Servizio SERCQ

Recapito certificato e qualificato

Service Practice Statement - PagoPA S.p.A.

PUBBLICO

Firmato Digitalmente da/Signed by:
AgID

In Data/On Date:
venerdì 12 aprile 2024 10:12:53

PagoPA S.p.A.
società per azioni con socio unico
capitale sociale di euro 1,000,000 interamente versato
sede legale in Roma, Piazza Colonna 370, CAP 00187
n. di iscrizione a Registro Imprese di Roma, CF e P.IVA 15376371009

MO_006_Service Practice Statement - rev 1.4	
Predisposto da	*Federica Ciampa* *Responsabile Service Line Piattaforma Notifiche*
Approvato da	*Alessio Biasutto* *Direttore Dipartimento Piattaforma Notifiche & Interoperabilità*
Visto da	
Team Security	
Team Privacy	
In vigore dal	*19 marzo 2024*
Distribuzione	*lista di distribuzione:* - *azienda → repository, → drive condiviso*
Classificazione	*Pubblico*
Contatti: - **per informazioni** - **per aggiornamenti**	

STORICO REVISIONI

REVISIONE		DESCRIZIONE MODIFICA
1.0	23/10/2023	Prima stesura
1.1	01/02/2024	Ridefinizione processo gestito dalla piattaforma SEND come da indicazioni di AgID
1.2	20/02/2024	Recepimento indicazione AgID
1.3	07/03/2024	Recepimento ulteriori indicazione AgID
1.4	19/03/2024	Recepimento ulteriori indicazione AgID

INDICE

SEZIONE I – INFORMAZIONI GENERALI

1. INTRODUZIONE

Il presente Service Practice Statement (SPS) definisce le procedure e politiche applicate da PagoPA (di seguito anche "Gestore") nell'erogazione del servizio di recapito certificato qualificato (SERCQ) ai sensi del Regolamento (UE) n. 910/2014.

Il servizio SERCQ è compreso all'interno di un servizio italiano di gestione della notificazione a valore legale (SEND - Servizio Notifiche Digitali) definito dall'art. 26 del Decreto-legge 17 luglio 2020, n. 76.

Se l'utente destinatario della comunicazione vuole usufruire del servizio SERCQ offerto all'interno di SEND deve esplicitamente accettare i termini e condizioni del servizio ed esplicitamente attivare il SERCQ nel proprio profilo.

All'interno del presente documento viene descritto il processo di Invio / ricezione delle comunicazioni nello scenario in cui venga utilizzato il servizio SERCQ offerto da SEND.

Ogni aggiornamento del Service Practice Statement è preventivamente sottoposto ad AgID prima della pubblicazione da parte del Gestore.

Il Service Practice Statement riporta i dati identificativi del Gestore.

2. CONTESTO NORMATIVO

[1]	Decreto Legislativo 7 marzo 2005, n° 82 e s.m.i.- Codice dell'amministrazione digitale
[2]	Decreto Legislativo 13 dicembre 2017 n. 217– Codice dell'amministrazione digitale (NUOVO CAD)
[3]	Decreto-legge 17 luglio 2020, n. 76, come convertito, con modificazioni, dalla legge 11 settembre 2020, n. 120 Misure urgenti per la semplificazione e l'innovazione digitale
[4]	D.lgs. 446/97 Albo concessionari art. 53 e art. 54
[5]	Regolamento UE n° 910/2014 – eIDAS (electronic IDentification Authentication and Signature) - identità digitale
[6]	ETSI EN 319 401, 319-411, 319-521, 319-522

[7]	Articolo 1, comma 402, della legge 27 dicembre 2019, n. 160
[8]	Decreto della Presidenza del Consiglio dei Ministri - Dipartimento per la trasformazione Digitale dell'8 febbraio 2022, n.58 (c.d. "Decreto Funzionamento")
[9]	Decreto del Ministro per la Trasformazione Digitale del 30 maggio 2022 dal titolo "Individuazione dei costi e dei criteri e modalità di ripartizione e ripetizione delle spese di notifica degli atti tramite la piattaforma di cui all'art. 26, comma 14 del decreto-legge 16 luglio 2020, n. 76" (c.d. "Decreto Costi")

3. DEFINIZIONI

Soggetti del servizio

Funzionario incaricato	Il soggetto che per primo accede alla piattaforma per conto del mittente al fine di predisporre le condizioni iniziali per l'impiego del sistema
Funzionario autorizzato	Il soggetto autorizzato ad operare sulla piattaforma per conto del mittente, ivi incluso il funzionario incaricato
Gestore della piattaforma	La società di cui all'articolo 8, comma 2, del decreto-legge 14 dicembre 2018, n. 135, convertito, con modificazioni, dalla legge 11 febbraio 2019, n. 12
PA Mittente	Le amministrazioni individuate dall'articolo 26, comma 2, lettera c), del decreto-legge n. 76 del 17 luglio 2020, come convertito, con modificazioni, dalla legge 11 settembre 2020, n. 120
Security Officer	Figura responsabile della gestione dell'attuazione delle pratiche di sicurezza prevista dalla norma ETSI EN 319 401 - REQ-7.2-15
System Administrator	Figura autorizzata a installare, configurare e mantenere i sistemi affidabili per la gestione del servizio prevista dalla norma ETSI EN 319 401 - REQ-7.2-15

System Operator	Figura responsabili della gestione dei sistemi affidabili. Autorizzato a eseguire il backup del sistema prevista dalla norma ETSI EN 319 401 - REQ-7.2-15
System Auditor	Figura autorizzata a visualizzare gli archivi e i registri di audit dei sistemi affidabili prevista dalla norma ETSI EN 319 401 - REQ-7.2-15
Identity Verification Officer	Figura responsabile di garantire che i processi effettivi condotti per verificare l'identità del mittente siano conformi al processo di verifica dell'identità definito prevista dalla norma ETSI EN 319 521 - REQ-QERDSP-7.2.2-01
PSP	Prestatore di Servizi di Pagamento
AgID	Agenzia per l'Italia Digitale

Autenticazione

Codice Fiscale (CF)	Codice alfanumerico o numerico che identifica univocamente rispettivamente le persone fisiche e le persone giuridiche e gli altri soggetti diversi dalle persone fisiche (es. associazioni non riconosciute), nei rapporti con la Pubblica Amministrazione. Si compone di 16 caratteri (alfanumerici) per le persone fisiche e di 11 caratteri (numerici) per le persone giuridiche e gli altri soggetti diversi dalle persone fisiche
SPID	Il Sistema Pubblico di Identità Digitale, disciplinato dall'articolo 64 del decreto legislativo 7 marzo 2005, n. 82

Consegna dei messaggi

Comunicazione	Processo end-to-end che inizia con il deposito, prosegue con l'invio e si conclude con la ricezione degli atti, documenti e/o

	informazioni da parte dei destinatari, che le PA Mittenti inoltrano ai Recapiti Certificati.
Invio	In questo documento, con il termine Invio si intende il momento in cui la PA Mittente ha completato la fase di deposito degli atti, documenti e/o informazioni oggetto del Recapito.
Ricezione	In questo documento, con il termine ricezione si intende il momento in cui gli atti, documenti e/o informazioni oggetto del Recapito sono effettivamente disponibili per il destinatario.
Certificazione di presa in carico	L'atto formato dal Gestore, con il quale si certifica l'acquisizione del documento informatico oggetto di invio. Certifica formalmente il corretto completamento da parte della PA Mittente del caricamento dati necessari per la comunicazione
Avviso di Avvenuta Ricezione (AAR)	Nel contesto del servizio SERCQ offerto all'interno di SEND l'avviso che attesta la disponibilità su SEND dei documenti da inviare

Componenti della trasmissione telematica

Identificativo Univoco della Notifica (IUN)	Il codice univoco attribuito dalla Piattaforma a ogni singola comunicazione effettuata dalle amministrazioni mittenti
Sigillo elettronico qualificato	Metodo matematico teso a dimostrare l'autenticità di un documento digitale autenticandone la persona giuridica che ne è l'autore
Marca Temporale	Evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile a terzi

Tipologie dei documenti a cui è possibile avere accesso su SeND	1. i Documenti, gli atti e/o tutte le altre informazioni caricati dalla PA Mittente e oggetto della comunicazione 2. le certificazioni opponibili a terzi generate da SEND (vedi paragrafo “Certificazione opponibile a terzi”)

4. DATI DEL GESTORE

Di seguito vengono riportati i dati dell’organizzazione che svolge la funzione di Gestore.

