

# Manuale Operativo

# PosteNotifica

MAN\_1229\_GR Ver.3.0 Manuale Operativo PosteNotifica

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

## Cronologia delle Versioni

N. Versione	Data di Approvazione	Redattore	Approvatore	Paragrafi modificati	Motivazioni dell'aggiornamento
1.0	30/04/2025	Responsabile delle verifiche e delle ispezioni (auditing)	Responsabile QTSP		Prima stesura
2.0	30/05/2025	Responsabile delle verifiche e delle ispezioni (auditing)	Responsabile QTSP	1.2.1: Aggiunto OID 3.2.1: Dettagliate le modalità di identificazione 9.5: Inserita descrizione del processo di assistenza clienti	Revisione
3.0	09/06/2025	Responsabile delle verifiche e delle ispezioni (auditing)	Responsabile QTSP	3.5.1: Aggiornamento paragrafo	Revisione

## Sommario

1.	INTRODUZIONE.....	5
1.1.	Quadro generale.....	5
1.2.	Identificazione del documento.....	6
1.2.1.	Nome e identificativo del documento.....	6
1.2.2.	Scopo e campo di applicazione del documento.....	6
1.2.3.	Riferimenti normativi e tecnici.....	7
1.2.3.1.	Riferimenti normativi e tecnici.....	7
1.2.3.2.	Standard di riferimento procedurali.....	7
1.2.3.3.	Standard di riferimento di sicurezza.....	8
1.2.4.	Definizioni.....	8
1.2.5.	Acronimi e abbreviazioni.....	11
1.3.	Manuale Operativo.....	12
1.3.1.	Periodo e meccanismo di notifica.....	12
1.3.2.	Soggetti responsabili dell'approvazione del Manuale Operativo.....	12

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
1.3.3.	Procedure di approvazione .....		12
1.3.4.	Revisione del Manuale Operativo .....		12
2.	<b>RUOLI DEL SERVIZIO POSTENOTIFICA</b> .....		13
2.1.	Fornitore del servizio PosteNotifica .....		13
2.2.	Intermediario autorizzato .....		13
2.3.	Cliente .....		13
2.4.	Titolare .....		13
2.5.	Responsabile .....		13
2.6.	Utente-Admin e Utente-Sender .....		14
2.7.	Mittente .....		14
2.8.	Destinatario .....		14
3.	<b>IDENTIFICAZIONE E AUTENTICAZIONE</b> .....		14
3.1.	Generalità sulle procedure per l'identificazione .....		14
3.2.	Identificazione del Titolare persona fisica o giuridica .....		14
3.2.1.	Procedura di Identificazione .....		14
3.3.	Processo di verifica e attivazione del servizio .....		15
3.3.1.	Processo di verifica della richiesta .....		15
3.3.2.	Attivazione del servizio .....		15
3.4.	Sistema OAuth 2.0 per l'autenticazione .....		15
3.4.1.	Profili utente del servizio .....		16
3.4.1.1.	Utente-Admin .....		16
3.4.1.2.	Utente-Sender .....		16
3.5.	Credenziali applicative per accesso API .....		16
3.5.1.	Rilascio delle credenziali API .....		16
3.5.2.	Sospensione o revoca delle credenziali API .....		17
4.	<b>FUNZIONALITÀ DEL SISTEMA</b> .....		17
4.1.	Generalità .....		17
4.2.	Modalità di utilizzo del servizio .....		17
4.2.1.	Interfaccia Web .....		17
4.2.2.	Interfaccia API .....		17
4.3.	Accesso al servizio .....		18
4.3.1.	Accesso tramite interfaccia Web .....		18
4.3.2.	Accesso tramite API .....		18
4.3.3.	Sessione e protocolli di trasmissione .....		18
4.4.	Gestione delle utenze .....		18
4.5.	Invio delle comunicazioni .....		19
4.5.1.	Invio tramite interfaccia Web .....		19

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

- 4.5.2. API di accesso al servizio .....20
- 4.6. Modalità di gestione del contenuto .....21
- 4.7. Canali per l'invio .....21
- 4.8. Ricezione del messaggio .....21
- 4.9. Evidenze .....21
  - 4.9.1. Eventi certificati .....22
    - 4.9.1.1. Certifica la ricezione della comunicazione .....22
    - 4.9.1.2. Certifica l'apertura degli allegati .....22
    - 4.9.1.3. Accettazione esplicita del messaggio .....22
  - 4.9.2. Evidenze supportate da PosteNotifica .....23
  - 4.9.3. Visualizzazione .....24
  - 4.9.4. Conservazione Evidenze .....25
- 5. MONITORAGGIO DELL'UTILIZZO DEL SISTEMA .....25
  - 5.1. LOG di accesso .....25
  - 5.2. LOG di invio .....26
  - 5.3. Servizio di monitoring .....26
- 6. LIVELLI DEL SERVIZIO .....26
  - 6.1. Livelli di servizio .....26
  - 6.2. Servizi di terze parti .....26
  - 6.3. Servizi di emergenza .....27
- 7. MISURE DI SICUREZZA E CONTROLLI .....27
  - 7.1. Generalità .....27
  - 7.2. Sicurezza fisica .....27
    - 7.2.1. Backup dei dati .....28
  - 7.3. Controlli procedurali e sicurezza logica .....28
    - 7.3.1. Ruoli chiave .....28
    - 7.3.2. Accesso ai sistemi .....28
    - 7.3.3. Regole comportamentali .....28
    - 7.3.4. Raccomandazioni per il Titolare .....28
  - 7.4. Controllo del personale .....29
    - 7.4.1. Qualifiche, esperienze e autorizzazioni richieste .....29
    - 7.4.2. Procedure di controllo delle esperienze pregresse .....29
    - 7.4.3. Requisiti di formazione .....29
    - 7.4.4. Frequenza di aggiornamento della formazione .....29
    - 7.4.5. Frequenza nella rotazione dei turni di lavoro .....29
    - 7.4.6. Sanzioni per azioni non autorizzate .....30
    - 7.4.7. Controlli sul personale non dipendente .....30

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

7.4.8.	Documentazione che il personale deve fornire.....	30
7.5.	Compromissione del servizio e Business continuity .....	30
7.5.1.	Procedure per la gestione degli incidenti .....	30
7.5.2.	Corruzione delle chiavi, del software o dei dati .....	30
7.5.3.	Servizi di firma e marcatura .....	30
7.6.	Cessazione del servizio di prestatore o provider di servizio .....	30
7.7.	Controlli sulla sicurezza informatica .....	31
7.7.1.	Requisiti di sicurezza specifici dei server.....	31
7.7.2.	Valutazioni di vulnerabilità .....	31
7.7.3.	Requisiti di sicurezza relativi agli amministratori dei sistemi .....	31
8.	CONTROLLI E VALUTAZIONI DI CONFORMITÀ .....	31
8.1.	Frequenza o circostanze per la valutazione di conformità .....	31
8.2.	Identità e qualifiche di chi effettua il controllo.....	32
8.3.	Rapporti tra Postel e CAB .....	32
8.4.	Aspetti oggetto di valutazione .....	32
8.5.	Azioni in caso di non conformità.....	32
9.	ALTRI ASPETTI LEGALI E DI BUSINESS.....	32
9.1.	Copertura assicurativa .....	32
9.2.	Proprietà intellettuale.....	32
9.3.	Rappresentanza e garanzie .....	32
9.4.	Canali di comunicazione ufficiali .....	33
9.5.	Assistenza clienti .....	33

## 1. INTRODUZIONE

### 1.1. Quadro generale

Il presente documento è il Manuale Operativo del Prestatore di Servizi Fiduciari **Postel S.p.A** (*Trust Service Provider*, di seguito Postel) che descrive il servizio **PosteNotifica, servizio elettronico di recapito certificato qualificato**.

**Il servizio è realizzato nel rispetto del Regolamento UE N. 910/2014 eIDAS.**

Il manuale contiene le politiche e le pratiche seguite nel processo di identificazione e rilascio del servizio PosteNotifica, le misure di sicurezza adottate, gli obblighi, le garanzie e le responsabilità, in conformità con la vigente normativa in materia di servizi fiduciari qualificati.

Pubblicando tale Manuale Operativo e inserendo i riferimenti a tale documento nella contrattualistica e in appositi link delle interfacce d'uso, si consente agli utenti di valutare le caratteristiche e l'affidabilità del servizio PosteNotifica offerto da Postel, e quindi le modalità di accesso al servizio nonché del legame ed i rapporti che intercorrono tra servizio stesso e *Cliente*.

Il presente Manuale Operativo contiene altresì le **politiche e le pratiche** seguite da Postel nel processo di controllo

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

delle richieste, identificazione del *Responsabile* in base al *Contratto* (cfr. paragrafo §1.2.4) e nel **rilascio del servizio** di cui all'art. 3, def. 37) e art. 44 del Regolamento UE N. 910/2014 eIDAS [1], **sulla base del Testo Unico del Codice dell'Amministrazione Digitale (CAD) [2] e delle disposizioni di AGID** sulle modalità per la presentazione delle domande di iscrizione nella Trusted List come ERDSP (Electronic Registered Delivery Service Provider), e **in conformità con** i requisiti e **policy di sicurezza** definite nello standard ETSI EN 319 521 [6] .

Il **servizio di recapito certificato qualificato**, specificato nel presente Manuale Operativo, è contraddistinto da una serie di caratteristiche che sono pienamente identificate e connesse, nei paragrafi che seguono, agli standard e ai regolamenti (o specifiche parti di essi) che ne rappresentano la base di supporto.

Si riportano qui di seguito gli aspetti essenziali di più alto livello che sono poi ulteriormente dettagliati nelle successive specifiche sezioni.

Il principale tratto che contraddistingue il servizio PosteNotifica è quello di essere definito in accordo alle **policy e security requirements** definite nello standard ETSI EN 319 521[6]. In altre parole, dal punto di vista più generale possibile, si tratta di un servizio che in tale standard è definito come **Electronic Registered Delivery Service (ERDS)**.

Un flusso di PosteNotifica, dal punto di vista generale e in assenza di ambiguità, può essere identificato dal cosiddetto *style of operation* denominato "**Store and Notify**" (**S&N** da qui in avanti): il messaggio del mittente viene sottoposto al servizio per essere inviato, il servizio lo memorizza (**store**) in delle aree dedicate al cliente mittente ed invia al destinatario una notifica (**notify**) con quanto necessario perché il ricevente possa accedere al messaggio del mittente.

## 1.2. Identificazione del documento

### 1.2.1. Nome e identificativo del documento

Questo documento è denominato "Manuale Operativo - PosteNotifica" (*QERDS Practice Statement*) ed è caratterizzato dal codice documento: **Man 1229**. La versione e il livello di rilascio sono identificabili nel piè di pagina.

Al documento sono associati gli Object Identifier (OID) (cfr. def. paragrafo §1.2.4) e gli Uniform Resource Identifier (URI), descritti in seguito.

#### L'*object identifier* (OID) che identifica Postel è 1.3.76.54

Lo *Uniform Resource Identifier* (URI) radice, che identifica degli oggetti significativi nell'ambito degli standard ETSI, è **http://uri.etsi.org** (o **https://uri.etsi.org**).

