di firma elettronica qualificata;
- mediante altri metodi di identificazione riconosciuti a livello nazionale che forniscono sicurezza equivalente in termini di affidabilità alla presenza fisica.

È necessario presentare documentazione idonea (documenti identificativi come carta d'identità nazionale, patente di guida, passaporto o contratto firmato elettronicamente con un certificato qualificato) che confermi che la persona è chi dice di essere, o nel caso di una persona giuridica (aziende, enti, società) le informazioni del legale rappresentante (atto pubblico o procura).

I ruoli di mittente e destinatario sono tra loro distinti e prevedono procedure di identificazione specifiche. Pertanto, qualora soggetto già identificato come mittente riceva un messaggio QERDS e assuma il ruolo di destinatario, sarà richiesta una nuova identificazione secondo le modalità previste per tale ruolo, poiché l'identificazione precedentemente effettuata come mittente non sarà ritenuta valida ai fini della ricezione del messaggio in qualità di destinatario.

In egual modo si procede qualora si passi da destinatario a mittente.

Una volta verificata l'identità della persona, verranno attivate le corrispondenti funzionalità di Namirial Notify previste per l'utente.

8.1.1 Identificazione del mittente

Namirial Notify è disponibile per mittenti rappresentati sia da persone fisiche sia giuridiche.

Il servizio, tuttavia, non può essere fornito a:

- minori di diciotto anni;
- persone fisiche o giuridiche la cui identificazione non è possibile o per le quali sussistono dubbi sulla veridicità dei dati comunicati;
- persone fisiche delegate da altra persona fisica.

L'utente mittente può attivare il servizio avviando la procedura di identificazione secondo le modalità descritte a seguire. Una volta conclusa con esito positivo, il servizio risulterà attivo e il mittente riceverà, all'indirizzo mail fornito per l'attivazione del servizio, le credenziali per accedere all'area di invio destinata alla propria organizzazione, per iniziare a utilizzarne le funzionalità. Identificazione de visu

L'identificazione de visu prevede che il soggetto mittente si rechi presso Namirial o una delle Autorità di Registrazione formalmente autorizzate e presenti l'originale dei seguenti documenti:

- per le persone fisiche: il proprio documento di identità in corso di validità (esclusivamente carta d'identità, patente di guida, passaporto) e il codice fiscale (tessera sanitaria o documento analogo che attesti l'attribuzione del codice fiscale);
- per le persone giuridiche: documentazione ufficiale che attesti l'esistenza del soggetto e che contenga la ragione sociale, la forma giuridica, il domicilio, l'identità dei suoi amministratori, statuto e numero di identificazione fiscale. Per il rappresentante legale, è necessario che questo presenti i documenti di cui al punto precedente.

8.1.1.1 Identificazione remota tramite firma elettronica qualificata

L'identificazione remota tramite contratto firmato con un certificato di firma elettronica qualificata consiste nell'apposizione di una firma elettronica qualificata del soggetto che richiede il servizio, per l'accettazione dei termini di contratto e dei termini di servizio.

Oltre al contratto firmato, devono essere fornite le seguenti informazioni:

- **persona fisica**: copia del documento di identità (esclusivamente carta d'identità, patente di guida, passaporto) e del codice fiscale (tessera sanitaria o documento analogo che attesti l'attribuzione del codice fiscale);
- **persona giuridica**: copia del documento di identità e del codice fiscale del legale rappresentante come specificato al punto precedente, nonché il documento ufficiale che attesti l'esistenza del soggetto e che contenga la ragione sociale, la forma giuridica, il domicilio, l'identità dei suoi amministratori, statuto e numero di identificazione fiscale.

8.1.1.2 Dati di registrazione

Per l'utilizzo del servizio, è necessario che siano trasmesse le seguenti informazioni.

Persona fisica:

- Nome e cognome;
- data e luogo di nascita;
- codice fiscale o attributo identificativo analogo;

- Documento d'identità, in corso di validità, di cui sarà conservata una copia;
- Data di rilascio del documento di identità;
- Data di scadenza del documento di identità;
- Nazionalità;
- Indirizzo postale;
- E-mail e numero di cellulare da registrare per l'utilizzo del servizio, come indicati nel contratto;
- Contratto firmato elettronicamente, nel caso in cui la verifica dell'identità sia stata effettuata a distanza tramite un contratto firmato elettronicamente, che verrà conservato.

Persona giuridica:

- Denominazione / ragione sociale;
- Codice fiscale, partita IVA, o analogo attributo;
- Per il rappresentante legale, tutti i dati indicati nella sezione precedente relativa alla persona fisica;
- Documento che attesti i poteri di rappresentanza, di cui verrà conservata una copia;
- Data del documento, come indicato nel documento stesso;
- Data di scadenza della procura, se presente, come indicato nel documento stesso;
- Documentazione ufficiale comprovante la validità della procura;
- E-mail e numero di cellulare da registrare nel servizio, come indicati nel contratto;
- Contratto firmato elettronicamente, nel caso in cui la verifica dell'identità sia stata effettuata a distanza tramite un contratto firmato elettronicamente, che verrà conservato.

Il set di dati sarà acquisito mediante riscontro e verifica del documento di identità del soggetto interessato, nonché sulla base delle informazioni fornite e riportate nel contratto. Verifica delle informazioni

Namirial effettua la verifica generale delle informazioni fornite, al fine di verificarne la veridicità.

Per le persone fisiche, è obbligatoria la verifica di:

- la validità dei documenti di riconoscimento, che devono essere in corso di validità al momento della richiesta di adesione al servizio;
- la validità del certificato di firma elettronica qualificata, se il contratto è firmato elettronicamente, va verificato che il certificato elettronico sia di tipo qualificato e sia:
    - valido;
    - rilasciato da una CA qualificata e attiva;
    - corrispondente al nominativo del richiedente;
    - non contenga espresse limitazione d'uso che ne vietino l'utilizzo.
- se i contratti sono firmati elettronicamente, inoltre, il documento non deve essere stato modificato dopo l'apposizione della firma.