Denominazione e Ragione sociale	**PagoPA S.p.A.**
Referente	Alessio Biasutto in qualità di Direttore di Dipartimento Piattaforma Notifiche & Interoperabilità
Sede legale	Roma, Piazza Colonna 370, CAP 00187
Sede operativa	Roma, Via Sardegna 38, CAP 00187
Sito Web	https://www.pagopa.it/it/
PEC	pagopa@pec.governo.it

4.1. SITO WEB DEL GESTORE

I riferimenti del sito web di PagoPA sono:

- indirizzo web https://www.pagopa.it/it/prodotti-e-servizi/piattaforma-notifiche-digitali/ dove è possibile trovare le informazioni relative al servizio SEND erogato da PagoPA;
- indirizzo web https://cittadini.notifichedigitali.it → risorse WEB del portale SeND per le persone Fisiche
- indirizzo web https://imprese.notifichedigitali.it → risorse WEB del portale SeND per le persone Giuridiche.
- indirizzo web https://helpdesk.notifichedigitali.it → risorse WEB del portale per gli operatori di helpdesk di SeND

4.2. RESPONSABILITÀ DEL SERVICE PRACTICE STATEMENT, CONTATTO PER UTENTI E COMUNICAZIONI

Il responsabile dell'aggiornamento del presente Service Practice Statement è Federica Ciampa, responsabile del Servizio di Notifiche Digitali.

Domande, osservazioni e richieste di chiarimento in ordine al presente Service Practice Statement dovranno essere rivolte all'indirizzo di seguito indicato:

Responsabile Servizio Notifiche Digitali PagoPA
Roma, Piazza Colonna 370, CAP 00187
Indirizzo: info@pagopa.it

È disponibile un servizio di assistenza clienti, tramite omonimo link all'interno delle pagine della piattaforma, differenziati per target di clientela.

Il presente Service Practice Statement si riferisce al servizio di Notifiche Digitali di PagoPA come implementati dal Gestore, in osservanza alla normativa vigente ed elencata al capitolo "Contesto normativo".

4.3. AMMINISTRAZIONE DEL SERVICE PRACTICE STATEMENT

4.3.1. Procedure per l'aggiornamento

Il Gestore si riserva di apportare modifiche al Service Practice Statement per modifiche del Servizio in seguito ad adeguamenti normativi, per cambiamenti organizzativi e/o della infrastruttura tecnologica oltreché per miglioramenti del Servizio.

Ogni nuova versione annulla e sostituisce la precedente versione.

4.4. PUBBLICAZIONE

Ogni variazione al Service Practice Statement è sottoposta preventivamente all'approvazione di AgID. Il presente documento è consultabile, dai dipendenti della PA Mittente e dagli utenti destinatari, nel footer dei seguenti indirizzi Internet:

- https://selfcare.notifichedigitali.it
- https://login.notifichedigitali.it
- https://cittadini.notifichedigitali.it
- https://imprese.notifichedigitali.it

SEZIONE II: SERVIZIO DI NOTIFICHE DIGITALI (SEND)

5. DESCRIZIONE DEL SERVIZIO

5.1. CARATTERISTICHE GENERALI DEL SERVIZIO

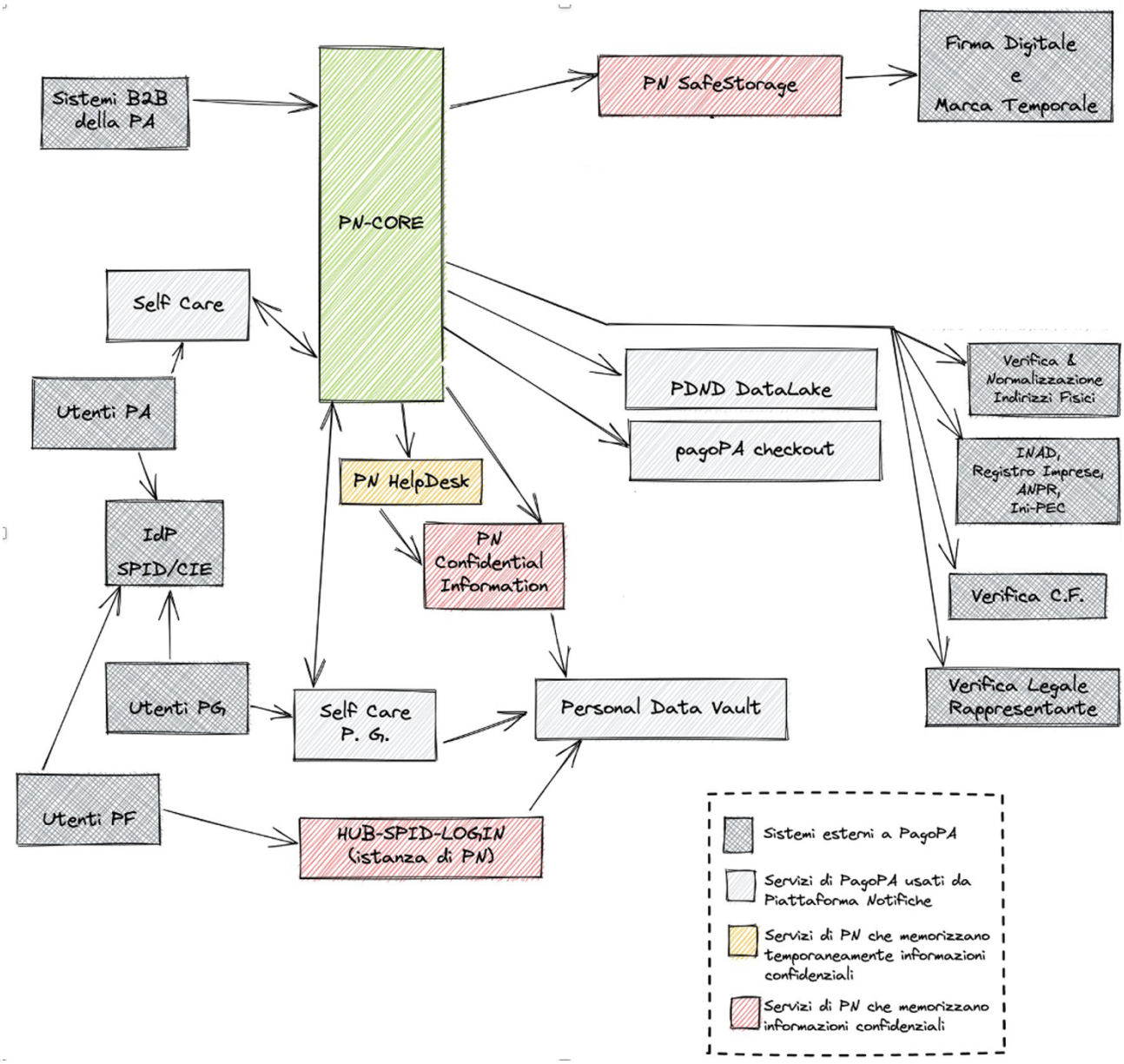
Servizio Notifiche Digitali (SEND) è un servizio di Recapito a valore legale che può essere utilizzato da qualsiasi PA Mittente per inviare atti a persone fisiche o giuridiche, enti od associazioni e ogni altro soggetto pubblico o privato titolari di Codice Fiscale attribuito ai sensi del D.P.R. n. 605/1973. SEND semplifica la gestione dell'invio delle comunicazioni per la PA Mittente che deve occuparsi del solo deposito sulla piattaforma dell'atto.

Le PA Mittenti possono utilizzare SEND solamente a valle della sottoscrizione di un accordo di adesione al servizio che comporta l'attivazione di un contratto di fornitura di servizio a titolo oneroso, servizio erogato da PagoPA S.p.A. alla PA Mittente.