Gli identificativi significativi per servizio di recapito certificato qualificato e per il relativo Manuale Operativo sono:

Descrizione	OID
Servizio recapito certificato qualificato	<b>1.3.76.54.1</b>
Manuale operativo servizio recapito certificato qualificato	<b>1.3.76.54.1.1</b>

Tabella 1 – Identificativi

### 1.2.2. Scopo e campo di applicazione del documento

Il presente documento ha lo scopo di descrivere le regole e le procedure operative adottate da Postel nella conduzione del **servizio di recapito certificato qualificato** in accordo alle norme e standard correnti, come riportato al paragrafo §1.1.

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

Il presente manuale costituisce, inoltre, un'integrazione di dettaglio all'informativa fornita al *Cliente* ai sensi dell'articolo 13 del D.Lgs. 196/03 e l'art. 13 del Regolamento (UE) 679/2016 [\[3\]](#).

Il diritto d'autore sul presente documento è di **Postel S.p.A.** Tutti i diritti sono riservati.

### 1.2.3. Riferimenti normativi e tecnici

#### 1.2.3.1. Riferimenti normativi e tecnici

[1] **Regolamento UE N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014** in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE modificato dal Regolamento UE N. 2024/1183 del Parlamento Europeo e del Consiglio dell'11 aprile 2024 (referenziato come EIDAS)

[2] **Decreto Legislativo 7 marzo 2005, n.82** (G.U. n.112 del 16 maggio 2005 - S.O. n. 93) – Codice dell'amministrazione digitale (referenziato anche come CAD) e ss.m.ii.

[3] **Decreto Legislativo 30 giugno 2003, n. 196** (G.U. n. 174 del 29 luglio 2003) – Codice Privacy e ss.mm.ii e Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (vigente dal 25 maggio 2018).

[4] **Direttiva 2011/83/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2011**, sui diritti dei consumatori e relative normative nazionali di recepimento.

[5] **ETSI EN 319 401** "Electronic Signatures and Infrastructures (ESI): General Policy Requirements for Trust Service Providers". Requisito vigente.

[6] **ETSI EN 319 521** "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers". Requisito vigente.

[7] **ETSI EN 319 522** "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services". Requisito vigente.

[8] **Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013** (GU Serie Generale n.117 del 21-05-2013) – "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71".

[9] **ETSI EN 319 403** "Requirements for conformity assessment bodies assessing Trust Service Providers".

[10] **IETF RFC 6749** "The OAuth 2.0 Authorization Framework"

[11] **IETF RFC 6750** "The OAuth 2.0 Authorization Framework: Bearer Token Usage"

#### 1.2.3.2. Standard di riferimento procedurali

Tutti i processi operativi del QERDSP Postel descritti in questo Manuale Operativo, come ogni altra attività del QERDSP Postel, sono svolti in modalità conforme al Piano di qualità aziendale e di sicurezza, in accordo agli standard **ISO/IEC 9001:2015** e **ISO/IEC 27001:2013**. È in fase di aggiornamento la versione dello standard ISO/IEC 27001:2022.

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

### 1.2.3.3. Standard di riferimento di sicurezza

Per assicurare la sicurezza del servizio di recapito certificato qualificato, Postel utilizza tecniche e procedure basate su standard (de jure o de facto) internazionali e sulle norme specifiche esistenti in Italia.

Nella redazione e nella messa a punto delle procedure ci si è basati sugli standard:

- **Information Technology Security Evaluation Criteria (ITSEC) v. 1.2**
- **Common Criteria for Information Technology Security Evaluation v 2.2**
- **ISO/IEC 27001:2013** - Sicurezza delle informazioni, cybersecurity e protezione della privacy - Sistemi di gestione per la sicurezza delle informazioni à è in corso una migrazione alla versione 2022 della norma
- **ISO IEC 27002:2022** – Information Technology – Security Techniques – Code of practice for Information Security Management
- **UNI CEI EN ISO/IEC 27017** - Tecnologie Informatiche - Tecniche di sicurezza - Raccolta di prassi sui controlli per la sicurezza delle informazioni per i servizi in cloud basata sulla ISO/IEC 27002
- **UNI CEI EN ISO/IEC 27018** - Tecnologie informatiche - Tecniche di sicurezza - Raccolta di prassi per la protezione dei dati personali trattati in cloud pubblici da responsabili del trattamento
- **UNI CEI ISO/IEC 29115** - Tecnologie informatiche - Tecniche per la sicurezza - Quadro di riferimento per la garanzia dell'autenticazione delle entità

I moduli crittografici (HSM) sono quelli di InfoCert, per le chiavi di firma digitale dei contenuti e delle evidenze (ERDS evidence) sono validati e certificati FIPS 140-2 level 3 e Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL).

### 1.2.4. Definizioni

Sono di seguito elencate in tabella le definizioni utilizzate nella stesura del presente documento. Per i termini definiti nelle norme sopra referenziate si rimanda alle definizioni in essi stabilite.

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

Termine	Definizione
<b>Cliente</b>	<b>Persona fisica o giuridica che acquista/richiede il servizio di recapito certificato qualificato e si assume la facoltà di sospenderlo o revocarlo.</b>
<b>Titolare</b>	Persona fisica o giuridica, richiedente il servizio, che dovrà essere identificata come Titolare del servizio del recapito certificato qualificato.  <b>Il Titolare è il soggetto mittente (Sender) di tutte le comunicazioni effettuate nell'utilizzo del servizio. In alcuni casi il Titolare coincide con il cliente.</b>
<b>Responsabile</b>	Persona fisica che verrà effettivamente identificata in quanto Titolare (persona fisica) o legale rappresentante del Titolare o persona munita di procura del Titolare
<b>Intermediario</b>	Con il termine <i>Intermediario autorizzato</i> (o semplicemente <i>Intermediario</i> ) si intende il rivenditore (o distributore) di Postel che svolge attività di vendita del servizio PosteNotifica.
<b>Utente</b>	Persona o applicazione autorizzata ad accedere al servizio PosteNotifica tramite autenticazione.
<b>Utente-Admin</b>	Utente che accede al servizio PosteNotifica attraverso le credenziali del servizio di recapito certificato qualificato che si occupa di censire nuove utenze.
<b>Utente-Sender</b>	Utente che accede al servizio PosteNotifica attraverso le credenziali del servizio di recapito certificato qualificato che si occupa dell'invio dei messaggi certificati.
<b>Mittente / Sender</b>	Il Titolare che invia la comunicazione al destinatario.
<b>Destinatario / Receiver</b>	Persona fisica (anche in rappresentanza di un'organizzazione) che riceve la comunicazione da parte del mittente a seguito di identificazione.
<b>Identity Provider (IdP)</b>	Gestore dell'identità digitale.
<b>Servizio elettronico di recapito certificato (SERC)</b>	«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» (cfr art, 3, def.36) eIDAS [1].
<b>Electronic registered delivery service (ERDS)</b>	Come definito all'articolo 3 del Regolamento eIDAS[1] « a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations; » (cfr art, 3, def.36) eIDAS [1].
<b>Servizio elettronico di recapito certificato qualificato (SERCQ) / Qualified Electronic Registered Delivery Service (QERDS)</b>	Servizio elettronico di recapito certificato che soddisfa i seguenti requisiti: <ul style="list-style-type: none"> <li>a) sono forniti da uno o più prestatori di servizi fiduciari qualificati;</li> <li>b) garantiscono con un elevato livello di sicurezza l'identificazione del mittente;</li> <li>c) garantiscono l'identificazione del destinatario prima della trasmissione dei dati;</li> <li>d) l'invio e la ricezione dei dati sono garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato in modo da escludere la possibilità di modifiche non rilevabili dei dati;</li> <li>e) qualsiasi modifica ai dati necessaria al fine di inviarli o riceverli è chiaramente indicata al mittente e al destinatario dei dati stessi;</li> <li>f) la data e l'ora di invio e di ricezione e qualsiasi modifica dei dati sono</li> </ul>

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

	<p>indicate da una validazione temporale elettronica qualificata.» (cfr art, 3, def.37) e art.44 eIDAS [1]).</p> <p>Ove non espressamente indicato, nel presente documento, per “servizio” si intende “servizio di recapito certificato qualificato”.</p>
<b>Servizio PosteNotifica</b>	<b>Il Servizio elettronico di recapito certificato qualificato erogato da Postel S.p.A.</b>
<b>Autorità per la marcatura temporale / Time-stamping authority</b>	Prestatore di servizi qualificato, che agisce da terza parte fidata, che eroga il servizio di marcatura temporale {Time-stamping authority}.
<b>Organismo di valutazione della conformità/ Conformity Assessment Body (CAB)</b>	Organismo accreditato a norma del Regolamento eIDAS come competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati. Redige il CAR. (cfr. art.3 def. 18) eIDAS [1]).
<b>Relazione di valutazione della conformità / Conformity Assessment Report (CAR)</b>	Relazione con cui l'organismo di valutazione della conformità conferma che il prestatore di servizi fiduciari qualificati e i servizi fiduciari stessi rispettano i requisiti del Regolamento (cfr. artt.21 e 51 eIDAS [1]).
<b>Open ID Connect &amp; OAuth2.0</b>	Protocollo di autenticazione interoperabile basato sul quadro di specifiche OAuth 2.0 (IETF RFC 6749 [10] e 6750[11]). Semplifica il modo di verificare l'identità degli utenti in base all'autenticazione eseguita da un server di autorizzazione e permette di ottenere informazioni sul profilo utente in modo interoperabile e simile al modello REST.TitolareOAuth
<b>Livello di Garanzia / Level of Assurance (LoA)</b>	<p>Livello di sicurezza o di garanzia dei regimi di identificazione elettronica progressivamente crescente in base alla sensibilità del servizio erogato. Sono individuati tre livelli di garanzia (cfr. art. 8 comma2 eIDAS [1]) in base a quanto definito dallo standard ISO/IEC 29115:</p> <ul style="list-style-type: none"> <li>• livello 1- Basso/Low (corrispondente al LoA2 dell'ISO-IEC 29115);</li> <li>• livello 2 – Medio/Substantial (corrispondente al LoA3 dell'ISO-IEC 29115);</li> <li>• livello 3 – Alto/High (corrispondente al LoA4 dell'ISO-IEC 29115).</li> </ul> <p>Per il dettaglio si rimanda alla norma ISO.</p> <p>Il livello minimo di garanzia permesso per autenticazione e riconoscimento del mittente è il livello 2.</p>
<b>Contratto</b>	Il contratto per l'attivazione del servizio di recapito certificato qualificato PosteNotifica è composto dalla Richiesta di Attivazione, dalle Condizioni Generali di Contratto, da questo Manuale Operativo e dai documenti ivi richiamati che costituiscono complessivamente la disciplina dei rapporti tra le parti.
<b>Credenziali dell'Utente</b>	Insieme di dati e fattori propri di un <i>Utente</i> utilizzati per accedere al servizio di recapito certificato qualificato attraverso un sistema di autenticazione a due fattori. Titolare.
<b>Dati di identificazione personale</b>	Un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona giuridica (cfr. eIDAS [1]).
<b>Identificazione elettronica</b>	Il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica (cfr. eIDAS [1]).
<b>Marca temporale</b>	Il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo (cfr. art.1, def, h) DPCM 22 febbraio 2013)[8].
<b>Mezzi di identificazione elettronica</b>	Un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online (cfr. eIDAS [1]).

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

<b>Password usata una sola volta / One Time Password (OTP)</b>	Password valida solo per una singola transazione. Nell'ambito del servizio di recapito certificato qualificato può essere utilizzata come <i>secondo fattore di autenticazione</i> a convalida delle <i>Credenziali dell'Utente</i> .
<b>Prestatore di servizi fiduciari qualificato</b>	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 (cfr. eIDAS [1]).
<b>Richiesta di attivazione</b>	La richiesta del <i>Titolare</i> in cui viene richiesta l'attivazione del servizio di recapito certificato qualificato PosteNotifica.