Per le persone giuridiche:

- la validità dei dati inclusi nella documentazione ufficiale fornita
- i poteri di rappresentanza del richiedente devono essere esplicitati nella documentazione ufficiale presentata.

Le operazioni di verifica adottate dal personale Namirial sono oggetto di una apposita procedura interna.

8.1.2 Identificazione del destinatario

Namirial Notify è disponibile per destinatari rappresentati da persone fisiche.

L'identità del destinatario può essere accertata mediante le seguenti modalità ed in conformità con l'art. 24 del Regolamento eIDAS.

Modalità	Soggetti abilitati ad eseguire l'identificazione	Condizioni tecnologiche di autenticazione richieste per l'identificazione
SPID/CIE	Qualified Delivery Authority Registration Authority (RA) Local Registration Authority (LRA)	Utilizzo di un mezzo di identificazione elettronica preesistente (identità digitale SPID o CIE)
Identificazione elettronica nazionale	Qualified Delivery Authority Registration Authority (RA)	Utilizzo di un mezzo di identificazione elettronica nazionale preesistente, notificato dallo Stato Membro

	Local Registration Authority (LRA)	
Processi AML	Titolari destinatari degli obblighi Antiriciclaggio ai sensi delle normative di recepimento della Direttiva 2005/60/CE del Parlamento Europeo e del Consiglio, nonché delle successive disposizioni (Decreto Legislativo n. 231/2007) e regolamentazioni europee recepite in Italia, quindi regolamento (AMLR), direttiva (AMLD), PSD2/3 e PSR.	Processo di autenticazione autorizzato AgID
Identificazione mediante eVideoID	Qualified Delivery Authority Registration Authority (RA)	Processo di identificazione autorizzato AgID

Sintesi delle metodologie di identificazione

A seguito del primo processo di identificazione, il destinatario viene registrato dal sistema. Tale gestione permette di non di ripetere il processo di identificazione per le successive ricezioni di tipo QERDS per il medesimo soggetto, che sarà chiamato alla sola autenticazione per accedere al contenuto della comunicazione.

8.1.2.1 Identificazione mediante strumenti di autenticazione elettronica

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

- notificato dallo Stato Membro ai sensi dell'articolo 9 del Regolamento eIDAS, di livello elevato;
- notificato dallo Stato Membro ai sensi dell'articolo 9 del Regolamento eIDAS, di livello significativo, a patto che fornisca una garanzia equivalente sotto il profilo dell'affidabilità alla presenza fisica;

Nello specifico, relativamente al contesto italiano, vengono riconosciuti come mezzi di identificazione elettronica adatti al riconoscimento:

a) la CIE (Carta di Identità Elettronica) di livello 2 o superiore;
b) Le identità digitali rilasciate nel contesto del sistema SPID di livello 2 o superiore;

Nei casi di cui sopra il destinatario, previo inserimento del PIN, effettua l'autenticazione sul portale del Service Provider o del CIE ID Server (caso CIE). I dati di registrazione sono conservati esclusivamente in formato elettronico.

8.1.2.2 Identificazione mediante processi AML

Con l'entrata in vigore del Regolamento eIDAS2, le modalità di identificazione a distanza assumono un ruolo centrale nei processi fiduciari, richiedendo l'adozione di strumenti e metodologie che garantiscano elevati standard di sicurezza e conformità normativa.

Tra le modalità previste, rientra l'utilizzo di identità digitali notificate ai sensi dell'art. 9 del Regolamento eIDAS2, corrispondenti a un livello di garanzia "elevato". In alternativa, è possibile ricorrere a metodi di identificazione che assicurino un livello di sicurezza equivalente, la cui conformità sia attestata da un organismo di valutazione della conformità, come previsto dall'art. 24, par. 1, lett. c.

A queste si affiancano le procedure di identificazione adottate nel settore finanziario, conformi al regolamento AMLR (Anti Money Laundering Regulation), le quali rappresentano una valida alternativa in quanto soggette a rigorosi controlli da parte delle autorità di vigilanza. Queste ultime sono responsabili della verifica dell'adeguatezza e dell'efficace applicazione delle procedure AML da parte degli istituti finanziari, garantendo così un elevato livello di affidabilità e sicurezza.

I destinatari già identificati da specifici enti (perlopiù banche e istituti finanziari), in conformità alle procedure AML, possono considerarsi identificati anche ai fini della ricezione di un messaggio di tipo QERDS senza ulteriori controlli, a condizione che l'ente stesso sia registrato e operi come Local Registration Authority per conto del QERDS Provider.

In tale contesto, sono richieste misure di mitigazione del rischio di frodi da parte della LRA, tra cui:

- **Acquisizione dei dati identificativi** mediante copia elettronica di un documento d'identità in corso di validità;
- **Verifiche supplementari** sui dati acquisiti, quali:
    - contatto telefonico tramite telefonia mobile (welcome call);
    - verifica dell'indirizzo di posta ordinaria (e-mail) mediante l'invio di un codice OTP;

- invio di comunicazioni cartacee con ricevuta di ritorno;
- bonifico proveniente da un conto intestato all'utente presso un intermediario bancario o finanziario con sede in Italia o in altro Stato membro dell'UE;
- richiesta di documentazione controfirmata;
- accertamenti su residenza, domicilio e attività lavorativa tramite richieste agli uffici competenti o incontri in presenza, anche tramite soggetti terzi incaricati.

Alla luce della vigilanza esercitata dalle autorità competenti e della solidità delle misure previste, tali procedure di identificazione sono da considerarsi pienamente conformi ai requisiti del livello di garanzia "elevato" stabilito dall'art. 8 del Regolamento eIDAS2, risultando pertanto idonee all'impiego nell'ambito dei servizi fiduciari.