L'utente invece, può usufruire del servizio SERCQ offerto all'interno di SEND esclusivamente attivando lo stesso all'interno del proprio profilo previa accettazione esplicita dei termini e delle condizioni del servizio SERCQ.

5.2. DEFINIZIONE APPLICATIVA DELLE COMPONENTI IL SERVIZIO

Di seguito l'architettura applicativa del servizio.



5.3. TIPOLOGIA DI QTSP COINVOLTI

Si ricorre ad un fornitore per Qualified Trusted Service di sigillo elettronico qualificato e marca temporale.

5.4. FIGURE CHIAVE DEL SERVIZIO

In conformità al requisito REQ-7.2-15 della ETSI EN 319 401, PagoPA ha provveduto alla nomina delle seguenti figure:

- Security Officer
- System Administrator
- System Auditor

- System Operator.

In conformità al requisito REQ-QERDSP-7.2.2-01 della ETSI EN 319 521, PagoPA ha provveduto alla nomina della seguente figura:

- Identity Verification Officer.

Le responsabilità di tali figure nell'ambito della gestione e del controllo del Servizio di Notifiche Digitali sono specificate nel "Piano della Sicurezza", cui si rimanda.

6. IL PROCESSO DI INVIO DELLE COMUNICAZIONI

Il processo di invio delle comunicazioni inizia con la PA Mittente che richiede a SEND di prendere in carico la documentazione oggetto dell'invio.

Questa operazione avviene in tre fasi: caricamento dei documenti, fornitura dei metadati del Recapito Certificato, verifica dei dati forniti.

Nella prima fase, la PA Mittente fornisce a SEND gli atti da inviare unitamente all'avviso PagoPA e/o ai metadati necessari per la generazione del modello F24, se previsto il pagamento da parte del destinatario. Gli atti devono essere in formato PDF e conformi a quanto richiesto dagli articoli 20 e 21 del CAD, perciò firmati digitalmente dalla PA mittente.

Nella seconda fase, la PA Mittente genera la richiesta di gestione dell'invio, fornendo i dati del destinatario (CF, indicazione del tipo di persona fisica o giuridica, nome e cognome o ragione sociale, indirizzo di domicilio o residenza, domicilio digitale se noto alla PA, Codice Avviso e Codice Fiscale dell'Ente creditore relativi all'avviso PagoPA), un numero di protocollo, l'oggetto dell'invio, importo e data di scadenza del pagamento (se presente), la lista dei documenti facenti parte dell'invio (attraverso gli identificativi forniti da SEND nella precedente fase) e l'hash SHA-256 dei documenti stessi. La PA Mittente può anche valorizzare facoltativamente un campo relativo all'oggetto con una descrizione; SEND ricevute queste informazioni, verifica che siano sintatticamente corrette e che non siano state utilizzate combinazioni di numero di protocollo (paProtocolNumber)/ID della PA (IdempotenceToken) oppure Codice Avviso/Codice Fiscale dell'Ente creditore già utilizzati in altri invii non annullati. Nel caso in cui le verifiche abbiano successo restituisce al mittente un token che servirà alla PA stessa per ricevere l'esito delle successive attività di verifica poste in essere da SEND.

È prevista anche la possibilità di inserire molteplici avvisi di pagamento (es. per gestire le rate della TARI), dando la possibilità al destinatario di selezionare l'avviso/i per i quali vuole procedere al pagamento.

Nella terza ed ultima fase, SEND verifica che lo SHA-256 fornito dalla PA coincida con quello calcolato da SEND a partire dai documenti allegati e che il destinatario indicato dalla PA sia un soggetto che ha attivato il servizio di SERCQ di SEND. Inoltre SEND effettua una serie di verifiche sulla correttezza dei metadati prodotti dalla PA Mittente.
Se le verifiche hanno successo, SEND genera lo IUN che viene restituito alla PA Mittente unitamente al token generato al momento di presa in carico dei documenti oggetto di invio. Con la presa in carico SEND garantisce l'invio delle comunicazioni. SEND genera una certificazione opponibile a terzi contenente le informazioni relative alla data e all'ora in cui la PA Mittente ha messo a disposizione del Gestore i documenti relativi ad un invio avente un determinato IUN.
Nel caso in cui, invece, le verifiche non abbiano successo, SEND informa la PA della presenza di errori nella richiesta inoltrata inviando un codice di errore unitamente al token generato al momento dell'invio.
Una volta che lo IUN è stato prodotto, SEND genera un AAR; lo stesso contiene le informazioni relative all'avvenuto deposito su SEND dei documenti, il suo IUN e la messa a disposizione del destinatario. Dopo 7 giorni dalla generazione dell'AAR si presume il perfezionamento della ricezione.
Per i destinatari che hanno attivato il servizio SERCQ di SEND, il deposito dei documenti in piattaforma da parte della PA Mittente e la generazione del certificato di presa in carica e dell'AAR terminano il processo di comunicazione a valore legale.
SEND può informare il destinatario della presenza di una nuova comunicazione attraverso l'invio di messaggi di cortesia verso recapiti digitali privi di valore legale. Il destinatario ha la possibilità di scegliere l'AppIO, un'email o un numero di cellulare forniti a SEND dal destinatario all'interno del proprio profilo per questo tipo di comunicazioni.
Le comunicazioni saranno considerate ricevute dal destinatario dopo 7 giorni dalla disponibilità dell'AAR presso il SERCQ. In particolare, se l'AAR è reso disponibile al destinatario dopo le ore 21.00, il termine di 7 giorni indicato in precedenza per il perfezionamento si computa a partire dal giorno successivo (art. 26 comma 9 n. 1 lettera b) D.L. 76/2020).
Il destinatario può accedere alle comunicazioni ricevute autenticandosi sul portale di SEND, utilizzando la propria identità digitale e selezionando la comunicazione in base al relativo IUN e quindi accedendo ai documenti scaricabili dal portale. Il destinatario ha inoltre la possibilità di accedere alle certificazioni opponibili a terzi attraverso i singoli link presenti nella sezione "Stato del recapito".

Nel caso in cui l'accesso ai documenti ricevuti avvenga prima dello scadere dei 7 giorni successivi al deposito dell'AAR, questo accesso perfeziona la ricezione per il destinatario.
I documenti trasmessi dalla PA mittente vengono conservati per 120 giorni a partire dalla data di perfezionamento della Ricezione per il destinatario.

6.1. SPECIFICHE TECNICHE DEI PDF ALLEGATI ALLA COMUNICAZIONE

I documenti pdf allegati alla Comunicazione devono presentare una serie di caratteristiche tecniche, volte a permetterne la corretta elaborazione digitale. È responsabilità della PA mittente garantire che i documenti siano aderenti a queste note tecniche.
I documenti inviati devono essere file pdf con le seguenti caratteristiche:

- Adobe PDF/A
- Le dimensioni "fisiche" della pagina devono essere conformi al formato A4 (210 x 297 mm)
- Al fine di regolare gli opportuni trattamenti di eventuali stampe fisiche viene imposta un'area di sicurezza" che regola lo spazio effettivamente utilizzabile per la stampa dei documenti da inoltrare". Tale area di sicurezza è definita in 1 (uno) centimetro per lato su un foglio di dimensioni standard A4 e dovrà essere lasciata libera a cura del cliente.