Tabella 2 - Definizioni

### 1.2.5. Acronimi e abbreviazioni

Acronimo	Definizione
<b>AgID</b>	Agenzia per l'Italia Digitale: autorità di Vigilanza sui Prestatori di Servizi Fiduciari
<b>CA</b>	Certification Authority
<b>CAB</b>	Conformity Assessment Body – Organismo di valutazione della conformità
<b>CAD</b>	Codice dell'Amministrazione Digitale (cfr. DL 7 Marzo 2005 0)
<b>CAR</b>	Conformity Assessment Report – Relazione di valutazione della conformità
<b>CIE</b>	Carta di Identità Elettronica
<b>eID</b>	Electronic Identity
<b>eIDAS</b>	Electronic Identification and Signature Regulation (cfr. 0)
<b>ETSI</b>	European Telecommunications Standards Institute
<b>HTTPS</b>	HyperText Transfer Protocol Secure
<b>IP (o Indirizzo IP)</b>	Indirizzo numerico che identifica gli elaboratori connessi alla rete.
<b>ISO</b>	International Organization for Standardization: fondata nel 1946, l'ISO è un'organizzazione internazionale costituita da organismi nazionali per la standardizzazione
<b>OID</b>	Object Identifier: è costituito da una sequenza di numeri, registrata secondo la procedura indicata nello standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia
<b>SPID</b>	Sistema Pubblico di Identità Digitale
<b>S&amp;N</b>	Store and Notify

Tabella 3 – Acronimi e abbreviazioni

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

### 1.3. Manuale Operativo

Il presente Manuale Operativo, compilato dal QERDS Postel nel rispetto delle disposizioni generali degli standard di riferimento (ETSI EN 319 521 [6]), è fornito all'organismo di vigilanza designato - che per l'Italia è AgID - ed è parte costituente la documentazione di qualificazione di prestatore di servizio di recapito certificato qualificato.

#### 1.3.1. Periodo e meccanismo di notifica

Il Manuale Operativo è pubblicato:

- in formato elettronico sul sito Web di Postel S.p.A.;
- in formato elettronico nell'elenco pubblico dei certificatori tenuto da AgID;
- in formato cartaceo può essere richiesto all'*Intermediario autorizzato* o al contatto per gli utenti finali.

#### 1.3.2. Soggetti responsabili dell'approvazione del Manuale Operativo

Questo Manuale Operativo viene verificato dai seguenti responsabili e approvato dalla Direzione Aziendale.

Incarico	Responsabile
<b>a) Responsabile della sicurezza e del piano per la sicurezza;</b>	Marco Bonanni (CISO Postel)
<b>b) Responsabile QTSP</b>	Nicolò Vaccaro (SGOV Postel)
<b>c) Responsabile della conduzione tecnica dei sistemi ERDS</b>	Massimo Tarola (TPDE Postel)
<b>d) Responsabile dei servizi tecnici e logistici</b>	Alessio Artico (SGOV Postel)
<b>e) Responsabile delle verifiche e delle ispezioni (auditing);</b>	Francesco Freda (SGOV Postel)
<b>f) Validation Specialist</b>	Gianni Bartolini (SGOV Postel)
<b>Incarico</b>	<b>Responsabile</b>
<b>Identity verification officer</b>	Giuseppe Apicerni (SOSM Postel)

#### 1.3.3. Procedure di approvazione

La redazione e l'approvazione del manuale seguono le procedure previste dal Sistema di Gestione per la Qualità dell'Azienda ISO 9001:2015.

Con frequenza non superiore all'anno, il Prestatore di Servizi Fiduciari esegue un controllo di conformità di questo Manuale Operativo al proprio processo di erogazione del servizio di certificazione.

#### 1.3.4. Revisione del Manuale Operativo

Postel si riserva di apportare variazioni al presente documento per esigenze tecniche o per modifiche alle procedure intervenute sia a causa di norme di legge o regolamenti, sia per ottimizzazioni del ciclo lavorativo.

Ogni nuova versione del Manuale Operativo annulla e sostituisce le precedenti versioni.

Variazioni che non hanno un impatto significativo sugli utenti comportano l'incremento del numero di release del documento, mentre variazioni con un impatto significativo sugli utenti (come, ad esempio, modifiche rilevanti alle procedure operative) comportano l'incremento del numero di versione del documento. In ogni caso il manuale sarà

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

prontamente pubblicato e reso disponibile.

Con frequenza non superiore all'anno, il QERDS Postel esegue un controllo di conformità di questo Manuale Operativo al proprio processo di erogazione del servizio di recapito certificato qualificato.

## 2. RUOLI DEL SERVIZIO POSTENOTIFICA

### 2.1. Fornitore del servizio PosteNotifica

Il servizio di recapito certificato qualificato PosteNotifica consente di trasmettere contenuti, fornendo prove relative al trattamento del messaggio trasmesso, fra cui l'avvenuto invio, e protegge i messaggi trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate.

In questo documento, quando non diversamente specificato, si usa il termine QERDS per indicare QERDS Service Provider Postel.

I dati completi dell'organizzazione che svolge la funzione di **QERDS** sono i seguenti:

<i>Denominazione sociale</i>	<b>Postel S.p.A.</b> <b>Società con socio unico, soggetta a direzione e coordinamento di Poste Italiane S.p.A.</b>
<i>Sede legale</i>	<b>Viale Europa, 175 - 00144 Roma</b>
<i>Sedi operative</i>	
<i>Rappresentante legale</i>	<b>Carlo Rosini - In qualità di Amministratore Delegato</b>
<i>N. di telefono</i>	<b>+39 06 514261</b>
<i>Codice Fiscale e n. iscr. al Registro delle Imprese</i>	<b>04839740489</b>
<i>Partita IVA</i>	<b>05692591000</b>
<i>Capitale Sociale</i>	<b>€ 20.400.000,00 i.v.</b>
<i>REA</i>	<b>912141</b>
<i>Sito Web</i>	<b><a href="https://www.postel.it/">https://www.postel.it/</a></b>

### 2.2. Intermediario autorizzato

Il servizio viene commercializzato da Postel S.p.A. attraverso rete di vendita sotto il nome di **Intermediario autorizzato** - come definito al paragrafo §1.2.4

L'intermediario ha come unico compito quello di rivendere il servizio erogato da Postel S.p.A.

### 2.3. Cliente

La presente persona o soggetto giuridico è definita al paragrafo §1.2.4.

### 2.4. Titolare

La presente persona o soggetto giuridico è definita al paragrafo §1.2.4.

### 2.5. Responsabile

La presente persona o soggetto giuridico è definita al paragrafo §1.2.4.

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

## 2.6. Utente-Admin e Utente-Sender

La persona all'interno della organizzazione del Titolare a cui è demandata la gestione del servizio (Utente-Admin) e l'invio delle comunicazioni (Utente-Admin o Utente-Sender) è definita al paragrafo § 1.2.41.2.4.

## 2.7. Mittente

Titolare che invia la comunicazione al destinatario, come definito al paragrafo §1.2.4.

## 2.8. Destinatario

La persona che riceve la comunicazione dal mittente, come definita al paragrafo §1.2.4.

# 3. IDENTIFICAZIONE E AUTENTICAZIONE

## 3.1. Generalità sulle procedure per l'identificazione

I paragrafi di questo capitolo descrivono le procedure usate per l'identificazione del *Titolare*, necessaria all'attivazione del servizio di recapito certificato qualificato PosteNotifica.

La procedura di identificazione comporta che il *Titolare* sia riconosciuto dal servizio, che ne verificherà l'identità attraverso una delle modalità definite nei successivi paragrafi del presente capitolo.

## 3.2. Identificazione del Titolare persona fisica o giuridica

La richiesta del servizio di recapito certificato qualificato per un **Titolare persona fisica** verrà effettuata attraverso la procedura descritta al paragrafo successivo.

La richiesta del servizio di recapito certificato qualificato per un **Titolare persona giuridica** (organizzazione) deve essere effettuata da una persona fisica, il *Responsabile*, identificata nello stesso modo del Titolare persona fisica, in una delle modalità descritte al paragrafo successivo.

Il Responsabile, inoltre, deve presentare la documentazione relativa alla persona giuridica e la documentazione o procura, che attesti il titolo ad avanzare la richiesta per conto della persona giuridica.

### 3.2.1. Procedura di Identificazione

La richiesta di attivazione del servizio può essere effettuata attraverso il Validation Specialist di Postel, attraverso la sottoscrizione del contratto di servizio sia in modalità digitale che cartacea.

Per l'attivazione del servizio PosteNotifica è necessario che il Titolare compili e firmi il modulo di richiesta di attivazione del servizio che dovrà contenere le seguenti informazioni:

- dati del Titolare del servizio di recapito certificato qualificato
- dati del Responsabile (se Titolare persona fisica è coincidente con il Titolare)
- dati della persona incaricata a svolgere le funzioni di utente "Admin" (cfr. paragrafo §1.2.4)
- accettazione delle condizioni generali del servizio
- riferimento (identificativo mail) della persona della struttura tecnica interna all'organizzazione, Titolare che seguirà le fasi operative di attivazione del servizio.

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

### 3.3. Processo di verifica e attivazione del servizio

#### 3.3.1. Processo di verifica della richiesta

Postel, attraverso personale, anche di terze parti, opportunamente formato, avvia il processo di verifica per procedere poi all'attivazione del servizio.

Le verifiche effettuate per permettere l'attivazione sono le seguenti:

- verifica della validità della firma del Richiedente;
- nel caso di entità giuridica, Postel, verifica che il richiedente abbia poteri di firma;
- eventuale verifica della procura in caso il richiedente non sia il legale rappresentante.

Il controllo, la supervisione e l'aggiornamento delle procedure necessarie alla verifica dei poteri di firma e delle eventuali verifiche relative alla procura sono effettuati da Postel o suoi delegati sotto propria responsabilità.

#### 3.3.2. Attivazione del servizio

Terminate le verifiche, l'attivazione procede con la seguente modalità.

Viene preso contatto con la struttura tecnica (indicata dal Titolare nel modulo di attivazione) per la raccolta delle informazioni relative al sistema di autenticazione e autorizzazione.

Il Titolare del servizio deve indicare le informazioni necessarie per poter abilitare un accesso sicuro almeno di livello 2 (*medio/substantial* - LoA3 dell'ISO-IEC 29115).

Per l'accesso al servizio è necessario configurare opportunamente il sistema OAuth 2.0 dedicato all'organizzazione cliente, impostando, tramite console Web:

- il nuovo Titolare, con le informazioni relative
- il sistema di autenticazione del Titolare, come da specifiche della struttura tecnica
- l'Utente-Admin, come indicato nel modulo di attivazione e informi il Titolare della avvenuta configurazione.

Dopo l'attivazione, l'Utente-Admin potrà accedere all'interfaccia Web di PosteNotifica (cfr. paragrafo §4.3.1) con le proprie credenziali, definite dall'organizzazione nell'ambito del proprio sistema di autenticazione, e da essa opportunamente profilate. Il sistema di autenticazione deve essere almeno di livello 2 (*medio/substantial* - LoA3 dell'ISO-IEC 29115).