8.1.2.3 Identificazione mediante eVideoID

Per questa tipologia di identificazione è richiesta la disponibilità di un dispositivo collegato ad internet (tablet, smartphone) dotato di webcam e sistema audio perfettamente funzionanti.

Il dispositivo deve essere dotato anche di un lettore di prossimità e possono essere utilizzati documenti di identità conformi alle norme ICAO (con MRZ), o comunque avere caratteristiche similari quali ad esempio la patente di guida, che, pur non essendo conforme allo standard ICAO 9303, può essere considerata un documento di riconoscimento valido in quanto rilasciata da un'autorità pubblica competente e dotata di adeguati elementi di sicurezza. Il destinatario, una volta iniziato il processo, viene indirizzato ad una procedura non assistita, in cui una serie di messaggi a video indicano passo per passo le azioni da svolgere. Sono richieste alcune azioni casuali che garantiscano la presenza fisica effettiva del destinatario e una serie di controlli biometrici che assicurano il maggior livello di sicurezza possibile alla soluzione.

Il processo eVideoID prevede delle funzionalità in tema di verifica dell'identità che vengono applicate per rafforzare i controlli sul destinatario, nella consapevolezza che i tentativi di furto d'identità diventano sempre più sofisticati e che il solo rispetto di alcuni requisiti standard potrebbe non essere sufficiente in situazioni ad alto rischio.

Per determinare l'autenticità e la validità del documento di identità i processi di eVideoID eseguono una serie di controlli, tra i quali:

- OCR sul documento;
- verifiche su elementi otticamente variabili (OVD);
- controlli sul checksum MRZ;
- rilevamento di eventuali occlusioni;

- controlli incrociati tra i dati presenti nella zona a lettura ottica (MRZ) e quelli presenti nella zona di ispezione visiva (VIZ).

Completati i controlli sul documento di identità, vengono eseguiti ulteriori controlli sul destinatario per verificare l'associazione al documento e la presenza fisica durante la sessione, tramite i seguenti moduli:

- Face Match;
- Liveness Detection.

Completati tutti i check, viene calcolato un punteggio e, eventualmente, vengono respinti i controlli che non sono portati a termine con una chiara evidenza di successo.

I processi di identificazione eVideoID utilizzati sono sottoposti a verifica e certificazione da parte di un Conformity Assessment Body, a garanzia della robustezza e della qualità delle procedure utilizzate per la verifica delle identità. La soluzione, a seguire, viene sottoposta ad approvazione di AgID.

Tale procedura prevede da parte di Namirial e del CAB sia una verifica degli algoritmi e delle tecniche di identificazione implementate durante il processo che della preparazione del personale impegnato nei controlli di back office.

8.2 Autenticazione del Mittente

A seguito del completamento con esito positivo del processo di identificazione, il mittente riceve via e-mail le credenziali di accesso all'area riservata destinata alla propria organizzazione.

L'autenticazione del mittente viene effettuata utilizzando un'autenticazione a più fattori, tramite l'utilizzo di un nome utente, di una password e di un secondo fattore che consiste in un codice OTP, inviato tramite sms. Il sistema permette al servizio di applicare politiche di password complesse e procedure sicure per il ripristino delle stesse.

8.3 Autenticazione del Destinatario

A seguito del completamento con esito positivo del processo di identificazione, il destinatario procede all'autenticazione.

L'autenticazione del destinatario viene effettuata utilizzando un'autenticazione a più fattori tramite l'inserimento del proprio codice fiscale (o del numero di passaporto in caso di utenti non italiani) e di un secondo fattore che consiste in un codice OTP inviato al telefono mobile o e-mail associati al destinatario stesso.

Per ciascun invio di tipo QERDS, il mittente è tenuto a indicare obbligatoriamente il codice fiscale (o il numero di passaporto in caso di utenti non italiani) del destinatario, nonché il

relativo indirizzo e-mail e numero di telefono cellulare. Il sistema effettua un controllo di univocità dei recapiti indicati, verificando che sia l'indirizzo e-mail sia il numero di telefono non risultino già associati ad altri utenti; qualora le verifiche falliscano, il sistema non permetterà di procedere.

Il destinatario, ricevuto il link di accesso alla comunicazione, è tenuto a inserire il proprio codice fiscale (o numero di passaporto), tale dato deve coincidere con quello previamente indicato dal mittente; in caso di mancata corrispondenza il sistema non permetterà l'autenticazione del destinatario.

In caso di identificazione effettuata tramite identità digitale preesistente SPID o CIE, il sistema, inoltre, verifica che il codice fiscale presente come attributo dell'identità digitale preesistente coincida con quanto inserito dell'utente in fase di autenticazione.

8.4 Verifica dei riferimenti di contatto

Per quanto riguarda i dati di contatto, quali indirizzo di posta elettronica e numerazione cellulare, viene sempre verificato che questi siano operativi mediante l'invio di un codice OTP

In aggiunta, il sistema effettua un'ulteriore verifica volta ad accertare che i suddetti dati di contatto, sia del mittente sia del destinatario, non risultino già associati ad altri utenti; in caso contrario, l'utilizzo del servizio non sarà consentito.

9. Descrizione della piattaforma e del flusso di recapito della comunicazione

9.1 Architettura

Namirial QERDS è una piattaforma digitale che consente agli utenti di gestire servizi relativi alla comunicazione elettronica certificata qualificata, sia tramite un'interfaccia web che tramite API. Inoltre, conferisce la possibilità, sia al mittente che al destinatario, di accettare o meno la comunicazione.

L'applicazione consente agli utenti di monitorare lo stato delle proprie transazioni e raccogliere le prove necessarie durante il processo, che saranno poi certificate, sigillate e archiviate nei sistemi per un periodo designato.