Come insieme minimo di regole di partenza si faccia riferimento allo standard PDF/A definito nelle raccomandazioni ISO 19005-1:2005, a cui nel prosieguo verranno aggiunti ulteriori vincoli volti a garantire la produzione di stampe di qualità adeguata (a titolo di esempio, lo standard ISO 19005-1:2005 considera adeguata una risoluzione delle immagini a 50 dpi, ma questa porta a stampe industriali di pessima qualità, per questa ragione, verrà richiesta una risoluzione maggiore).
Le dimensioni della pagina (e dimensioni della CROPBOX, TRIMBOX, ARTBOX e MEDIABOX) devono essere in formato A4 portrait (210 mm x 297 mm).
Non sono consentiti oggetti, anche se non contenenti grafica stampabile, fuori dalla media box.
I file PDF che possono essere accettati devono possedere le seguenti caratteristiche:

- PDF standard Adobe raccomandati PDF/X-3:2003 compliant
- Risoluzione delle immagini pari a 300 dpi (si sconsiglia di eccedere tale valore per non appesantire i flussi o di scendere sotto tale soglia per non degradare l'immagine)
- Nessuna protezione applicata, nessuna encryption

- Non sono ammessi elementi non strettamente testuali o grafici, come ad esempio note, commenti, file audio, multimediali, evidenziazioni, annotazioni, macro, script e così via
- Proibita la trasparenza
- Evitare Clipping Path
- Non usare per quanto possibile elementi grafici che si sovrappongono (totalmente o parzialmente)
- Fare in modo che il testo sia sempre reindirizzato per ultimo (sopra tutto il resto)
- Il testo nero così come elementi grafici come barcode e datamatrix qualora definiti con informazione di colore devono essere definiti come 100% black (CMYK (0,0,0,100) e quindi 0% delle altre componenti cromatiche)
- Non sono ammesse pagine contenenti più di 1000 elementi
- Ridurre in generale la complessità delle pagine, ridurre al minimo gli anchor points, I layer non sono consentiti
- Total Area Coverage massimo 220% per carta standard
- Evitare di creare linee sottili o testo sottile con colori composti in quanto potrebbero verificarsi fenomeni di sfocatura, meglio utilizzare in questi casi un colore base e.g. CMYK (0,100,0,0)
- Non inserire profili (e.g. profili ICC) all'interno delle risorse grafiche e immagini in genere
- Non utilizzare scaling
- Non usare drop shadow style nel testo
- Non utilizzare Alternate Image, Embedded Page Thumbnails e JavaScript
- Proibiti pdf mono-documento, creare invece un PDF unico multi-documento che sia autoconsistente cioè contenga tutte le risorse necessarie e mettendo a fattor comune le risorse stesse evitando proliferare di risorse ripetute o spezzettate e sparse nel file
- Raggruppare il testo in entità ampie, righe o paragrafi, per favorire le performance.

Le immagini e gli oggetti grafici contenuti nei file PDF devono:

- Rispettare le dimensioni massime della pagina
- Rispettare i margini della pagina senza fuoriuscire dalla cropbox e dalla media

- box per nessuna componente anche priva di grafica
- Avere una risoluzione di 300 dpi
- Essere sempre nel numero minimo indispensabile (ad es., evitare di disegnare una tabella utilizzando tante piccole righe a comporre le celle ognuna delle quali è un oggetto grafico distinto e separato)
- Ridurre la complessità, ridurre eccessivo uso di anchor points, evitare vector patterns complessi (eventualmente convertirli), ridurre al minimo il numero di layer e di risorse grafiche
- Per le stampe in b/n, si consiglia di evitare sfondi grigi ed in generale sfumature di grigio poiché potrebbero non essere resi in modo soddisfacente
- Evitare l'uso di righe troppo sottili (inferiori o superiori di poco al punto tipografico) che potrebbero non essere rese alla risoluzione di stampa standard
- Evitare la rotazione o lo scaling delle immagini ed in genere di oggetti rasterizzati
- Evitare di inserire oggetti grafici a tutta pagina, per esempio evitare di inserire una risorsa a tutta pagina A4 che contengano la grafica di solo logo e footer e tutti il resto bianco; in questi casi si richiede al cliente di spezzare le due risorse in grafiche più piccole e che contengano solo quanto necessario.

Gli algoritmi di compressione degli stream (es. immagini) supportati sono:

- LZW
- ZIP da verificare
- NON usare JPEG2000 e JBig2
- Raccomandati TIFF con LZW (non usare per TIFF la compressione 8)
- L'utilizzo di immagini JPEG a seconda della qualità rende necessario ridurre a 100 il numero massimo di immagini per file.

L'uso di font outline (vettoriali) è preferibile in quanto la quantità di dati trasmessa con il documento è inferiore rispetto alla trasmissione di font bitmap. Si richiede:

- Utilizzare solo Font totalmente incorporati di tipo Type1 (outline) con encoding WinISO Encoding Latin1 (MS Windows 1252 Latin1)
- Evitare i font Type 3, Outline Bitmap e All And None
- Minima font size 6pt

- Non è ammesso l'uso della funzione di scaling (sia horizontal che vertical scaling) né sulle stringhe di testo né sull'intera pagina; non sono altresì ammesse altre funzioni di trasformazione dei font (skew, ecc.)
- I font utilizzati, anche quelli standard, devono essere totalmente incorporati all'interno del PDF (senza subsetting), font non presenti anche se standard potrebbero dare luogo ad una stampa non corretta
- I font utilizzati devono essere inclusi nel PDF una volta sola (no ripetizioni, no frammentazioni)
- Font uguali devono avere nomi uguali
- Limitare comunque il numero di font utilizzati nel PDF, il numero di font concesso verrà valutato sulla base degli esiti dei test preliminari a seconda delle caratteristiche del flusso
- Definire il testo colorato sempre come font senza convertirlo in immagine
- Font CID con grande numero di caratteri sono da valutare caso per caso per garantire le performance di velocità di stampa.

Nel caso di utilizzo all'origine di font con codifica diversa da WinISO Encoding (MS Windows 1252 Latin1), non viene garantita la conformità del prodotto finale stampato rispetto alla presentazione su video del documento stesso operata tramite Adobe Reader o altri visualizzatori PDF.

7. COMPRENDERE LO STATO DELLA COMUNICAZIONE E I DOCUMENTI DISPONIBILI SUL PORTALE

L'invio delle comunicazioni segue un ciclo di vita che la fa transitare lungo una serie di stati che vengono tracciati e visualizzati sul portale di SEND nella sezione Stato della Comunicazione disponibile visualizzandone il dettaglio.

La timeline presenta inizialmente solamente gli eventi che determinano un cambiamento di stato della Comunicazione. Eventi secondari sono disponibili aprendo le sezioni "Mostra di più". Eventuali documenti collegati agli eventi secondari sono disponibili anche attraverso i link presenti negli eventi principali.

Per i diversi stati sono disponibili attraverso link i relativi certificati opponibili a terzi aventi valore legale. In alcuni casi molteplici eventi fanno riferimento alla stessa certificazione opponibile a terzi.

7.1. RECAPITO DIGITALE SERCQ

Il percorso di Recapito Digitale per destinatari che hanno attivato il servizio SERCQ di SEND prevede le seguenti fasi:

- Presa in carico: la PA mittente richiede di effettuare l'invio
- Perfezionamento per mittente: la richiesta è accettata da SEND
- Creazione dell'AAR per il destinatario sul SERCQ
- Perfezionamento per destinatario: indica il momento in cui la ricezione si è perfezionata per il destinatario, in qualsiasi circostanza questo avvenga
- Primo accesso all'atto ricevuto da parte del destinatario
- Inizio e Fine di eventuali malfunzionamenti della piattaforma che rendano impossibile l'inoltro telematico, da parte dell'amministrazione, dei documenti informatici, ovvero l'accesso, il reperimento, la consultazione e l'acquisizione dei documenti informatici messi a disposizione.

7.2. DESTINATARI MULTIPLI

Esistono casi nei quali l'invio delle comunicazioni deve essere indirizzato a più di un destinatario (comunicazione multi-destinatario). In questo caso la timeline contiene informazioni sui processi di invio intrapresi per ciascun destinatario, ciascuno di essi raggiunto con le modalità proprie derivanti dalle informazioni in possesso di SEND. Il perfezionamento della Ricezione avviene indipendentemente per ciascun destinatario.

Nello Stato della Comunicazione multi-destinatario al quale accede la PA Mittente sono visibili i diversi stati attraversati e le relative certificazioni opponibili a terzi, comprese le informazioni sugli eventi di dettaglio per singolo destinatario.

Occorre precisare che nello Stato della Comunicazione multi-destinatario visibile per il singolo destinatario, nel caso in cui il passaggio da uno stato all'altro sia prodotto da azioni compiute da un altro dei destinatari, gli stessi hanno una valenza puramente informativa, senza informazioni su chi ha scatenato un determinato evento (se diverso da sé stesso) e senza la possibilità di scaricare le relative attestazioni.
Questo perché un destinatario può visualizzare e/o avere disponibilità solo delle sue informazioni e/o delle sue certificazioni.