### 3.4. Sistema OAuth 2.0 per l'autenticazione

Per l'autenticazione degli utenti (*Utente-Admin* e *all'Utente-Sender*), PosteNotifica utilizza OpenID Connect (OIDC).

OpenID Connect (OIDC) è un protocollo di autenticazione basato su OAuth 2.0, uno standard ampiamente adottato, che permette alle applicazioni di autenticare gli utenti verificando l'identità attraverso un Identity Provider (IdP) compatibile con OIDC, come ad esempio Google, Microsoft Azure, o un IdP aziendale.

Applicando un'autenticazione forte, con almeno un livello 2 (*medio/substantial* - LoA3 dell'ISO-IEC 29115) OIDC garantisce che gli account del mittente aderiscano a protocolli di autenticazione avanzati (Multi-Factor Authentication - MFA) per una maggiore sicurezza. Ciò è particolarmente importante data la natura sensibile delle comunicazioni gestite da PosteNotifica. Viene richiesto, pertanto, che l'organizzazione Titolare del servizio, sia provvista di un servizio di autenticazione e autorizzazione con protocollo OAuth (*i sistemi più utilizzati sono Microsoft Authenticator e Google Authenticator*) e che l'autenticazione debba essere almeno di livello 2 (*medio/substantial* - LoA3 dell'ISO-IEC 29115).

La responsabilità della verifica dell'identità degli utenti è pertanto delegata al servizio di autenticazione e autorizzazione utilizzato dal Titolare.

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

Postel ha la facoltà di non accettare sistemi di autenticazione ritenuti non idonei all'utilizzo di PosteNotifica.

### 3.4.1. Profili utente del servizio

Il servizio PosteNotifica prevede due profili: l'Utente-Admin e l'Utente-Sender.

#### 3.4.1.1. Utente-Admin

La persona, che accede al servizio PosteNotifica attraverso le credenziali del servizio di recapito certificato qualificato, a cui è demandata, all'interno dell'organizzazione del Titolare, la gestione del servizio.

In particolare, l'Utente-Admin si occupa di censire nuove utenze (di tipo Utente-Admin e Utente-Sender) (cfr. paragrafo §1.2.4).

Il profilo abilitato solo nell'interfaccia Web.

#### 3.4.1.2. Utente-Sender

Utente che accede al servizio PosteNotifica attraverso le credenziali del servizio di recapito certificato qualificato e si occupa dell'invio dei messaggi certificati (cfr. paragrafo §1.2.4). [il profilo abilitato nell'interfaccia Web e in API.](#)

## 3.5. Credenziali applicative per accesso API

Oltre alla modalità manuale tramite interfaccia Web, il servizio di recapito certificato qualificato permette di avere una API di accesso per le funzioni di invio e verifica, che possono essere integrate dal Titolare in modalità applicativa.

In questo scenario un'applicazione del Titolare può collegarsi al servizio e schedulare in modo automatizzato gli invii, effettuare verifiche sullo stato dei recapiti, integrare processi del cliente con invii certificati all'interno del servizio.

Per l'integrazione applicativa Postel rilascia credenziali OAuth 2.0 che il Titolare può portare nelle applicazioni per l'autenticazione API.

L'interfaccia API mette a disposizione le funzioni descritte al paragrafo §4.5.2.

### 3.5.1. Rilascio delle credenziali API

Per il rilascio delle credenziali applicative, il Titolare:

- effettua richiesta a InfoCert, indicando un identificativo per distinguere l'applicazione/processo del cliente che utilizzerà tali credenziali
- InfoCert predispone e fornisce le credenziali di accesso in modalità sicura al Titolare.

Per l'autenticazione applicativa viene utilizzato lo standard di settore OAuth 2.0. Attraverso tale standard è possibile semplificare in modo significativo la gestione delle credenziali nel tempo.

La configurazione di un canale applicativo si articola in due macrofasi: nella prima si generano le credenziali e si impostano manualmente nell'applicativo; la seconda consente il rinnovo automatico delle stesse da parte dell'applicazione, senza la necessità di ulteriori interventi degli operatori.

Nella prima macrofase si ottiene un token autorizzativo alla risorsa (tipicamente indicato come token JWT) che ha una durata dell'ordine dei minuti, ma comunque sufficiente a consentire la configurazione della parte applicativa. Il token contiene al suo interno la validità dello stesso e delle credenziali di rinnovo che, se utilizzate all'interno della validità del token stesso, permettono il rinnovo e quindi il relativo mantenimento automatico nel tempo delle credenziali di canale di accesso.

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

Nella richiesta è pertanto possibile indicare la durata delle credenziali, comunque non oltre i 15 minuti, per permettere al Titolare di limitare l'accesso al solo tempo necessario all'applicazione/processo che ne deve fare uso.

Il servizio, nell'utilizzo dell'interfaccia API, tiene traccia nei log delle operazioni effettuate dalle applicazioni, con identificazione delle credenziali utilizzate.

Il Titolare deve concordare con InfoCert le modalità di rilascio e distribuzione delle credenziali sul proprio sistema di autenticazione che dovrà rispettare almeno il livello 2 (medio/substantial - LoA3 dell'ISO-IEC 29115).

### 3.5.2. Sospensione o revoca delle credenziali API

Il Titolare, in qualsiasi momento, può sospendere o revocare le credenziali API.

Questa operazione permette di bloccare, nella fase di autenticazione, l'accesso al servizio.

Per procedere alla sospensione/revoca delle credenziali API, il Titolare ne fa richiesta a Postel che:

1. verifica autenticità della richiesta;
2. sospende/revoca dell'utenza e delle credenziali;
3. avvisa il Titolare della rimozione.

In seguito alla sospensione/revoca non verrà più permesso l'accesso al servizio.

## 4. FUNZIONALITÀ DEL SISTEMA

### 4.1. Generalità

Il servizio di recapito certificato qualificato **PosteNotifica**, erogato da Postel, permette a un mittente di inviare delle comunicazioni certificate qualificate ad uno o più destinatari, nel paradigma *Store and Notify (Memorizzazione e Notifica)*.

Il contenuto della comunicazione, che può contenere anche allegati, viene preso in carico dal servizio e propagato al destinatario, secondo le modalità operative descritte in questo capitolo.

Sia il mittente sia il destinatario vengono identificati nella transazione di invio della comunicazione. Tutte le operazioni effettuate dal mittente e dal destinatario vengono tracciate e gestite in modo sicuro dal servizio.

Il servizio non permette alcuna modifica del contenuto originale una volta inviato.

I paragrafi che seguono descrivono nel dettaglio le modalità operative di utilizzo.

### 4.2. Modalità di utilizzo del servizio

Il servizio di recapito certificato qualificato PosteNotifica prevede due modalità per l'utilizzo del servizio.

#### 4.2.1. Interfaccia Web

In questo caso gli utenti possono utilizzare le varie funzionalità previste dal servizio in modalità manuale.

#### 4.2.2. Interfaccia API

Tramite API, un'interfaccia applicativa esposta per l'integrazione da parte di applicazioni del Titolare, il servizio PosteNotifica può essere utilizzato dai processi gestiti dal cliente.

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

## 4.3. Accesso al servizio

### 4.3.1. Accesso tramite interfaccia Web

Dopo l'attivazione, gli utenti (*Utente-Admin* e *Utente-Sender*) possono accedere all'interfaccia Web con le proprie credenziali, definite dall'organizzazione nell'ambito del proprio sistema di autenticazione, e da essa opportunamente profilate.

L'accesso all'interfaccia Web di PosteNotifica prevede l'autenticazione di livello 2 (*medio/substantial - LoA3 dell'ISO-IEC 29115*).

Ad ogni accesso è necessario effettuare una nuova autenticazione.

Anche al destinatario (*Receiver*) viene richiesto di identificarsi, tramite autenticazione SPID di livello 2 (*medio/substantial - LoA3 dell'ISO-IEC 29115*) o CIE, per poter accedere al contenuto a lui destinato.

Una volta autenticato al servizio (cfr. capitolo §3), l'utente può accedere all'interfaccia Web ed utilizzare le funzionalità del sistema fino alla scadenza della sessione o al logout esplicito dell'utente.

### 4.3.2. Accesso tramite API

L'accesso tramite API viene protetto tramite protocollo OAuth 2.0, con credenziali rilasciate al Titolare (vedi procedure descritte al § 3.5), che permettono di autenticare l'applicazione chiamante del Titolare.

### 4.3.3. Sessione e protocolli di trasmissione

La sessione, sia nell'interfaccia Web sia in API, scade in modo automatico dopo 1 ora di inattività.

L'accesso, sia tramite interfaccia Web sia tramite API, prevede l'utilizzo di protocollo HTTPS TLS versione 1.2 o 1.3, garantendo l'autenticazione del server in modo sicuro, la protezione del dato nella fase di invio del mittente (interfaccia Web o API) e l'accesso ai contenuti del *destinatario/Receiver* (interfaccia Web).

## 4.4. Gestione delle utenze

L'interfaccia Web di PosteNotifica consente all'Utente-Admin di gestire le utenze già presenti nel proprio Identity Provider (IdP).

La gestione dei profili consente agli amministratori di gestire e mantenere il controllo sull'accesso al sistema, garantendo che solo gli utenti autorizzati possano utilizzare PosteNotifica.

Attraverso l'interfaccia Web, l'Utente-Admin può registrare nuove utenze (di tipo *Utente-Admin* e *Utente-Sender*) e assegnare ruoli e permessi specifici agli utenti all'interno del servizio.

Nello specifico, l'Utente-Admin è infatti autonomo, nel poter:

- abilitare e gestire nuovi Utente-Admin per la gestione del servizio;
- abilitare e gestire nuovi Utente-Sender per predisporre ed effettuare nuovi invii.

Gli utenti, Utente-Admin e Utente-Sender, devono far parte dell'organizzazione del Titolare, e, pertanto, devono essere censiti nel sistema di autenticazione configurato.

Una volta registrate le utenze, l'autenticazione delle stesse viene delegata al sistema di autenticazione del Titolare tramite il protocollo OAuth 2.

Nel caso in cui si desideri revocare l'accesso di una di queste utenze al servizio PosteNotifica, l'Utente-Admin può cancellarla dall'interfaccia. In questo modo, l'utenza non potrà più accedere a PosteNotifica.

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

The screenshot shows a 'Create user' form with the following fields and sections:

- Email \***: A text input field.
- First name \***: A text input field.
- Last name \***: A text input field.
- Roles**: A dropdown menu.
- Time zone\***: A dropdown menu.
- Sender permissions**: A section containing several toggle switches:
  - Sender:**
    - View process types
    - Create process types
    - Edit process types
    - View campaigns
    - Create campaigns
    - Edit campaigns
    - Access to analytics and reports
  - Admin:**
    - Manage users
    - Read users
- Available cost centers \***: A text input field.

Figura 1- Schermata di creazione utenza

Per creare un nuovo Utente-Sender, l'utente-Admin deve inserire l'e-mail aziendale registrata sul IdP della propria azienda, assegnare un ruolo appropriato e configurare il centro di costo a cui l'Utente-Sender apparterrà.