Per quanto riguarda il funzionamento intero dell'applicazione, la piattaforma è composta da diversi moduli che eseguono funzioni differenti e indipendenti.

Il sistema è reso altamente affidabile e disponibile (Available e Reliable) adottando una serie di pratiche che rendono il sistema resiliente agil errori, facilmente scalabile e capace

di fornire continuità operativa anche in caso di guasti. Ciò è possibile introducendo nel sistema vari fattori come:

- ridondanza dei componenti.
- load balancer.
- architettura a microservizi.
- backup su DB di recupero.

Le informazioni di dettaglio relative all'architettura del servizio sono riportate nel corrispondente *Piano della Sicurezza*, documento classificato come interno a Namirial e messo a disposizione esclusivamente nei repository aziendali, o su richesta dell'Autorità di Vigilanza, in conformità alle politiche di sicurezza e ai requisiti di audit applicabili.

9.2 Invio notifiche e modalità apertura dei messaggi

La piattaforma garantisce l'identificazione certa del mittente e del destinatario, in conformità con le specifiche della normativa eIDAS e nel rispetto della normativa nazionale vigente.

L'invio dei messaggi QERDS avviene a seguito dell'identificazione del mittente. L'invio potrà avvenire attraverso l'interfaccia web della piattaforma o attraverso API.

Per ciascuna comunicazione, il mittente potrà gestire le seguenti opzioni:

- Canale di notifica della comunicazione: eMail, SMS o WhatsApp;
- Il metodo di identificazione del destinatario: SPID/CIE, modalità eVideo, AML , le tre opzioni sono mutuamente esclusive;
- Lingua per le comunicazioni;
- Tipologia di eventi per i quali generarele attestazioni qualificate di evento;
- Personalizzazione del template utilizzato per la notifica;
- Permettere accettazione o rifiuto della notifica;
- Permettere l'inserimento di commenti da parte del destinatario;
- Scadenza per la consegna,
- Abilitazione Reminder per l'apertura e relativo intervallo di notifica.

Il mittente può accedere in qualsiasi momento all'archivio delle comunicazioni inviate e a tutte le evidenze generate, sia tramite un pannello di controllo dedicato, che attraverso le API della piattaforma. Anche il destinatario ha la possibilità di consultare, fino alla scadenza del periodo di conservazione previsto (30 giorni), le comunicazioni ricevute e relative evidenze, autenticandosi in modo forte ogni qualvolta necessiti della consultazione. Questo avviene direttamente all'interno del servizio, utilizzando una dashboard dedicata. La consultazione da parte del destinatario è possibile attraverso il link ricevuto sul canale di notifica designato.

Il periodo di conservazione dei messaggi QERDS e delle relative attestazioni qualificate di evento è estendibile fino a un massimo di un anno, resta salvo l'obbligo del QERDS Provider di conservare tale documentazione per un periodo di 20 anni, o per il diverso termine previsto dalla normativa vigente.

9.3 Stato ed esito dell notifiche

Nel processo di recapito elettronico certificato qualificato, vengono distinti stato ed esito delle notifiche di messaggio.

Lo **stato** rappresenta una particolare fase che il processo di comunicazione attraversa, mentre l'**esito** rappresenta il risultato del processo di comunicazione. Inoltre, durante il processo di comunicazione si verificano degli **eventi,** ovvero dei segnali distinti (ad esempio, una conferma di ricezione), che, secondo la logica del processo determinano il passaggio da uno stato all'altro. Quindi, il cambiamento di stato avviene in base ai diversi eventi che si verificano nel contesto del processo di comunicazione, ma non tutti gli eventi generano un cambiamento di stato. Ad esempio, un evento di accettazione della comunicazione potrebbe non generare un cambiamento di stato qualora in precedenza fosse già stato registrato un evento di rifiuto della comunicazione oppure qualora si fosse già registrato un esito finale del processo di comunicazione. Nel caso in cui si verifichino più eventi capaci di determinare una transizione di stato (ad esempio, due eventi ricevuti quasi contemporaneamente), il sistema prevede delle regole che stabiliscono la priorità e l'ordine temporale di questi eventi, in modo tale da garantire che sia soltanto uno di essi a causare la transizione di stato.

L'esito finale di ogni processo di comunicazione genera una attestazione qualificata di recapito riepilogativa. L'utente può, altresì, decidere facoltativamente di richiedere al servizio la produzione di ulteriori attestazioni qualificate di recapito, generate al verificarsi di un determinato evento (ad esempio, invio, consegna, apertura).

9.3.1.1 Stati

Gli stati di un processo di comunicazione di recapito elettronico certificato qualificato sono elencati di seguito:

- **Nuovo (New)**: Il messaggio è stato creato ma non è stato ancora inviato o preso in carico dal sistema;
- **Bozza (Draft)**: Il messaggio non è ancora stato inviato, ma è memorizzato sul server, consentendo quindi eventuali modifiche e/o l'invio successivo;
- **Sottomesso (Submitted)**: Il messaggio è stato ammesso per la certificazione ed è in attesa di elaborazione da parte del sistema;
- **Pronto – in corso (Ready – in progress)**: Il messaggio è stato elaborato localmente e verrà successivamente inviato;

- **Inviato (Sent)**: Il messaggio è stato inviato al server o all'operatore che gestisce il canale di recapito del destinatario; da questo momento, il sistema gestirà il processo di ricezione;
- **Trasferito al canale di invio (Dispatched)**: Il canale di recapito del destinatario ha accettato il messaggio e tenterà di recapitarlo al destinatario stesso;
- **Consegnato (Delivered)**: Il messaggio è stato consegnato al destinatario, ma il contenuto non è ancora stato aperto/letto;
- **Letto (Read)**: Il messaggio è stato aperto/letto dal destinatario finale;
- **Chiuso (Closed)**: Fine del monitoraggio dello stato; non sono previste ulteriori notifiche o risposte, seguirà la conservazione sostitutiva;
- **Fallito (Failed):** Si è verificato un errore che impedisce l'invio del messaggio.