7.3. STATO DELLA COMUNICAZIONE

Gli stati attraverso i quali inizia e si conclude il processo di Invio / Ricezione, sono i seguenti:

- **Depositata**: quando l'invio risulta correttamente eseguito dalla PA; tale stato iniziale determina il perfezionamento per il mittente e genera la certificazione opponibile a terzi di presa in carico;
- **Perfezionata per decorrenza termini**: quando la Ricezione si è perfezionata per decorrenza termini (a norma di legge) per almeno un destinatario e se nessuno dei destinatari ha preso visione delle informazioni recapitate nei 7 giorni successivi il deposito
- **Avvenuto accesso**: quando almeno un destinatario, entro od oltre i termini di decorrenza, ha acceduto agli atti recapitati
- **Annullata**: nel caso l'invio sia stato annullato della PA Mittente.

Per i destinatari che hanno attivato il servizio SERCQ di SEND, il termine di perfezionamento previsto per legge (art. 26 DL 76/2020) corrisponde al settimo giorno successivo alla data di creazione dell'AAR e quindi della sua disponibilità in piattaforma per il destinatario. Se l'AAR è reso disponibile al destinatario dopo le ore 21.00, il termine di sette giorni si computa a decorrere dal giorno successivo.
In ogni caso, quando il destinatario accede alle informazioni recapitate per la prima volta tramite la piattaforma, SEND genera la certificazione opponibile a terzi indicante la data e l'ora di avvenuto accesso e lo Stato della Comunicazione in time line è quello di "Avvenuto accesso". Se questo accesso avviene prima del termine dei 7 giorni dalla messa a disposizione dell'AAR, l'accesso perfeziona il Recapito per il destinatario.
Nel caso di destinatari multipli, lo stato aggregato ha solamente valenza informativa sullo stato complessivo della Ricezione.
In particolare, lo stato di perfezionamento può non corrispondere all'effettiva data di perfezionamento per ogni diverso destinatario.

7.4. CERTIFICAZIONE OPPONIBILE A TERZI

Le certificazioni opponibili a terzi sono dei file in formato PDF, sigillati elettronicamente da PagoPA con Sigillo Elettronico Qualificato così come definito dal CAD e dotati di marcatura temporale certificata. Queste caratteristiche garantiscono l'irripudiabilità e l'immodificabilità delle certificazioni. Le stesse sono conservate a norma per 10 anni.

Le certificazioni sono rese disponibili per Mittente e Destinatario all'interno delle rispettive sezioni "Stato della Comunicazione".

Le certificazioni vengono generate al verificarsi di alcuni eventi rilevanti per l'Invio / Ricezione ed hanno il formato descritto nei paragrafi seguenti.

7.4.1. Certificazione opponibile a terzi: presa in carico

La certificazione viene generata alla conclusione dei passaggi di deposito su SEND ed è associata allo stato "Depositata".

In caso di Invio multi-destinatario, la certificazione è unica e visibile per tutti i co-destinatari.

7.4.2. Certificazione opponibile a terzi: avvenuto accesso

La certificazione viene generata quando il destinatario accede alla documentazione recapitata (secondo le modalità previste) ed è associata allo stato "Avvenuto Accesso".

Nel caso di Invio multi-destinatario, la certificazione attesta l'avvenuto accesso per ciascun destinatario e, quindi verranno generate tante certificazioni quanti sono i destinatari e ciascuno di essi avrà a disposizione/visibilità esclusivamente della propria. Mentre il Mittente le avrà tutte a disposizione.

7.4.3. Certificazione opponibile a terzi: malfunzionamento e ripristino

La certificazione viene generata nei casi di disservizio della piattaforma, previsti dalla norma di funzionamento, che rendano impossibile l'inoltro telematico, da parte dell'amministrazione, dei documenti informatici oggetto di invio, ovvero l'accesso, il reperimento, la consultazione e l'acquisizione dei documenti informatici messi a disposizione; ed è disponibile nelle informazioni relative al dettaglio della comunicazione nella sezione "Altri documenti".

In caso di Invio multi-destinatario, la certificazione è unica e visibile per tutti i destinatari.

8. MITTENTE

Le PA sono gli utenti di SEND che possono inviare le comunicazioni sia manualmente attraverso il portale web, sia in modalità automatica attraverso integrazione B2B. Le PA Mittenti possono essere, ovviamente, anche destinatari di Comunicazioni; in questo caso la PA segue il flusso previsto per le persone giuridiche (cfr. capitolo dedicato alle persone giuridiche).

8.1. ONBOARDING TRAMITE AREA RISERVATA PORTALE SELFCARE

Per poter depositare gli atti, documenti e/o informazioni oggetto di Invio su SEND, una PA Mittente deve per prima cosa completare il processo di onboarding nell'Area Riservata messa a disposizione da PagoPA attraverso il portale SelfCare[1].

Il processo di onboarding si articola come segue.

8.1.1. Richiesta di adesione

Una PA può richiedere di aderire al servizio tramite il sito vetrina di SEND (sezione Enti/Documenti/Aderisci a SEND). Da qui il referente dell'Ente viene indirizzato sul Portale Self Care.

8.1.1.1. Accesso all'area riservata

Una volta reindirizzata sul Portale Self Care, la PA mittente può accedere con una delle seguenti modalità:

- Autenticazione mediante SPID (Sistema Pubblico di Identità Digitale);
- Autenticazione mediante CIE (Carta d'Identità Elettronica).

8.1.1.2. Compilazione Della Richiesta

Il referente seleziona l'Ente (che deve essere censito su IPA) per cui attivare la richiesta di adesione al servizio. Una volta che la richiesta è stata inviata correttamente, l'Ente riceve al proprio indirizzo PEC (domicilio digitale censito su IPA) una PEC mail contenente l'Accordo di Adesione (disponibile come allegato) e le istruzioni per completare l'adesione.

Il funzionario munito di poteri di firma, individuato dall'ENTE, compila l'Accordo di Adesione auto dichiarando il suo ruolo e le sue responsabilità nell'ambito dell'Accordo e sottoscrivendo lo stesso con firma digitale fornita dalla PA. Una volta compilato e sottoscritto, l'Accordo verrà caricato attraverso l'utilizzo del link ricevuto via PEC

[1] portale B2B web dedicato a tutti gli enti che collaborano con PagoPA, coincide con l'Area Riservata dell'Ente

8.1.1.3. Accesso amministratori

Una volta completata la fase di onboarding, l'/gli Amministratore/i (censiti all'interno dell'Accordo di Adesione) potranno autenticarsi attraverso SPID o CIE all'Area Riservata e da questa accedere a SEND nei ruoli di Referente amministrativo. Potranno inoltre identificare altre persone alle quali consentire l'accesso a SEND come Referente amministrativo.

Questo meccanismo permette di associare ad una PA Mittente le persone individuate come rappresentanti dell'Ente e di conseguenza attribuire alla PA Mittente tutte le azioni effettuate da tali rappresentanti, in particolare la creazione di Comunicazioni sia attraverso gestione manuale che tramite API.

8.1.2. Rimozione del mittente da SEND

Il processo di rimozione della PA come mittente su SEND avviene in due modalità diverse: cessazione richiesta dalla PA o da PagoPA S.p.A.

8.1.2.1. Cessazione richiesta dalla PA

Nel caso in cui sia la PA Mittente a richiedere la cessazione dell'operabilità su SEND, il processo avviene attraverso la sezione dedicata a SEND nell'Area Riservata sul portale SelfCare dove un Referente Amministrativo accede selezionando dapprima la PA Mittente per cui opera, dando inizio al processo di cessazione richiedendo l'invio della lettera di De-registrazione, dove saranno indicati gli estremi del soggetto firmatario (nome, cognome, codice fiscale ed e-mail del soggetto firmatario operante nella qualità di Rappresentante Legale e/o un suo procuratore speciale).

La lettera di De-registrazione è inviata al domicilio digitale della PA mittente ed indica due istanti temporali: l'istante di cessazione dei servizi di SEND per la PA Mittente (90 giorni successivi al ricevimento della lettera di cessazione controfirmata) e l'istante di cessazione dell'accesso da parte della PA ai dati residenti su SEND e relativi alla PA (180 giorni successivi alla cessazione dei servizi).