I privilegi previsti per i profili sono i seguenti:

- **Utente-Admin:**
  - **Manage users:** *creare/cancellare e gestire le utenze assegnando il centro di costo su cui gli utenti hanno visibilità;*
  - **Read users:** *visualizzare le utenze censite sulla piattaforma.*
- **Utente-Sender:**
  - **View process types:** *visionare la lista dei tipi di processo già creati*
  - **Create process types:** *creare nuovi tipi di processo*
  - **Edit process types:** *abilitare l'utente-sender a cambiare i tipi di processo*
  - **View campaigns:** *visionare le campagne create*
  - **Create campaigns:** *creare nuove campagne*
  - **Edit campaigns:** *modificare campagne esistenti*
  - **Access to analytics and reports:** *accedere alla Dashboard delle comunicazioni*

## 4.5. Invio delle comunicazioni

Per l'invio delle comunicazioni, il Titolare può scegliere il metodo più adatto alle proprie esigenze e preferenze:

- tramite interfaccia Web;
- tramite una interfaccia applicativa API.

### 4.5.1. Invio tramite interfaccia Web

L'interfaccia di PosteNotifica offre una piattaforma per la configurazione e l'invio delle comunicazioni.

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

Una volta effettuato l'accesso al sistema (cfr. paragrafo §4.3), l'utente (*Utente-Admin* e *Utente-Sender*) accede a un'interfaccia che fornisce gli strumenti necessari per poter creare un processo di creazione della comunicazione.

La prima fase consiste nella definizione dei dettagli fondamentali, come il titolo della comunicazione, la lista dei destinatari e il contenuto del messaggio. Qui, il mittente ha la possibilità di personalizzare il testo, aggiungere allegati e selezionare il canale di invio preferito tra le opzioni disponibili, come e-mail o SMS.

Una volta definiti tutti i parametri necessari (Figura 2), il mittente può visualizzare un'anteprima della comunicazione per verificare che tutto sia corretto e completo.

PosteNotifica offre anche altre funzionalità, come la programmazione dell'invio in un momento specifico nel futuro e la creazione di modelli predefiniti per semplificare il processo di configurazione delle comunicazioni ricorrenti.

Dopo aver confermato i dettagli, il mittente può inviare la comunicazione. Una volta inviato, PosteNotifica monitora attentamente lo stato della comunicazione, fornendo aggiornamenti in tempo reale sulle consegne, le aperture e le interazioni dei destinatari. Questa visibilità completa consente al mittente di tracciare l'efficacia della comunicazione.

Figura 2 - Schermata di configurazione di un processo

#### 4.5.2. API di accesso al servizio

PosteNotifica offre API pubbliche che consentono agli sviluppatori di integrare facilmente le funzionalità della piattaforma nei propri sistemi e applicazioni. L'accesso a queste API è gestito tramite OAuth 2 (cfr. paragrafo §4.3.2).

OAuth 2 fornisce una serie di caratteristiche che lo rendono ideale per l'integrazione delle API di PosteNotifica. Tra queste caratteristiche vi sono la gestione sicura delle credenziali degli utenti, la delega delle autorizzazioni tramite token di accesso, la separazione dei ruoli e delle autorizzazioni e la scalabilità per supportare un grande numero di utenti e applicazioni.

Per semplificare ulteriormente il processo di integrazione delle API di PosteNotifica, è disponibile un DevPortal online. Questa piattaforma fornisce agli sviluppatori un accesso centralizzato a documentazione dettagliata, esempi di codice,

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

specifiche di Swagger e altre risorse utili per comprendere e utilizzare le API di PosteNotifica in modo efficace. Attraverso il DevPortal, gli sviluppatori possono accedere a istruzioni dettagliate su come autenticarsi, eseguire le richieste API e utilizzare tutte le funzionalità offerte dal prodotto.

## 4.6. Modalità di gestione del contenuto

Il servizio di recapito certificato qualificato PosteNotifica prevede che il contenuto dell'invio, con relativi allegati, non venga inviato al destinatario attraverso i canali di comunicazione, bensì:

- il contenuto da mettere a disposizione del destinatario viene preso in carico dal servizio e viene mantenuto in modo protetto e sicuro all'interno del servizio;
- viene predisposto un URL unico per permettere al destinatario di accedere al contenuto tramite il servizio;
- viene inoltrato al destinatario l'URL tramite il canale di comunicazione scelto dal mittente.

Il destinatario non può quindi accedere al contenuto prima di aver effettuato le fasi di accesso al servizio e identificazione, come previsto dalle specifiche QERDS.

## 4.7. Canali per l'invio

PosteNotifica offre una varietà di canali per l'invio delle comunicazioni tramite cui il destinatario può accedere all'interfaccia di PosteNotifica. Gli attuali canali di invio offerti sono email e SMS. Ogni canale presenta caratteristiche uniche che consentono agli utenti di scegliere quello più adatto al tipo di comunicazione e al destinatario.

Il servizio, attualmente, si affida ai seguenti provider per l'invio della comunicazione, attraverso l'utilizzo delle licenze software open source o delle API messe a disposizione del provider come descritto di seguito:

- **SMS** – Twilio – Licenza MIT Open Source
- **Email** – Amazon SES (simple email service) - Amazon BOTO – Licenza Open-source Apache License 2.0

I manuali operativi e le policy d'uso, che includono le obbligazioni delle parti nell'utilizzo del servizio sono accessibili ai rispettivi siti Web dei provider.

Inoltre, PosteNotifica offre la possibilità di configurare un canale secondario per garantire la consegna dei messaggi anche in situazioni critiche o impreviste. Il canale secondario entra in azione nel caso in cui l'invio attraverso il canale principale incontrasse delle difficoltà, come ad esempio problemi tecnici o indisponibilità di un servizio esterno come, ad esempio, la mail server del destinatario. Configurando un canale secondario, gli utenti possono assicurarsi che il messaggio venga comunque recapitato al destinatario, garantendo continuità e affidabilità nella comunicazione.

## 4.8. Ricezione del messaggio

Quando PosteNotifica crea una campagna di comunicazione, genera una prova iniziale per tracciare l'inizio del processo. Successivamente, ogni interazione correlata a questa campagna genera ulteriori evidenze, fornendo una traccia completa delle attività svolte.

Queste interazioni possono includere la ricezione della comunicazione da parte del server remoto, l'apertura del messaggio da parte del destinatario o il download di eventuali allegati. È importante notare che tutte queste evidenze sono conformi agli standard stabiliti dall'ETSI (European Telecommunications Standards Institute). Pertanto, ogni feedback ricevuto dai sistemi esterni e dal destinatario stesso genererà ulteriori evidenze, contribuendo a fornire una panoramica dettagliata e accurata dell'intero processo di comunicazione.

## 4.9. Evidenze

Le evidenze iniziano a essere generate al momento della creazione della campagna e dell'aggiunta dei destinatari. Quando la campagna di comunicazione viene accettata e pianificata, PosteNotifica crea l'evidenza SubmissionAcceptance. Quando la notifica è pronta per essere inviata, PosteNotifica contatta il server o il provider destinatario e, una volta ricevuta la conferma dal server, viene generata l'evidenza NotificationForAcceptance (Tabella

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

6). Se è configurato per attestare la visualizzazione degli allegati, PosteNotifica genera l'evidenza ContentHandover, che conferma l'avvenuta visualizzazione degli allegati configurati nella comunicazione.

Tutti gli ulteriori eventi relativi al processo sono tracciati in linea con le disposizioni di cui alla normativa ETSI applicabile.

### 4.9.1. Eventi certificati

Quando viene configurato un modello per inviare una comunicazione, l'utente-sender ha la possibilità di scegliere il tipo di certificazione che desidera ottenere per quel processo di comunicazione.

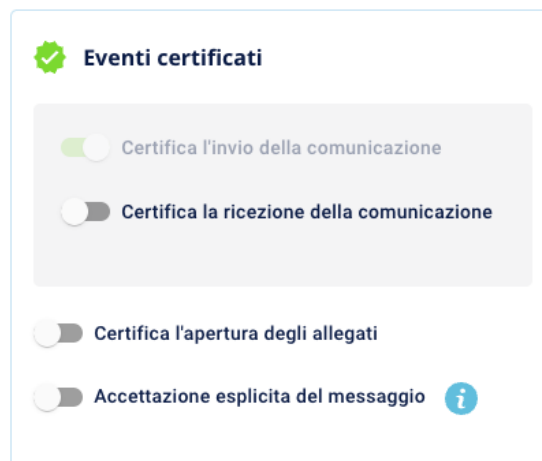


Figura 3 - Configurazione degli eventi certificati

#### 4.9.1.1. Certifica la ricezione della comunicazione

La certificazione offerta da PosteNotifica attesta ufficialmente la ricezione della comunicazione da parte del destinatario. Quando abilitato, vengono prodotte le evidenze ContentAccessTracking o NotificationAccessTracking a seconda della tipologia di messaggio.

#### 4.9.1.2. Certifica l'apertura degli allegati

La funzione di certificazione dell'apertura degli allegati attesta che il destinatario ha effettivamente aperto i file allegati alla comunicazione. Questo offre una prova concreta e verificabile che il contenuto allegato è stato visualizzato, aggiungendo un ulteriore livello di trasparenza e controllo. Tale certificazione è particolarmente utile per garantire la tracciabilità e la conformità in contesti dove è cruciale sapere che il destinatario non solo ha ricevuto, ma anche aperto e visualizzato gli allegati della comunicazione. Quando abilitato, viene prodotta la evidenza ContentHandover.

#### 4.9.1.3. Accettazione esplicita del messaggio

La funzione di accettazione esplicita del messaggio consente di ottenere una conferma chiara e verificabile che il destinatario ha accettato consapevolmente la comunicazione. Questo meccanismo richiede al destinatario di compiere un'azione specifica per confermare la ricezione e l'accettazione del messaggio, garantendo così che il messaggio non solo è stato ricevuto, ma anche accettato con piena consapevolezza. Quando abilitato, viene prodotta l'evidenza ConsignmentAcceptance o ConsignmentRejection, a seconda di come il destinatario interagisce con il sistema.

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

#### 4.9.2. Evidenze supportate da PosteNotifica

La seguente classificazione degli eventi è implementata da PosteNotifica in piena conformità con i pertinenti standard ETSI.

Evidenza ETSI	Descrizione
<b>SubmissionAcceptance</b>	Il messaggio originale è stato inviato con successo all'S-ERDS dal mittente.
<b>SubmissionRejection</b>	Il contenuto dell'utente-sender che è stato inviato all'S-ERDS dal mittente non è stato accettato dall'S-ERDS.
<b>NotificationForAcceptance</b>	L'R-ERDS ha notificato al destinatario la disponibilità di un messaggio (senza necessariamente rivelare il mittente, il contenuto, ecc.) e ha chiesto la disponibilità del destinatario ad accettarlo.
<b>RelayToNonERDS</b>	Un contenuto dell'utente-sender è stato inoltrato con successo a un sistema non ERDS per la consegna.
<b>NotificationForAcceptanceFailure</b>	Il destinatario non ha potuto essere notificato (o è chiaro che sarà impossibile notificare il destinatario) entro un determinato periodo di tempo a causa di errori tecnici e/o altre ragioni, oppure non esiste alcuna prova di notifica entro il periodo di tempo dato. Questo periodo di tempo può essere determinato dalla legislazione, dalle regole di politica dell'R-ERDS o dai parametri forniti dal mittente o dall'S-ERDS.
<b>RelayToNonERDSFailure</b>	Il tentativo di inoltrare un contenuto dell'utente-sender a un sistema non ERDS è fallito a causa di errori tecnici e/o altre ragioni.
<b>ConsignmentAcceptance</b>	Il destinatario ha eseguito un'azione esplicita indicando all'ERDS che ha emesso la notifica l'accettazione di ricevere un contenuto dell'utente.
<b>ConsignmentRejection</b>	Il destinatario, dopo una corretta identificazione e autenticazione, ha eseguito un'azione esplicita indicando all'R-ERDS il rifiuto di ricevere un contenuto dell'utente.
<b>ContentHandover</b>	Le prove correlate attestano che il contenuto dell'utente, in un momento specifico indicato dalle prove, ha attraversato il confine dell'R-ERDS ed è stato consegnato all'UA/Applicazione del destinatario dopo un'adeguata autenticazione.
<b>ConsignmentNotificationFailure</b>	Indica che la consegna del messaggio è fallita. Ciò può accadere a causa di un timeout nella consegna del messaggio quando scade il limite di tempo della campagna e il destinatario non ha ancora completato la politica di invio.