9.3.1.2 Esiti

Gli esiti di un processo di comunicazione di recapito elettronico certificato qualificato sono elencati di seguito:

- **Non definito (None)**: Non si è ancora verificato un esito per il processo di comunicazione;
- **Certificato (Certified)**: Il messaggio è stato preso in carico e il suo contenuto è stato certificato, ma non è stato consegnato;
- **Inviato (Sent)**: Il messaggio è stato inviato al destinatario della comunicazione (ma non sono stati ricevuti ulteriori eventi o notifiche);
- **Consegnato (Delivered)**: Il messaggio è stato consegnato al canale di ricezione del destinatario (confermato tramite risposta automatizzata del server di destinazione o altro evento tecnico che permette di dedurre questo esito);
- **Accettato (Accepted)**: Il messaggio e il suo contenuto sono stati esplicitamente accettati dal destinatario;
- **Letto (Read)**: Il messaggio è stato letto/aperto dal destinatario ed è quindi certificato nel sistema;
- **Rifiutato (Rejected)**: Il messaggio e il suo contenuto sono stati esplicitamente rifiutati dal destinatario;
- **Fallito (Failed)**: Si è verificato un errore che rende impossibile l'invio del messaggio;
- **Annullato (Cancelled)**: Il mittente ha annullato l'invio prima che il destinatario potesse accedervi.

9.4 Eventi e Attestazioni qualificate di evento

Namirial Notify, tramite la combinazione di eventi e stati, permette di **verificare in tempo reale l'esito delle comunicazioni**. Gli esiti delle attività potranno essere utilizzati per eventuali integrazioni con sistemi e processi di gestione del rollback, consentendo il ripristino o la rielaborazione delle operazioni in caso di necessità. Inoltre, tali esiti potranno essere impiegati per l'instradamento verso servizi alternativi di stampa, imbustamento e postalizzazione, garantendo continuità operativa e flessibilità nell'erogazione del servizio.

L' **attestazione qualificata di evento** è un documento avente valore probatorio, idoneo a certificare l'invio, la ricezione e l'integrità dei dati, in conformità a quanto previsto dagli articoli 43 e 44 del Regolamento eIDAS, ed è opponibile a terzi.L'attestazione qualificata di vento consiste in un documento in formato PDF, firmato elettronicamente con sigillo elettronico qualificato, cui viene apposta una marca temporale qualificata. Si tratta di un'evidenza che raccoglie tutte le informazioni e certificazioni che si verificano dal momento in cui il mittente invia una comunicazione fino alla sua ricezione, accettazione o rifiuto da parte del destinatario.

9.4.1 Tipologie di eventi e corrispondenza nelle attestazioni qualificate di evento

Nel contesto del servizio elettronico di recapito certificato qualificato, disciplinato dallo standard ETSI EN 319 522, ogni evento rilevante che si verifica nel processo di comunicazione genera un'attestazione qualificata di evento, ossia una certificazione qualificata dell'evento stesso, prodotta quale evidenza opponibile a terzi.

Di seguito si riporta l'elenco delle tipologie di evento obbligatorie e delle corrispondenti attestazioni qualificate di evento previste dal servizio:

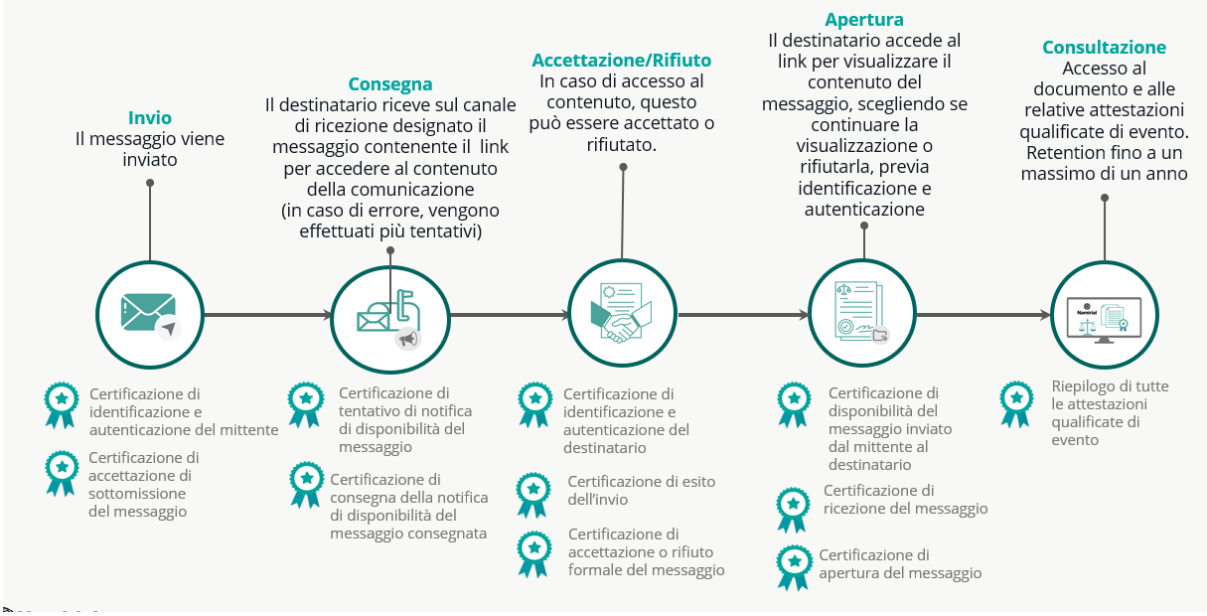
Tipologia evento	Descrizione	Attestazione qualificata di evento corrispondente
Accettazione di sottomissione del messaggio **(Submission acceptance)**	Il messaggio originale è stato correttamente sottomesso dal mittente. L' evento attesta l'intenzione del mittente di inviare un determinato messaggio, l'indirizzo del destinatario e del mittente, l'origine e l'integrità del contenuto, nonché l'orario del tentativo	**Certificazione di sottomissione** Attesta che il mittente, opportunamente identificato e autenticato, ha sottomesso con successo un messaggio al QERDS Provider, che lo ha accettato con la finalità di tentare la consegna al destinatario previsto.