Il funzionario munito di poteri di firma, individuato dall'ENTE, compila la lettera di De-registrazione auto dichiarando il suo ruolo e le sue responsabilità nell'ambito dell'accordo, sottoscrivendo la stessa con firma digitale fornita dalla PA e caricandola sul portale.

PagoPA S.p.A. verifica tecnicamente l'esistenza e la validità della firma digitale ei poteri di rappresentanza del firmatario verificando la corrispondenza con i dati dichiarati dallo stesso all'interno della lettera di De-registrazione. In caso di riscontro positivo delle verifiche di cui sopra, per il periodo di preavviso che avrà durata di 90 giorni solari,

l'attività della PA Mittente su SEND non subirà variazioni. Per i successivi 180 giorni, decorrenti quindi dal termine del già menzionato periodo di preavviso, la PA Mittente avrà accesso in sola visualizzazione.

Precedentemente all'istante di cessazione dei servizi, tutto si svolge come se la PA non avesse iniziato il processo di rimozione.

Dopo l'istante di cessazione dei servizi ma prima dell'istante di cessazione dell'accesso, gli utenti abilitati della PA possono continuare ad accedere a SEND ma sono disabilitate tutte le operazioni che modificano lo stato di SEND: non è quindi possibile inviare nuove Comunicazioni o apportare modifiche alla configurazione.

Dopo l'istante di cessazione dell'accesso, gli utenti abilitati della SEND non possono più accedere a SEND nei ruoli di referente amministrativo o tecnico della PA.

SEND preserva le informazioni di configurazione della PA fino a quando sono presenti a sistema Comunicazioni inoltrate dalla PA stessa. Nel caso la PA effettui una nuova procedura di onboarding queste informazioni vengono ripristinate.

8.1.2.2. Cessazione richiesta da PagoPA S.p.A.

Alle condizioni previste nei ToS, PagoPA può intraprendere misure volte alla sospensione o interruzione dei servizi. Il processo si svolge all'esterno del portale SelfCare e, una volta definite le relative tempistiche, la sospensione/interruzione viene gestita dal personale di supporto tecnico di SEND.

8.2. ACCESSO REFERENTE TECNICO / OPERATORE

Il Referente Tecnico / Operatore accede a SEND nelle stesse modalità previste per il Referente amministrativo (autenticandosi tramite SPID / CIE).

Una volta effettuato l'accesso il Referente tecnico di una PA mittente ha la possibilità di gestire gli invii, sia manualmente che tramite API B2B, e visualizzare tutte le Comunicazioni inviate, comprese quelle inviate manualmente. Non ha la possibilità di gestire gli utenti e i gruppi.

8.2.1. Utilizzo di SEND attraverso API B2B

PagoPA fornisce un insieme di API che permettono l'integrazione dei sistemi gestionali della PA mittente con SEND per ottenere, dove necessario, la gestione automatica delle Comunicazioni.

Tutte le API B2B di SEND prevedono, per essere utilizzate, un'interazione conforme alle indicazioni per le tecnologie accolte dal Modello di Interoperabilità (ModI) e specificate nelle Linee Guida sull'infrastruttura tecnologica della Piattaforma Digitale Nazionale Dati

per l'interoperabilità dei sistemi informativi e delle basi di dati. Pertanto, i fruitori di tale servizio dovranno ottenere il Voucher atto a confermare l'applicazione dei corretti Requisiti di Fruizione del servizio. SEND ne verificherà l'autenticità e il corso di validità prima di restituire le informazioni legittimamente richieste dal fruitore

Per abilitare le API B2B a specifici gruppi di notifiche, sempre come previsto dal Modello di Interoperabilità (ModI) e specificate nelle Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni – Pattern di sicurezza, è richiesto in particolare l'utilizzo di AUDIT_REST_01.

9. DESTINATARI

Le persone fisiche e le persone giuridiche che hanno attivato il servizio di SERCQ di SEND possono essere destinatarie di Comunicazioni da parte delle PA.

9.1. ACCESSO A SEND DA PARTE DELLE PERSONE FISICHE

Una persona fisica accede a SEND all'indirizzo https://cittadini.notifichedigitali.it autenticandosi con la sua identità digitale SPID / CIE.

Al primo accesso l'utente deve confermare la presa visione dei termini di servizio (ToS) e dell'informativa privacy generici per la piattaforma SeND.

All'interno della sezione profilo l'utente può manifestare l'intenzione di attivare SEND come servizio di SERCQ.

L'utente ha così accesso all'Area Riservata di SEND per gestire le proprie Comunicazioni ricevute.

9.2. ACCESSO A SEND DA PARTE DELLE PERSONE GIURIDICHE

In questa sezione con "persone giuridiche" (di seguito anche PG) intendiamo riferirci ai destinatari di Comunicazioni che non sono configurabili come persone fisiche. In questa accezione intendiamo quindi le persone giuridiche, gli enti, le associazioni e ogni altro soggetto pubblico o privato, residenti o aventi sede legale nel territorio italiano ovvero all'estero, ove titolari di codice fiscale attribuito ai sensi del decreto del Presidente della Repubblica 29 settembre 1973, n. 605. La persona giuridica non accede a SEND direttamente ma tramite una persona fisica, nello specifico, il Legale Rappresentante, il quale procede poi ad abilitare altri utenti all'utilizzo di SEND.

In questa sezione descriviamo quello che le persone fisiche che accedono per conto di una persona giuridica possono effettuare.

9.2.1. Accesso a SEND del Legale Rappresentante

Il Legale Rappresentante accede a SEND attraverso l'Area Riservata messa a disposizione da PagoPA sul portale persone giuridiche (https://imprese.notifichedigitali.it/): il Legale Rappresentante accede identificandosi attraverso SPID/CIE.

Attraverso l'interrogazione dei Registri Pubblici viene restituito l'elenco delle persone giuridiche di cui risulta essere il Legale Rappresentante; passaggio successivo è la scelta da parte del Legale Rappresentante della persona giuridica per la quale intende accedere alle comunicazioni ricevute su SEND.

Al primo accesso l'utente deve confermare la presa visione dei termini di servizio (ToS) e dell'informativa privacy generici per la piattaforma SeND.

All'interno della sezione "Profilo" l'utente può manifestare l'intenzione di eleggere SEND come servizio di SERCQ della PG rappresentata.

Prima di attivare il servizio l'utente deve confermare la presa visione dei termini di servizio (ToS) e dell'informativa privacy specifici per il servizio SERCQ.

9.2.2. Accesso a SEND di un dipendente della persona giuridica

Il dipendente della persona giuridica accede a SEND all'indirizzo https://imprese.notifichedigitali.it autenticandosi con la sua identità digitale.

Al primo accesso l'utente deve confermare la presa visione dei termini di servizio (ToS) e dell'informativa privacy.

SEND verifica che il soggetto che ha effettuato l'accesso abbia un ruolo tra quelli previsti e sopra descritti, assegnato dal Legale Rappresentante per la relativa persona giuridica; solo se la verifica ha esito positivo gli è consentito operare per conto di essa.

Operando per conto della persona giuridica, la persona designata accede con le restrizioni legate al suo ruolo.

9.3. USCITA DA SEND

Selezionando il proprio nome e cognome/ denominazione posto in alto a destra nella pagina viene mostrato un menu che contiene, oltre alla voce che permette di visualizzare i dati estratti da SPID o CIE, anche una voce che permette all'utente di uscire da SEND. Per operare nuovamente, l'utente dovrà effettuare nuovamente l'accesso.

10. CONDIZIONI DI FORNITURA

10.1. ONEROSITÀ DEL SERVIZIO

Il costo della Comunicazione si determina sulla base di quanto previsto dal Decreto 30 maggio 2022 «Individuazione dei costi e dei criteri e modalità di ripartizione e ripetizione delle spese di notifica degli atti tramite la piattaforma di cui all'art. 26, comma 14 del decreto-legge 16 luglio 2022, n. 76». Tale decreto considera due componenti di costo. La prima componente, a copertura dei costi di gestione sostenuti da PagoPA S.p.A., è indicata in € 1,00. La seconda componente a copertura dei costi, sostenuti dai mittenti, per l'elaborazione degli atti, provvedimenti e avvisi oggetto di Comunicazione, per il relativo deposito sulla piattaforma e per la gestione degli esiti della Comunicazione, è indicata in € 1,00. Questa seconda componente non è prevista per la Comunicazione degli atti dell'amministrazione finanziaria e dell'agente della riscossione.