Tabella 4- Evidenze ETSI supportate da PosteNotifica

Al fine di implementare funzionalità aggiuntive non esplicitamente previste dagli standard ETSI, viene aggiunta la seguente evidenza:

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

Evidenza ETSI	Descrizione
ContentAccessTracking	Il destinatario ha aperto e letto l'email, che contiene la comunicazione nel suo contenuto. Questa comunicazione non include un link a PosteNotifica (lato destinatario).  <b>Questa evidenza è utilizzata solo quando l'OTP (one-time password) è disabilitato.</b>
NotificationAccessTracking	Il destinatario apre un'email che contiene un link che punta al sistema del destinatario.  Questa evidenza è applicabile solo quando la comunicazione include un livello di certificazione di accettazione esplicita, quando vi è evidenza che l'allegato è stato aperto e/o quando l'OTP è abilitato.
FailoverSubmission	Il canale principale di comunicazione non era accessibile a causa di un errore tecnico (ad esempio, l'indirizzo email non esiste o il server è inattivo). Viene attivato il canale di fallback per la comunicazione.  Questa evidenza è applicabile solo quando è stato configurato un canale secondario per la consegna.

Tabella 5 - Evidenze create in piena conformità ETSI

### 4.9.3. Visualizzazione

Una volta completato il processo di invio, sia che ciò avvenga per il completamento della politica di invio, per un timeout o per errori, verrà abilitato un tasto "audit".

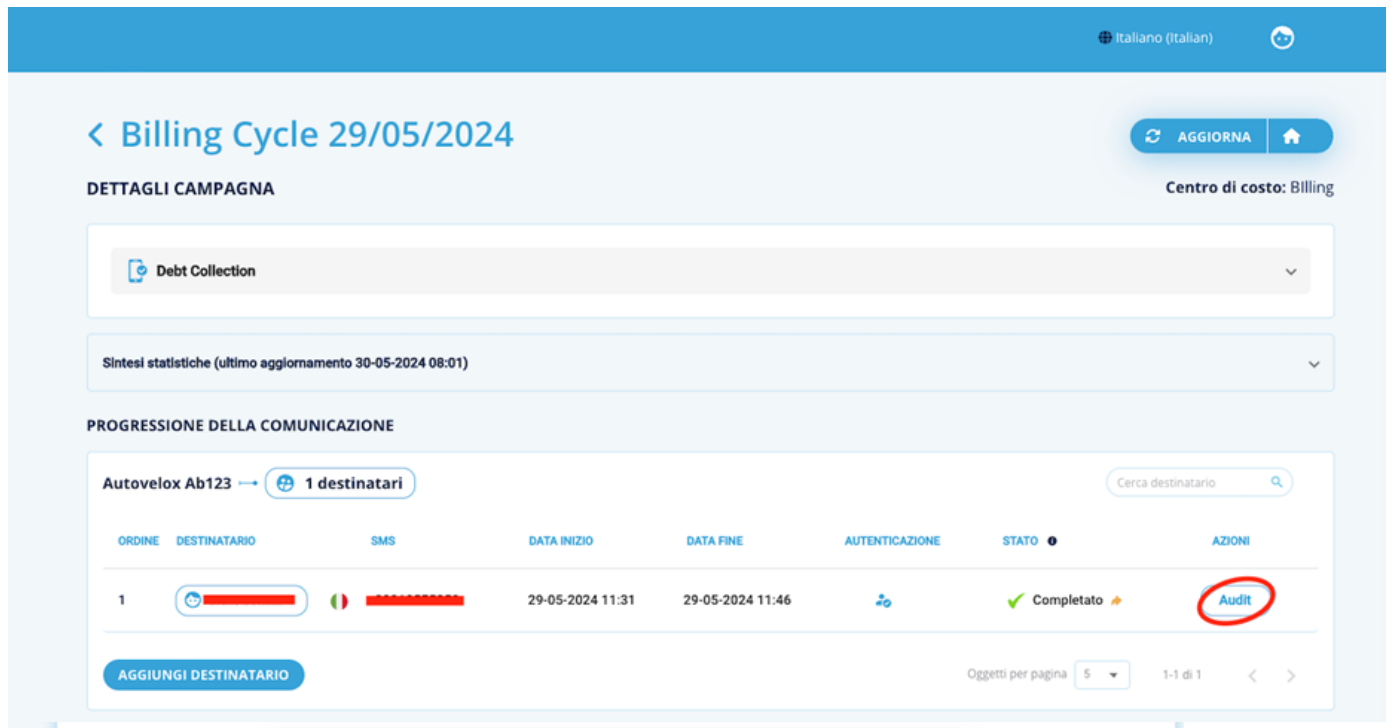


Figura 4 - Cruscotto gestione comunicazioni e tasto Audit

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

Cliccando su “Audit”, sarà possibile scaricare un report, firmato digitalmente, in formato PDF. All'interno di questo report, si trova un sommario dettagliato di tutto ciò che è accaduto durante il processo di comunicazione, fornendo una panoramica chiara e comprensibile delle attività e degli esiti delle operazioni di invio.

Oltre al sommario, il report PDF include anche tutte le evidenze generate durante il processo, allegate in formato XML. Queste evidenze contengono informazioni precise e dettagliate che documentano ogni fase del processo di invio. Utilizzando un software apposito, è possibile estrarre e visualizzare queste evidenze per un'analisi più approfondita. Questo sistema di reportistica garantisce trasparenza e tracciabilità, consentendo di verificare e comprendere ogni aspetto della comunicazione inviata tramite PosteNotifica.

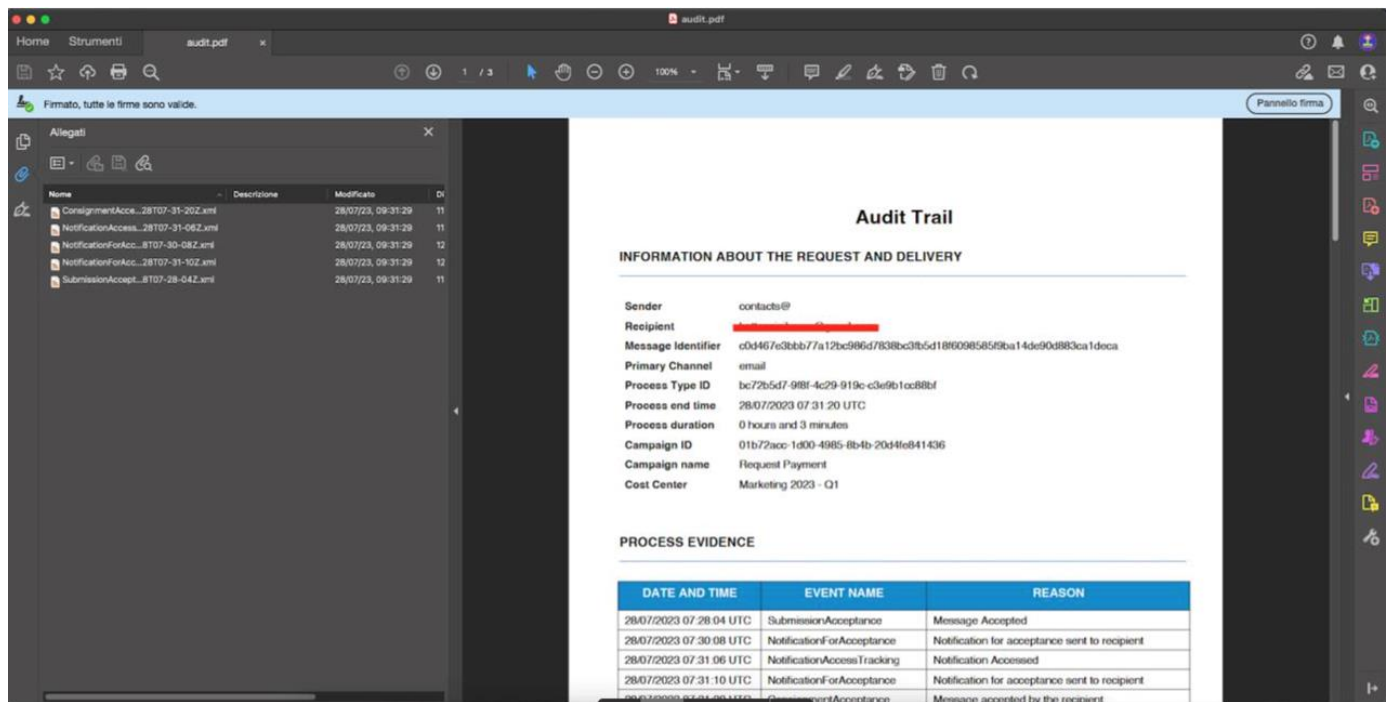


Figura 5 – Audit Trail

#### 4.9.4. Conservazione Evidenze

Tutte le evidenze generate da PosteNotifica sono archiviate e sottoposte a una politica di retention che garantisce la loro conservazione per un periodo di 20 (venti) anni.

Tutte le evidenze relative ai riconoscimenti del mittente e destinatario sono archiviate e sottoposte a una politica di retention che garantisce la loro conservazione per un periodo di 20 (venti) anni.

Questo significa che ogni interazione, evento o attività relativa alle comunicazioni inviate tramite la piattaforma viene accuratamente registrata e mantenuta accessibile per un arco di tempo sufficiente a soddisfare eventuali esigenze di verifica, audit o conformità normativa.

## 5. MONITORAGGIO DELL'UTILIZZO DEL SISTEMA

### 5.1. LOG di accesso

I log di accesso sono gestiti tramite il software Keycloak, un'applicazione open source per la gestione dell'identità e degli accessi. Inizialmente, i log rimangono salvati su Keycloak, dopodiché vengono trasferiti su un database di

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

retention, dove vengono conservati per almeno 2 (due) anni.

Tuttavia, nel caso di autenticazione tramite SPID/CIE, la gestione dei log di accesso non è gestita da Keycloak, bensì da eID Gateway, un progetto creato per centralizzare la gestione dell'accesso. Una volta effettuato l'accesso, sarà eID Gateway ad occuparsi della retention dei log di accesso per almeno 2 (due) anni.

## 5.2. LOG di invio

Durante l'utilizzo di PosteNotifica, ogni attività e ogni evento rilevante sono registrati e archiviati come log.

Questi log servono per tracciare l'utilizzo del sistema, monitorare le performance e identificare eventuali problemi. Per garantire un'archiviazione affidabile e duratura di tali dati, PosteNotifica utilizza Amazon CloudWatch come piattaforma di registrazione. CloudWatch offre una soluzione robusta e scalabile per la gestione dei log, consentendo di conservare i dati per lunghi periodi di tempo. In particolare, i log generati da PosteNotifica vengono mantenuti su CloudWatch per almeno 2 (due) anni, garantendo un accesso a lungo termine a tutte le informazioni rilevanti sull'utilizzo della piattaforma.