	di comunicazione del messaggio.	
Rifiuto della sottomissione del messaggio **(Submission failed)**	Il messaggio originale è stato correttamente sottomesso dal mittente, ma non è stato accettato dal QERDS Provider.	**Certificazione di sottomissione fallita** Attesta che il mittente, opportunamente identificato e autenticato, ha sottomesso con successo un messaggio al QERDS Provider, ma quest'ultimo ha rifiutato di tentare la consegna al destinatario previsto.
Tentativo di notifica per l'accettazione del messaggio **(Notification for acceptance)**	Il sistema ha tentato di notificare al destinatario la disponibilità di un messaggio per richiederne l'accettazione.	**Certificazione di tentativo di notifica** Attesta che è stato tentato l'invio al destinatario di una notifica per richiedere l'accettazione del messaggio.
Mancata notifica per l'accettazione del messaggio **(Notification for acceptance failure)**	Il sistema non ha potuto notificare al destinatario la disponibilità di un messaggio da accettare.	**Certificazione di notifica fallita** Attesta che non è stato possibile inviare al destinatario la notifica per richiedere l'accettazione del messaggio, dopo un certo numero di tentativi o al termine del time-out stabilito dalle policy applicabili.
Notifica consegnata **(Notification delivered)**	Il sistema ha notificato con successo al destinatario la disponibilità di un messaggio da accettare.	**Certificazione di consegna della notifica** Attesta la consegna avvenuta con successo al destinatario di una notifica di richiesta di accettazione del messaggio
Accettazione del messaggio **(Consignment acceptance**)	Il destinatario ha compiuto l'azione esplicita di accettazione del messaggio, selezionando la casella "Accetta" e cliccando sul pulsante "Continua", posizionata accanto alla visualizzazione del contenuto.	**Certificazione di accettazione formale** Attesta che il destinatario, previa corretta identificazione e autenticazione, ha accettato il messaggio da parte del mittente.
Rifiuto del messaggio **(Consignment rejection)**	Il destinatario ha compiuto l'azione esplicita di rifiuto del messaggio, selezionando la casella "Rifiuta", posizionata	**Certificazione di rifiuto formale** Attesta che il destinatario, previa corretta identificazione e autenticazione, ha rifiutato il messaggio da parte del mittente.

	accanto alla visualizzazione del contenuto.	
Scadenza dei termini per l'accettazione o il rifiuto **(Acceptance rejection expiry)**	Il sistema ha inviato una notifica al destinatario, ma il destinatario non ha reagito alla notifica né con accettazione né con rifiuto.	**Certificazione di scadenza del termine di accettazione/rifiuto** Attesta che il destinatario non ha reagito alla richiesta di accettare o rifiutare il messaggio entro un periodo di tempo definito. Il periodo di tempo è fissato da norme legislative o contrattuali, definito previamente dal mittente, o determinato dalla policy del QERDS Provider.
Disponibilità del messaggio **(Content consignment)**	Il sistema rende disponibile il messaggio del mittente per il destinatario.	**Certificazione di disponibilità del messaggio** Attesta la disponibilità del messaggio inviato dal mittente per il destinatario, previa corretta identificazione e autenticazione.
Mancata disponibilità del messaggio **(Content consignment failure)**	Il sistema non ha potuto rendere disponibile il messaggio per il destinatario, entro un determinato periodo di tempo a causa di errori tecnici e/o altri motivi.	**Certificazione di mancata disponibilità del messaggio** Attesta la mancata disponibilità del messaggio per il destinatario dopo un certo numero di tentativi o al termine del time-out stabilito dalle policy applicabili.
Notifica di disponibilità del messaggio **(Consignment notification)**	Il destinatario riceve una notifica relativa alla disponibilità del messaggio.	**Certificazione di ricezione** Attesta che è stata inviata al destinatario una notifica relativa alla disponibilità del messaggio, L'attestazione certifica l'invio della notifica, ma non garantisce che questa sia stata effettivamente ricevuta dal destinatario.
Mancata notifica di disponibilità del messaggio **(Consignment notification failure)**	Non è stato possibile notificare al destinatario la disponibilità del messaggio.	**Certificazione di mancata ricezione** Attesta che non è stato possibile notificare al destinatario la disponibilità del messaggio dopo un certo numero di tentativi o al termine del timeout stabilito dalle policy applicabili.

Tracciamento di accesso alla notifica **(Notification access tracking)**	Il sistema ha inviato al destinatario una notifica che è stata effettivamente visualizzata o aperta dal destinatario stesso.	**Certificazione di esito dell'invio** Attesta che una notifica è stata di fatto inviata al destinatario ed è stata aperta dal destinatario stesso.
Tracciamento di apertura del messaggio **(Content access traking)**	Il messaggio inviato dal mittente al destinatario è stato effettivamente aperto dal destinatario stesso.	**Certificazione di apertura** Attesta che il messaggio inviato al destinatario è stato aperto dal destinatario stesso, correttamente identificato e autenticato.
Consegna del messaggio **(Content handover)**	Il messaggio ha lasciato la piattaforma del mittente e ha raggiunto il destinatario tramite il canale di recapito prescelto (via e-mail, sms, messaggio WhatsApp). Il destinatario non ha ancora cliccato sul link per accedere al messaggio.	**Certificazione di disponibilità del messaggio** Attesta che il messaggio inviato dal mittente è stato consegnato al canale di ricezione del destinatario a seguito della corretta autenticazione.
Fallimento della consegna del messaggio **(Content handover failure)**	Il messaggio ha lasciato la piattaforma del mittente e ha raggiunto il destinatario tramite il canale di recapito prescelto (via e-mail, sms, messaggio WhatsApp). Il destinatario non ha ancora cliccato sul link per accedere al messaggio.	**Certificazione di mancata disponibilità del messaggio** Attesta che il messaggio inviato dal mittente non stato consegnato al canale di ricezione del destinatario entro un periodo prestabilito a causa di errori tecnici e/o altri motivi.