SEND permette alla PA - Mittente di definire, all'atto della creazione di ciascuna Comunicazione, se il costo da ripetere al cittadino sia calcolato alla luce del Decreto citato nel precedente paragrafo o se debba essere calcolato in modo forfettario. Questo secondo caso si applica in caso di leggi speciali relative a particolari Comunicazioni o nel caso in cui la PA - Mittente voglia farsi carico integralmente dei relativi costi.

In ogni caso SEND fatturerà alla PA mittente le spese effettive sostenute per ciascun destinatario. In caso di destinatari multipli, il pagamento sarà reso disponibile a tutti i destinatari fino al pagamento effettuato da parte di uno di essi (il primo che effettua il pagamento). I costi sostenuti per raggiungere gli altri destinatari dovranno essere riscossi dalla PA - Mittente in autonomia.

SEND fornisce alla PA - Mittente indicazione precisa delle diverse componenti del costo così come previste nel Decreto.

Per permettere la corretta determinazione del costo, SEND mette a disposizione della PA - Mittente una specifica API che, fornendo Codice Avviso e Codice Fiscale dell'Ente creditore per il pagamento, restituisce il costo della Comunicazione e la data di perfezionamento per il destinatario della stessa. Queste stesse informazioni possono essere dedotte dalla PA - Mittente a partire dalle informazioni relative allo stato della Comunicazione fornite da SEND ma, non essendo queste informazioni disponibili in tempo reale, la modalità corretta di gestione dell'attualizzazione del costo è quella di effettuare tale attualizzazione all'atto del pagamento ed utilizzando l'API menzionata precedentemente. Per gli intermediari tecnologici della piattaforma PagoPA che adottano la modalità asincrona di aggiornamento della posizione debitoria è invece

disponibile l'opzione di attualizzazione gestita direttamente da SEND integrata nativamente con PagoPA.

È responsabilità della PA - Mittente utilizzare gli strumenti messi a disposizione da parte di SEND per attualizzare correttamente, prima del suo pagamento, la posizione debitoria eventualmente associata ad una Comunicazione. Non sono imputabili a PagoPA S.p.A. errati pagamenti dovuti all'errata attualizzazione delle posizioni debitorie.

Per permettere una corretta gestione dei pagamenti effettuati al di fuori di SEND, la PA - Mittente deve informare SEND dell'avvenuto pagamento appena ne viene a conoscenza.

SEZIONE III: OBBLIGHI E RESPONSABILITÀ

11. OBBLIGHI E RESPONSABILITA'

11.1. OBBLIGHI DEL GESTORE

- Genera il Certificato di presa in carico e l'AAR
- Contrassegna con uno IUN, codice univoco attribuito dalla piattaforma, ogni singola Comunicazione inviata dalle amministrazioni
- Permettere alle amministrazioni di rendere disponibili telematicamente sulla piattaforma i documenti informatici (atti, provvedimenti, avvisi e comunicazioni) corrispondenti all'Invio
- Assicura l'autenticità, l'integrità, l'immodificabilità, la leggibilità e la reperibilità dei documenti informatici resi disponibili dalle amministrazioni
- Identifica gli utenti attraverso gli strumenti di autenticazione forte SPID e CIE
- Assicura ai destinatari l'accesso alla piattaforma per il reperimento, la consultazione e l'acquisizione dei documenti informatici oggetto di Comunicazione
- Permette ai destinatari di recuperare i documenti informatici resi disponibili dalle amministrazioni corrispondenti alla Comunicazione inviata
- Rendere disponibile al destinatario l'AAR, per ogni atto, provvedimento, avviso o comunicazione inviata
- Formare e rendere disponibili sulla piattaforma, alle amministrazioni e ai destinatari, le relative certificazioni opponibili a terzi
    a) alla data di messa a disposizione dei documenti informatici sulla piattaforma da parte delle amministrazioni;
    b) alla data in cui il destinatario ha avuto accesso al documento informatico oggetto della Comunicazione;
    c) al periodo di malfunzionamento della piattaforma e alla data di ripristino delle funzionalità della piattaforma.

11.2. OBBLIGHI DELL'UTENTE (PA - MITTENTE, DESTINATARI PG E PF)

- Accettare i termini e le condizioni del servizio di Recapito Certificato erogato dalla Piattaforma e rispettarli in ogni momento.
- Utilizzare la Piattaforma esclusivamente per gli scopi autorizzati e in conformità alla legge applicabile.
- Non utilizzare, direttamente o indirettamente, la Piattaforma:

- sfruttando l'identità di un'altra persona o implicando l'utilizzo non personale delle funzionalità della Piattaforma, salvo quando eventualmente ed espressamente previsto;
- per comunicare dati o informazioni false, ingannevoli o illecite;
- per trasmettere virus, malware o altri codici dannosi per qualsivoglia dispositivo o sistema;
- in violazione dei diritti del Gestore o di terzi;
- per finalità o scopi commerciali;
- in modo illecito, diffamatorio, osceno, volgare, intimidatorio, offensivo nei confronti della Società o di terzi;
- per trasmettere comunicazioni illeciteo non autorizzate, quali messaggi massivi, spam o messaggi automatici.

11.3. OBBLIGHI TERZE PARTI

PagoPA identifica i fornitori critici per il servizio di Recapito Certificato e definisce e concorda in fase contrattuale gli obblighi degli stessi e i relativi livelli di servizio, finalizzati a garantire la sicurezza delle informazioni trattate nel rispetto delle policy e delle procedure del sistema di gestione aziendale, formalizzandoli negli accordi contrattuali stipulati tra le parti, con particolare riferimento a quelli inerenti la confidenzialità, l'integrità e la disponibilità delle informazioni, anche in condizioni di crisi.

12. ESCLUSIONI E LIMITAZIONI DI RESPONSABILITÀ

Qualsiasi contestazione relativa all'esecuzione del Servizio dovrà essere comunicata per iscritto dal Cliente a PagoPA tramite raccomandata A/R all'indirizzo Via Sardegna 38, 00187 Roma o PEC all'indirizzo pagopa@pec.governo.it.

PagoPA non sarà responsabile per i danni conseguenti ad un utilizzo non conforme del servizio.

PagoPA sarà responsabile per i danni subiti dal Cliente imputabili a titolo di dolo o colpa.

13. POLIZZA ASSICURATIVA

PagoPA ha stipulato un contratto assicurativo per la copertura dei rischi dell'attività e dei danni cagionati per dolo o colpa a terzi nell'esercizio dell'attività di Gestore di SEND, ai sensi del DPR 11 febbraio 2005, n° 68, con i massimali:

- € 1.000.000,00[2] euro per evento dannoso assicurato (con franchigia di € 10.000,00)

[2] la Somma Assicurata rappresenta il limite massimo di risarcimento per evento e per anno assicurativo

SEZIONE IV: STANDARD E PROCEDURE

14. STANDARD E PROCEDURE APPLICATE

14.1. STANDARD DI QUALITÀ E SICUREZZA DEI PROCESSI

14.1.1. Standard di qualità

Di seguito l'elencazione degli standard per la Gestione del Sistema di Qualità usati da PagoPA come riferimento per la definizione, gestione e controllo dei processi oppure come standard di certificazione.

Codice Documento	**Titolo**
UNI EN ISO 9001:2015	Sistemi di gestione per la qualità - Requisiti
UNI EN ISO 9000:2015	Sistemi di gestione per la qualità - Fondamenti e vocabolario
UNI EN ISO 19011:2012	Linee guida per gli audit dei sistemi di gestione

14.1.2. Standard di sicurezza

Di seguito l'elencazione degli standard per la Gestione del Sistema di Sicurezza delle Informazioni applicati nell'azienda PagoPA come riferimento per pianificazione, implementazione, gestione e controllo dei processi di sicurezza e come standard di certificazione.