## 5.3. Servizio di monitoring

Per verificare la disponibilità del servizio sono state attivate sonde Web e strumenti di Event Management che, a fronte di componenti non disponibili, provvedono ad allertare sistemisti ed operatori.

Ognuno di questi strumenti, qualora rilevi un malfunzionamento, provvede ad allertare le figure preposte al fine che vengano attuate le contromisure previste per la tipologia di problematica riscontrata nel servizio.

In particolare, le segnalazioni delle sonde vengono analizzate dal processo di Problem Management aziendale; il processo prevede la produzione di specifici output.

# 6. LIVELLI DEL SERVIZIO

## 6.1. Livelli di servizio

Qualora non diversamente specificato dalle Condizioni Generali di Contratto, i livelli di servizio previsti sono dalle 0.00 alle 24.00, 7 giorni su 7 (disponibilità minima 99,9%).

## 6.2. Servizi di terze parti

Per l'erogazione del servizio di recapito certificato qualificato Postel si avvale di servizi di terze parti che garantiscono alta affidabilità e resilienza:

Postel si avvale dei servizi professionali specialistici di InfoCert, finalizzati all'evoluzione funzionale della piattaforma SERC/SERCQ con l'obiettivo di garantire un miglioramento continuo delle sue capacità, consentendo, ad esempio:

- Integrazione con sistemi eterogenei, come i sistemi di Multicanalità Postel, per ottimizzare la comunicazione e l'interoperabilità con altre piattaforme aziendali;
- Configurazione di interfacce dati per facilitare la connessione con sistemi di billing Postel e altri sistemi di gestione dei dati dei clienti, migliorando l'efficienza e l'accuratezza delle informazioni scambiate;
- Sviluppo di personalizzazioni specifiche della piattaforma SERC/SERCQ, al fine di soddisfare esigenze operative particolari dei clienti Postel, garantendo soluzioni su misura;
- Cloud pubblico AWS per l'erogazione del servizio. L'architettura prevede l'utilizzo di servizi gestiti per container, storage, backup, etc., con attivazione dei micro-servizi in più availability zones delle Region AWS scelte (Region attualmente utilizzate Dublin).
- Twilio per invio notifiche via SMS
- AWS SES per invio notifiche via mail

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

- KeyCloak, come servizio per l'autenticazione di utenti (IdP OAuth 2.0) e Token
- Kong per l'esposizione delle API di servizio

Vengono inoltre utilizzati servizi di backup immutabile degli storage usati per dati applicativi, contenuti ed evidenze.

### 6.3. Servizi di emergenza

Al fine di garantire il corretto completamento gestione dei contenuti ed il rilascio delle relative evidenze (QERDS Evidences) sono state predisposte le seguenti soluzioni tecniche ed organizzative.

- **Utilizzo di sistemi ad alta disponibilità su Cloud AWS**, con una architettura a microservizi attivi su più availability zones, in modo da garantire l'alta affidabilità del servizio.
- **Strumenti di controllo automatico**: sono attivi nel sistema di recapito certificato qualificato strumenti automatici di verifica del sistema e delle varie componenti funzionali. In base ai problemi rilevati il sistema prevede azioni per la risoluzione degli stessi o la notifica ad operatori per consentirne l'intervento
- **Gestione dei disastri**: il QERDS Postel ha adottato le procedure necessarie a garantire la continuità del servizio anche in situazioni di elevata criticità – PosteNotifica

## 7. MISURE DI SICUREZZA E CONTROLLI

### 7.1. Generalità

Il QERDS Postel ha realizzato un sistema di sicurezza del sistema informativo relativo al servizio di recapito certificato qualificato.

Il sistema di sicurezza implementato è articolato su più livelli tra cui:

- L'utilizzo di un Cloud pubblico (AWS), che garantisce la resilienza e la sicurezza dei servizi in esso caricati;
- un livello procedurale e logistico, con aspetti prettamente organizzativi;
- un livello logico, tramite la predisposizione di misure tecnologiche hardware e software che affrontano i problemi e i rischi connessi con la tipologia del servizio;

Tale sistema di sicurezza è realizzato per evitare rischi derivanti dal malfunzionamento dei sistemi, della rete e delle applicazioni, oltre che dall'intercettazione non autorizzata o dalla modifica dei dati.

Tutti i processi operativi del QERDS Postel nella erogazione del servizio di recapito certificato qualificato sono conformi al Piano di qualità aziendale.

Un estratto della politica di sicurezza Postel è disponibile facendone richiesta alla seguente casella di recapito certificato qualificato: [affarisocietari.postel@pec.postel.it](mailto:affarisocietari.postel@pec.postel.it).

Le politiche di sicurezza in Postel sono sottoposte a review non meno che annualmente, vengono inoltre aggiornate a fronte di ogni cambiamento significativo. Ogni review viene tracciata all'interno del documento stesso quand'anche non sia stato necessario apportare alcuna modifica.

### 7.2. Sicurezza fisica

La sicurezza fisica è demandata al servizio Cloud AWS.

Attualmente la region di erogazione è Dublino, con i servizi attivi distribuiti su tre availability zone.

AWS dispone di certificazioni di conformità ai sensi degli standard ISO/IEC 27001:2022, 27017:2015, 27018:2019 e ISO/IEC 9001:2015 e le sue pratiche sono pubblicamente disponibili sul sito Web: Il manuale operativo di AWS EC2 è pubblicamente disponibile sul sito Web: <https://docs.aws.amazon.com/> Il manuale operativo di AWS EC2 è

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

pubblicamente disponibile sul sito Web: <https://docs.aws.amazon.com/> Il manuale operativo di AWS EC2 è pubblicamente disponibile sul sito Web: <https://docs.aws.amazon.com/>

### 7.2.1. Backup dei dati

Per i sistemi di recapito certificato qualificato il fornitore esegue regolarmente i backup.

Il fornitore di infrastruttura fa uso delle più moderne tecnologie per l'esecuzione di salvataggi dei contenuti dei dischi. I prodotti utilizzati per la gestione dei backup controllano e gestiscono l'esecuzione dei salvataggi e la loro archiviazione.

Il tempo di ritenzione di un salvataggio è mensile.

## 7.3. Controlli procedurali e sicurezza logica

### 7.3.1. Ruoli chiave

I ruoli chiave sono coperti da figure dotate dei necessari requisiti di esperienza, professionalità e competenza tecnica e giuridica, che vengono continuamente verificati mediante le valutazioni annuali.

La lista dei nomi e l'organigramma delle figure in ruolo chiave è stata depositata presso AgID in occasione del primo accreditamento e viene costantemente tenuta aggiornata per seguire la naturale evoluzione dell'organizzazione aziendale.

### 7.3.2. Accesso ai sistemi

L'accesso ai sistemi è consentito solo al personale autorizzato.

Gli operatori Postel e quelli del fornitore hanno diritto di accesso ai sistemi con le autorizzazioni minime necessarie allo svolgimento delle proprie mansioni.

I sistemi mantengono traccia degli accessi e delle operazioni effettuate.

### 7.3.3. Regole comportamentali

Le Politiche di Sicurezza di Postel e i documenti collegati illustrano le linee guida e la policy aziendale per tutti i servizi presenti in azienda. Tali documenti hanno l'obiettivo di creare una maggiore coscienza e considerazione in tutto il personale, circa la riservatezza delle informazioni e delle attività effettuate durante l'orario d'ufficio. Il personale viene esplicitamente invitato "alla massima riservatezza" riguardo a tutte le informazioni di cui venga in possesso. Sono indicate le norme per l'accesso fisico dei dipendenti e dei consulenti esterni, le norme per l'utilizzo del badge, e le regole per l'accesso fuori orario. Parte dei documenti sono dedicati alla sicurezza delle apparecchiature, dei sistemi e delle applicazioni informatiche. Sono indicate le norme circa l'uso della password (segretezza e necessità di cambiarla periodicamente) e del PC (utilizzo limitato all'uso professionale, cura e responsabilità della macchina, divieto di utilizzo di software non rilasciato dall'apposito ufficio, norme per la connessione remota, norme per la gestione dei virus, norme per l'accesso ad Internet e per l'utilizzo della posta elettronica, rimozione immediata degli accessi qualora non più necessari). Obiettivo delle politiche in essi espresse è, anche, minimizzare la possibilità che software illegale o non autorizzato possa essere introdotto, anche involontariamente, nella rete interna.

Tutti i documenti non riservati rivolti al personale sono disponibili nella Intranet aziendale.

### 7.3.4. Raccomandazioni per il Titolare

Il *Titolare* deve custodire in maniera sicura le credenziali e gli strumenti di autenticazione al servizio; deve utilizzare il servizio per le sole modalità previste dal Manuale Operativo e dalle vigenti leggi nazionali e internazionali.

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

È opportuno dotare le stazioni di lavoro di un antivirus costantemente aggiornato per garantire maggiore sicurezza per quanto viene spedito e ricevuto.

## 7.4. Controllo del personale

### 7.4.1. Qualifiche, esperienze e autorizzazioni richieste

Effettuata la pianificazione annuale delle Risorse Umane, il Responsabile Funzione/Struttura Organizzativa identifica le caratteristiche e le skill della risorsa da inserire (job profile). Successivamente, di concerto con il responsabile selezione, viene attivato il processo di ricerca e selezione.

### 7.4.2. Procedure di controllo delle esperienze pregresse

I candidati individuati partecipano al processo di selezione affrontando un primo colloquio conoscitivo-motivazionale con il responsabile della selezione e un successivo colloquio tecnico con il responsabile di Funzione/Struttura Organizzativa, volto a verificare le skill dichiarate dal candidato. Ulteriori strumenti di verifica sono esercitazioni e test.

### 7.4.3. Requisiti di formazione

A garanzia che nessun individuo possa singolarmente compromettere o alterare la sicurezza globale del sistema oppure svolgere attività non autorizzate, è previsto di affidare la gestione operativa del sistema a persone diverse, con compiti separati e ben definiti. Il personale addetto alla progettazione ed erogazione del servizio di recapito certificato qualificato è un dipendente Postel ed è stato selezionato in base alla esperienza nella progettazione, realizzazione e conduzione di servizi informatici, con caratteristiche di affidabilità e riservatezza. Interventi di formazione sono pianificati periodicamente per sviluppare la consapevolezza dei compiti assegnati. In particolare, prima dell'inserimento del personale nell'attività operativa, sono realizzati interventi formativi allo scopo di fornire ogni competenza (tecnica, organizzativa e procedurale) necessaria a svolgere i compiti assegnati.

### 7.4.4. Frequenza di aggiornamento della formazione

Ogni inizio anno viene svolta l'analisi delle esigenze formative propedeutica alla definizione delle attività formative da erogare nell'anno. L'analisi è strutturata nel modo seguente:

Incontro con la Direzione per la raccolta dei dati relativi alle esigenze formative necessarie per raggiungere gli obiettivi aziendali;

Intervista ai Responsabili per la rilevazione delle esigenze formative specifiche delle proprie aree;

Restituzione dei dati raccolti alla Direzione Aziendale per chiusura ed approvazione del Piano Formativo.

Entro il mese di febbraio il Piano Formativo così definito viene condiviso e reso pubblico.