A titolo di esempio, la figura seguente illustra il flusso di trasmissione della comunicazione, con l'indicazione delle fasi del processo e dei relativi eventi che danno luogo alla generazione delle attestazioni qualificate di evento.



Flusso di recapito elettronico certificato qualificato

9.4.2 Campi di una attestazione qualificata di evento

Nella piattaforma QERDS Namirial, tutte le attestazioni qualificate di evento comprendono diverse sezioni fondamentali per garantire l'autenticità, la validità legale del documento e la certificazione della comunicazione.

La **prima pagina** è dedicata all'identificazione del messaggio e dei suoi elementi. Al suo interno, la sezione relativa all'**identificazione dell'evidenza** fornisce informazioni sul messaggio, tra cui un codice alfanumerico che distingue il documento all'interno del sistema (ad esempio, *b70c6811-532c-4eb3-bebc-e47d5d2d3132*), la data di ammissione, ovvero il momento in cui la notifica è stata accettata nel sistema e la tipologia di evidenza, incluso il canale di notifica utilizzato.

Segue la sezione relativa ai **dettagli del mittente**, che identifica chi è l'utente della piattaforma che ha inviato il messaggio e ne specifica l'indirizzo di posta elettronica. Viene inclusa anche l'evidenza di identificazione, attraverso uno degli strumenti supportati (es. De-Visu, SPID, CIE) e Codice Fiscale o P.IVA del mittente.

Analogamente, quella relativa ai **dettagli del destinatario** riporta il nome della persona o dell'azienda che riceve la notifica di messaggio, il suo indirizzo e-mail e, se necessario, le informazioni relative ai destinatari in copia (CC). Viene inclusa anche l'evidenza di identificazione, attraverso uno degli strumenti supportati (es. De-Visu, SPID, CIE) e Codice Fiscale o P.IVA del destinatario.

La sezione relativa ai **dettagli del contenuto** include una breve descrizione dell'oggetto del messaggio, la sua dimensione in byte e il numero di eventuali allegati. Inoltre, per garantire la sicurezza e l'integrità del contenuto, viene generato un codice di

autenticazione del messaggio, che consiste in un hash crittografico calcolato con l'algoritmo SHA-256.

Un'altra sezione essenziale è quella relativa ai **dettagli dell'attore dell'evento**, ovvero chi ha generato l'evento, il metodo di autenticazione utilizzato per accedere alla piattaforma, l'identificativo (nel caso del mittente, la sua e-mail) e l'indirizzo IP dell'attore, le informazioni di geolocalizzazione, il sistema operativo, e, infine, l'ID, la lingua impostata e i dettagli dell'user agent del browser utilizzato.

Per garantire la validità legale del documento anche in formato cartaceo, l'attestazione qualificata di evento include una sezione contenente un **codice QR** o un *data matrix*, che includono i dati elettronici necessari per verificarne l'autenticità.

Infine, ogni *attestazione qualificata di evento* è dotata di una sezione contenente un **identificativo univoco e permanente**, che consente solo al mittente e al destinatario di accedere al documento. Questo identificativo è generato in conformità con gli standard IETF RFC 1738, 2396, 4122 e lo standard ISO/IEC 9824-8:2005, garantendo la massima sicurezza. L'identificativo è riportato su ogni pagina del documento e non può essere dedotto mediante tecniche statistiche o attacchi *brute-force* sulla rete.

Nel caso in cui siano presenti allegati, la **seconda pagina** conterrà informazioni dettagliate su ciascun file allegato, inclusi il nome, la dimensione e il riepilogo crittografico (hash).

A partire dalla **terza pagina**, e nelle eventuali pagine successive, verrà incluso il contenuto degli eventi da certificare mediante il servizio.

Se, invece, non sono presenti allegati, la seconda pagina, e le eventuali pagine successive, saranno dedicate interamente alla certificazione del contenuto, elencando cronologicamente e in maniera dettagliata gli eventi del processo di comunicazione elettronica certificata qualificata, garantendo in ogni caso la validità legale del documento.

EVENTS SUMMARY			
DATE (UTC)	TYPE	DESCRIPTION	TRACEABILITY

Attestazione qualificata di evento: campi degli eventi valorizzati

9.4.3 Garanzie di integrità

Come indicato nell'articolo 3.n.36 del regolamento eIDAS, il servizio elettronico di recapito elettronico certificato è "un servizio che consente di trasmettere dati tra terze parti per via elettronica e fornisce prove relative alla gestione dei dati trasmessi, inclusa la prova dell'invio e della ricezione dei dati, e che **protegge i dati trasmessi contro i rischi di perdita, furto, deterioramento o alterazione non autorizzata**". Per tale

ragione, dunque, il servizio di recapito elettronico certificato qualificato Namirial prevede la raccolta di evidenze che assicurano le comunicazioni inviate dal mittente vengano consegnate al destinatario con garanzia di integrità e di veridicità dell'evidenza stessa.

Il responsabile di garantire l'integrità e la veridicità è il fornitore stesso del QERDS, che utilizza – a tale scopo – una serie di processi crittografici, come l'applicazione di firme elettroniche e marche temporali qualificate. Tali servizi sono forniti da Prestatori di Servizi di Fiducia qualificati, in conformità con quanto previsto dal regolamento eIDAS (nello specifico, si tratta di servizi forniti dalla stessa Namirial e dal fornitore Uanataca come back-up).

Ogni attestazione qualificata di evento è dotata, quindi, di una firma elettronica qualificata e di una marca temporale qualificata, al fine di garantire l'integrità del documento e prevenire qualsiasi modifica successiva. Durante la generazione della marca temporale qualificata il server della TSA utilizza la data e l'ora dall'orologio del sistema, mantenuto allineato con l'ora UTC (Tempo Universale Coordinato).

Il mittente avrà accesso a tutte le sue attestazioni qualificate di evento tramite la propria area di invio, per un periodo di conservazione standard di un anno, con possibilità di richiesta di estensione temporale di consultazione. Il destinatario, allo stesso modo, avrà accesso alle attestazioni qualificate di evento per un periodo standard di trenta giorni, o per un anno, attraverso il servizio di supporto o tramite le informazioni fornite dal mittente. Una volta trascorso il periodo di conservazione stipulato, nessuna delle parti avrà accesso alle attestazioni qualificate di evento, fermo restando che Namirial provvederà in ogni caso alla conservazione offline per 20 anni.

In caso di compromissione dell'integrità delle attestazioni qualificate di eventoo di qualsiasi incidente relativo all'integrità del contenuto durante il processo di recapito, il servizio di supporto di informerà le parti interessate.

9.5 Erogazione del servizio

La piattaforma è disponibile tramite interfaccia web e tramite integrazione API.

L'accesso ai servizi è sicuro e personalizzato per ogni cliente, tramite protocollo HTTPS e comunicazione cifrata TLS 1.2 o superiore. Durante la registrazione, vengono forniti token di accesso che garantiscono l'utilizzo protetto delle API.

Inoltre, Namirial offre un insieme di servizi REST che coprono tutte le operazioni della piattaforma Le URL per l'integrazione sono fornite sia per l'ambiente di produzione che quello di test.

Gli end-point sono progettati per garantire la protezione delle credenziali utente, evitando la loro esposizione. Le credenziali devono essere gestite esclusivamente in

ambienti sicuri e controllati, al fine di ridurre al minimo i rischi di accesso non autorizzato o vulnerabilità nei sistemi di autenticazione.

L'autenticazione è performata con **un'autenticazione a due fattori**, con nome utente e password e con un certificato client.

Anche la configurazione tramite API dà la possibilità di impostare vari dettagli, come il mittente, i destinatari (inclusi i destinatari in copia) compresa la possibilità di aggiungere allegati o personalizzare l'aspetto del messaggio, ad esempio includendo loghi certificati. Inoltre, è possibile scegliere il livello di tracciabilità e certificazione del messaggio, che può essere impostato su due livelli:

- **Standard**: genera una *attesatzione qualificata di evento* quando il tracciamento dello stato del messaggio è completato.
- **Avanzato**: prevede la generazione di più *attestazioni qualificate di evento*, uno per ciascun evento, come la ricezione o la lettura del messaggio, con l'aggiunta di una marca temporale qualificata per ogni evento.

9.5.1 Tracciamento avanzato dei messaggi tramite API

Un'ulteriore funzionalità accessibile tramite API consente di ottenere informazioni sullo stato del messaggio mediante **notifiche push**. Tali notifiche informano in tempo reale il mittente riguardo eventi significativi relativi al messaggio, come la ricezione o l'apertura del messaggio da parte del destinatario.

Un'ulteriore funzionalità, accessibile tramite le API, permette all'utente mittente di poter inviare **query** al sistema, per poter ottenere informazioni in tempo reale sullo stato del messaggio. Le informazioni di maggior interesse che si possono ottenere tramite notifiche push o query sono:

- **Ready**: Il messaggio è stato elaborato localmente e sarà inviato successivamente.
- **Sent**: Il messaggio è stato inviato al server o al gestore del dispositivo del destinatario.
- **Dispatched**: Il servizio di messaggistica che gestisce il destinatario ha accettato il messaggio e tenterà di inviarlo al destinatario finale.
- **Delivered**: Il messaggio è stato consegnato al destinatario finale, ma il contenuto non è stato ancora aperto o letto.
- **Read**: Il messaggio è stato aperto o letto dal destinatario finale.
- **Failed**: Il messaggio non è stato consegnato al destinatario.
- **Replied**: Il destinatario ha risposto, accettando o rifiutando il messaggio.

- **Closed**: Il tracciamento del messaggio è terminato, e non sono previste ulteriori notifiche o risposte, seguito dal deposito notarile del documento.

10. Giornale di controllo

10.1 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.

10.2 Frequenza di salvataggio del giornale di controllo

Tutti gli eventi vengono salvati con data e ora di sistema dell'evento, la frequenza di salvataggio del giornale di controllo è giornaliera. L'ora esatta di tutti gli eventi significativi viene registrata ed èsincronizzata con UTC almeno una volta al giorno.

10.3 Conservazione delle registrazioni del giornale di controllo

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.

L'integrita' del giornale di controllo e' verificata con frequenza almeno mensile.

10.4 Backup del giornale di controllo

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

10.5 Tipi di eventi memorizzati

Per il servizio oggetto del presente documento, vengono registrati almeno i seguenti eventi:

- gli eventi relativi alla gestione del ciclo di vita dei certificati utilizzati nelle attestazioni qualificate di evento;
- gli accessi al sistema di emissione e gestione dei suddetti certificati;
- gli eventi relativi alle attività di timestamping.
- i log di identificazione degli utenti coinvolti nell'erogazione del servizio, che vengono registrati nelle attestazioni qualificate di evento