### 7.4.5. Frequenza nella rotazione dei turni di lavoro

La presenza in sede o in modalità di lavoro agile (smart working) si distribuisce su una fascia oraria dalle ore 08:00 alle ore 19:00 dal lunedì al venerdì.

Il presidio degli ambienti di produzione nella fascia notturna e nella fascia festiva viene garantito attraverso un piano di turnazione della reperibilità predisposto dal responsabile di unità organizzativa mensilmente con un anticipo di almeno 10 giorni. A seconda della necessità, gli interventi potranno essere condotti da remoto (teleintervento) o richiedere l'accesso alle sedi.

Fermo restando il possesso dei necessari requisiti tecnici e professionali, l'Azienda provvede ad avvicinare nella reperibilità il maggior numero possibile di lavoratori, dando priorità ai dipendenti che ne facciano richiesta.

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

### 7.4.6. Sanzioni per azioni non autorizzate

Per la procedura di irrogazione delle sanzioni, si fa riferimento ai seguenti CCNL di categoria:

- CCNL per i Dirigenti di Aziende produttrici di Beni e Servizi;
- CCNL per il personale non dirigente di Poste Italiane.

### 7.4.7. Controlli sul personale non dipendente

L'accesso al personale non dipendente è regolato da una specifica policy aziendale.

### 7.4.8. Documentazione che il personale deve fornire

Al momento dell'assunzione, il dipendente deve fornire copia di un documento d'identità valido, copia della tessera sanitaria valida e una foto in formato tessera per il badge di accesso ai locali. Dovrà in seguito compilare e firmare il consenso al trattamento dei dati personali e l'impegno a non divulgare notizie e/o documenti riservati. Dovrà infine prendere visione del Codice Etico e della Netiquette Postel.

## 7.5. Compromissione del servizio e Business continuity

### 7.5.1. Procedure per la gestione degli incidenti

Il QERDS Postel ha descritto le procedure di gestione degli incidenti nell'ambito del SGSI certificato ISO/IEC 27001 e 22301. Ogni eventuale evento anomalo di sicurezza, non appena rilevato, è soggetto a puntuale analisi, individuazione delle contromisure correttive e verbalizzazione da parte del responsabile del servizio. Il verbale è firmato digitalmente; una copia è inviata anche a AgID, unitamente alla dichiarazione delle azioni di intervento mirate a eliminare le cause che possono aver dato luogo all'incident, se sotto il controllo di Postel conforme all'articolo 19 del Regolamento.

### 7.5.2. Corruzione delle chiavi, del software o dei dati

Per aumentare la resilienza in caso di problemi o compromissione della chiave utilizzata per la firma delle evidenze, sono predisposte due chiavi e certificati differenti, con tecnologie di cifratura differenti (RSA 2048 e Curve Ellittiche). In casi di compromissione di una delle chiavi si prevede di sospenderne l'uso e di utilizzare solo la chiave non compromessa.

Tutte le evidenze del sistema di recapito certificato qualificato vengono portate nel sistema di conservazione InfoCert, garantendo integrità e disponibilità anche in caso di compromissione della chiave utilizzata o del servizio.

I dati vengono gestiti, all'interno del servizio QERDS, in modalità sicura su storage ridondati, gestiti dal Cloud Provider, con attivi backup immutabili per garantire il massimo della sicurezza.

Il software è gestito secondo procedure standard secondo i sistemi di qualità ISO 9000.

### 7.5.3. Servizi di firma e marcatura

Il servizio QERDS utilizza nella gestione dei contenuti e delle evidenze, la firma elettronica qualificata e il servizio di marcatura temporale InfoCert, garantendo quindi il massimo in termini di sicurezza e resilienza del servizio.

## 7.6. Cessazione del servizio di prestatore o provider di servizio

Postel ha previsto un piano di terminazione per tutti i casi, schedulati e non schedulati, in cui sia necessario interrompere l'erogazione del servizio QERDS.

Nel caso di cessazione dell'attività di QERDS Provider, Postel comunicherà questa intenzione all'Autorità di vigilanza

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

(AgID) e l'ente di certificazione (CAB) con un anticipo di almeno 6 (sei) mesi, indicando, eventualmente, il QERDS Provider sostitutivo. Con pari anticipo Postel informa della cessazione delle attività tutti i Titolari del servizio di recapito certificato qualificato attivi.

Nella comunicazione, nel caso in cui non sia indicato un provider sostitutivo, sarà chiaramente specificato le modalità operative per l'accesso alle informazioni (evidenze) ancora in carico al gestore.

Si veda il documento QERDS Termination Plan dei Servizi di recapito certificato qualificato PosteNotifica disponibile presso il certificatore qualificato.

## 7.7. Controlli sulla sicurezza informatica

### 7.7.1. Requisiti di sicurezza specifici dei server

Il sistema operativo dei dispositivi, dei server e degli elaboratori utilizzati nelle attività di setup, gestione ed erogazione del servizio di recapito certificato qualificato sono messi in sicurezza, sono cioè configurati, in modo da minimizzare l'impatto di eventuali vulnerabilità eliminando tutte le funzionalità che non servono per il funzionamento e la gestione del servizio stesso.

### 7.7.2. Valutazioni di vulnerabilità

Postel e InfoCert svolgono periodicamente delle valutazioni sulle vulnerabilità del Sistema (vulnerability assessment) e test anti-intrusione (penetration test). A fronte dei risultati mette in atto tutte le contromisure per mettere in sicurezza le applicazioni.

### 7.7.3. Requisiti di sicurezza relativi agli amministratori dei sistemi

L'accesso da parte degli Amministratori di sistema, all'uopo nominati in conformità con quanto prescritto dalla normativa vigente, avviene tramite applicazioni dedicate e predisposte per mantenere l'appropriato livello di sicurezza e i privilegi ad agire sui sistemi, sulle configurazioni e sulle applicazioni solo previa autenticazione individuale. Gli accessi sono tracciati e loggati e conservati per 12 mesi.

## 8. CONTROLLI E VALUTAZIONI DI CONFORMITÀ

Per ottenere la qualifica di prestatore di servizi fiduciari qualificati e non, in conformità al Regolamento eIDAS 0 è necessario espletare l'iter previsto dall'articolo 21 del suddetto Regolamento.

Postel ha presentato ad AgID l'apposita richiesta per ottenere il riconoscimento di "prestatore del servizio fiduciario qualificato" allegando un report della valutazione di conformità con il Regolamento (Conformity Assessment Report - CAR) rilasciato da un organismo di valutazione autorizzato dal preposto organismo nazionale (CAB), che in Italia è ACCREDIA.

Postel presta il Servizio quale prestatore di servizi fiduciari qualificati ai sensi del Regolamento (UE) N. 910/2014 [1] del 23/07/2014, sulla base di una valutazione di conformità effettuata dal Conformity Assessment Body CSQA Certificazioni S.r.l., ai sensi del Regolamento di cui sopra e della Norma ETSI EN 319 401[5] secondo lo schema di valutazione eIDAS 0[1] definito da ACCREDIA a fronte delle norme ETSI EN 319\_403[9] e UNI CEI EN ISO/IEC 17065:2012.

### 8.1. Frequenza o circostanze per la valutazione di conformità

La valutazione di conformità viene ripetuta ogni 2 (due) anni, ma ogni anno il CAB esegue un audit di sorveglianza.

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

## 8.2. Identità e qualifiche di chi effettua il controllo

Il controllo viene effettuato da:

<i>Denominazione sociale</i>	<b>CSQA Certificazioni S.r.l.</b>
<i>Sede legale</i>	<b>Via S. Gaetano n. 74, 36016 Thiene (VI)</b>
<i>N. di telefono</i>	<b>+39 0445 313011</b>
<i>N. Iscrizione Registro Imprese</i>	<b>Business Register no. 02603680246/REA no. 258305</b>
<i>Partita IVA/Codice Fiscale</i>	<b>02603680246</b>
<i>Website</i>	<b><a href="https://www.csqa.it">https://www.csqa.it</a></b>

## 8.3. Rapporti tra Postel e CAB

Postel e CSQA non hanno interessi finanziari né relazioni di affari.

Non sono in corso rapporti commerciali o di partnership che possono creare pregiudizi a favore o contro Postel nella valutazione obiettiva di CSQA.

## 8.4. Aspetti oggetto di valutazione

Il CAB è chiamato a valutare la conformità rispetto al Manuale Operativo, al Regolamento e alla normativa applicabile delle procedure adottate, dell'organizzazione del QERDS Postel, dell'organizzazione dei ruoli, della formazione del personale, della documentazione contrattuale.

## 8.5. Azioni in caso di non conformità

In caso di non conformità, il CAB deciderà se inviare comunque il rapporto ad AgID, o se riservarsi di rieseguire l'audit dopo che la non conformità sia stata sanata.

Postel si impegna a risolvere tutte le non conformità in maniera tempestiva, mettendo in atto tutte le azioni di miglioramento e adeguamento necessarie.

# 9. ALTRI ASPETTI LEGALI E DI BUSINESS

## 9.1. Copertura assicurativa

Postel ha stipulato un contratto assicurativo per la copertura dei rischi dell'attività e dei danni causati a terzi, che ha come massimali:

- 150.000 euro per singolo sinistro;
- Almeno 1.500.000 euro per annualità.

## 9.2. Proprietà intellettuale

Il diritto d'autore sul presente documento è di Postel Tutti i diritti sono riservati.

## 9.3. Rappresentanza e garanzie

Postel mantiene la responsabilità per l'osservanza delle procedure prescritte nella propria policy sulla sicurezza delle informazioni, anche quando alcune funzioni vengono delegate ad un altro soggetto, ai sensi dell'art. 2.4.1. dell'Allegato al Regolamento di esecuzione UE 2015/1502 della Commissione.

Il Titolare è responsabile della veridicità dei dati comunicati nella Richiesta di Attivazione al servizio. Qualora lo stesso, al momento dell'identificazione, abbia, anche attraverso l'utilizzo di documenti personali non veri, celato la propria

Titolo	Titolo documento	Funzione emittente	CCSA/CASD
--------	------------------	--------------------	-----------

reale identità o dichiarato falsamente di essere altro soggetto o, comunque, agito in modo tale da compromettere il processo di identificazione e le relative risultanze indicate nel certificato, sarà considerato responsabile di tutti i danni derivanti al QERDS Postel e/o a terzi dall'inesattezza delle informazioni contenute nella richiesta, con obbligo di garantire e manlevare il QERDS Postel da eventuali richieste di risarcimento danni.

Il Titolare è responsabile dei danni derivanti al QERDS Postel e/o a terzi nel caso di ritardo da parte loro dell'attivazione delle procedure previste nel paragrafo §3.5.2 del presente Manuale Operativo (revoca e sospensione del servizio).

#### 9.4. Canali di comunicazione ufficiali

Si rimanda alle procedure e ai canali di contatto presenti nel paragrafo §0 ed in particolare al Responsabile del Manuale Operativo indicato nel paragrafo §1.3.2.

#### 9.5. Assistenza clienti

Per l'assistenza di primo livello è disponibile un form di Richiesta di contatto sul sito <https://www.postel.it/contattaci>; in alternativa è disponibile un numero verde 800.038.908 (gratuito e accessibile da rete fissa e mobile, attivo dal lunedì al venerdì dalle ore 8.30 alle ore 19:00 esclusi i festivi) o un indirizzo mail [customer.service@postel.it](mailto:customer.service@postel.it).

\*\*\*\* QUESTA È L'ULTIMA PAGINA DEL DOCUMENTO \*\*\*\*