Codice Documento	**Titolo**
UNI CEI ISO/IEC 27001:2013	Tecnologie Informatiche – Tecniche di sicurezza - Sistemi di gestione della sicurezza dell'informazione - Requisiti
UNI CEI ISO/IEC 27002:2013	Tecnologie Informatiche – Tecniche di sicurezza - Codice di pratica per la gestione della sicurezza delle informazioni

Codice Documento	Titolo
Regolamento UE n 910/2014 - eIDAS (electronic IDentification Authentication and Signature)	Identità digitale
ETSI EN 319 401, 319-411, 319-521, 319-522	ETSI

14.1.3. Standard tecnologici

Relativamente ai processi ed alle applicazioni individuate dall'allegato tecnico al DM 2 novembre 2005, SEND è conforme agli standard elencati nella tabella che segue.

Codice	Titolo
RFC 1847	Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted
RFC 1891	SMTP Service Extension for Delivery Status Notifications
RFC 1912	Common DNS Operational and Configuration Errors
RFC 2252	Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
RFC 2315	PKCS #7: Cryptographic Message Syntax Version 1.5
RFC 2633	S/MIME Version 3 Message Specification
RFC 2660	The Secure HyperText Transfer Protocol
RFC 2849	The LDAP Data Interchange Format (LDIF) - Technical Specification
RFC 3174	US Secure Hash Algorithm 1 (SHA1)

Codice	Titolo
RFC 3207	SMTP Service Extension for Secure SMTP over Transport Layer Security
RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
ISO/IEC 9594-8:2001	Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

14.2. GESTIONE DELLA PIATTAFORMA TECNOLOGICA

Lo scopo delle procedure messe in atto da PagoPA per la conduzione dei servizi di Recapito Certificato è quello di:

- rendere disponibili informazioni certe sulla configurazione del sistema e le relazioni che intercorrono tra i vari elementi anche al fine di apportare modifiche in modo controllato;
- assicurare il controllo delle modifiche alla configurazione nel rispetto dei ruoli come definiti dalla norma e che hanno competenza sulle attività di modifica agli elementi di configurazione;
- tracciare la storia della configurazione per ricostruire versioni del sistema di gestione del Recapito Certificato ed identificare cause di eventuali problemi verificatisi a seguito di modifiche ai sistemi per l'erogazione.

14.2.1. Attivazione della procedura di gestione della configurazione

La procedura è attivata dal Responsabile della Piattaforma per controllare periodicamente lo stato della configurazione su base periodica o su specifica richiesta delle funzioni interessate.

14.2.2. Aggiornamento della configurazione

L'aggiornamento della configurazione viene effettuato con l'ausilio di strumenti di sistema che generano una tracciatura completa dello stato di configurazione di ogni componente il sistema SEND.

Le informazioni sono generate dal sistema di GitHub e documentate su piattaforma Confluence per le specifiche risorse a supporto del servizio.

Le informazioni minime tracciate sono:

- repository;
- microservizi;
- API;
- eventi relativi all'utilizzo del servizio e all'efficienza / efficacia, resilienza e continuità delle risorse sottese.

Sono inoltre associate informazioni aggiuntive utili al responsabile della gestione della risorsa di elaborazione ed al responsabile delle risorse dati, secondo lo schema che segue:

- Alta: se la compromissione della risorsa impatta in maniera bloccante tale per cui una o più funzionalità critiche per l'utenza non sono disponibili;
- Media: se la compromissione della risorsa limita la funzionalità in alcune sue componenti secondarie tali da non impedirne comunque una fruizione anche se parziale;
- Bassa: se la compromissione della risorsa che fa parte del sistema SEND può essere accomunata ai comuni malfunzionamenti e dunque non sono riscontrabili ripercussioni significative sulla fruizione del servizio.

14.2.3. Controllo dello stato di configurazione

Con periodicità almeno trimestrale, o su richiesta della funzione responsabile del servizio SEND viene effettuato il controllo dello stato della configurazione.

Tali informazioni sono riportate in un apposito report contenente al minimo le seguenti informazioni:

- identificativo dell'item di configurazione;
- stato dell'item (attivo/non attivo);
- data (attivazione/disattivazione).

14.3. GESTIONE DELLE VERIFICHE AFFERENTI ALLA SICUREZZA

Gli strumenti che sono implementati ai fini della sicurezza permettono di:

- individuare le vulnerabilità;
- classificare il grado di gravità delle situazioni di rischio;
- individuare le azioni correttive per minimizzare il rischio.

Lo stato dei processi relativamente alla sicurezza è monitorato mediante apposite verifiche tecniche e di conformità svolte rispettivamente dal Responsabile della Sicurezza e dal Responsabile dell'Audit nominati per il Servizio di Recapito Certificato.

La procedura di verifica è attivata a seguito di:

- attività pianificate e definite nei piani di vulnerability assessment;

- attività pianificate e definite nei piani degli audit interni svolte in conformità alla pianificazione;
- attività non pianificate ma che possono rendersi necessarie in forma occasionale;
- mutamenti significativi della infrastruttura di rete e dei sistemi;
- sostanziali mutamenti dello scenario delle minacce cui le reti ed i sistemi sono soggetti;
- incidenti di sicurezza, quando (dopo averne eliminato gli effetti) sia necessario effettuare approfondite analisi per determinare le possibili cause.

Il Responsabile della Sicurezza, per lo svolgimento delle attività, si avvale del Team di assessment che può essere formato da personale interno con specifiche competenze o da personale appartenente a società operanti nel settore della sicurezza.

15. SOLUZIONI FINALIZZATE A GARANTIRE IL COMPLETAMENTO DELLA TRASMISSIONE

15.1. APPROCCIO ORGANIZZATIVO

La continuità del servizio, anche al fine di assicurare il completamento delle fasi di trasmissione dei messaggi, è assicurata attraverso procedure di escalation che mirano alla gestione affidabile e controllata di SEND.

Il team gestisce le emergenze attraverso la reperibilità on-call. Ci sono due tipi di reperibilità: on-call 9-18, durante l'orario di lavoro dal lunedì al venerdì, e on-call 18-9, fuori dall'orario di lavoro e durante i weekend.

Il team on-call 9-18 è composto da first-responders e team-shadow. I first-responders sono membri del team che conoscono perfettamente la procedura di gestione delle emergenze e sono in grado di eseguire tutti gli step dei runbook in autonomia. Il team-shadow, invece, è formato da membri che ancora non hanno raggiunto questa competenza e agiscono come assistenti dei first-responders.

Durante l'orario lavorativo, il team on-call 9-18 gestisce le emergenze e non si occupa delle segnalazioni provenienti dal livello L2 di assistenza, che sono gestite dal team L3 di SEND.

In sintesi, in caso di alert:

- scatta un allarme relativo a un servizio e collegato a Opsgenie, che si occupa di notificare al team dei first Responders in base all'on-call scheduling;
- l'utente on-call avrà la responsabilità di prendere in carico l'allarme per analizzarlo. A seguito dell'analisi si possono presentare tre scenari:

- avviare un'escalation;
- sospendere l'alert
- creare un Incident.

Il processo termina con la completa risoluzione del malfunzionamento; la chiusura (data ed ora) del processo viene registrata dallo strumento stesso.

15.2. APPROCCIO TECNOLOGICO

15.2.1. Sistemi tecnologici

L'architettura fisica di SEND è in totale carico del Cloud Service Provider AWS. Tale scelta è volta a garantire elevati livelli di affidabilità e resilienza del servizio.

Tale architettura garantisce le seguenti funzionalità:

- affidabilità:
- sicurezza:
- scalabilità.

16. LOG DI SISTEMA - ANONIMIZZAZIONE E CONSERVAZIONE

SEND anonimizza le informazioni che possono ricondurre all'identificazione di persone. Ad esempio, SEND utilizza un servizio che genera una versione anonimizzata del CF e che mantiene permanentemente la relazione tra il CF e la sua versione anonimizzata.

Le informazioni presenti nei log di sistema e nei record di Invio/Ricezione sono anonimizzate.

Solo i documenti allegati alle Comunicazioni e le certificazioni opponibili a terzi possono contenere informazioni in chiaro.

I log di sistema vengono prodotti su database, indicizzati per versione anonimizzata del CF e partizionati per data. Ogni record di log può contenere più di un CF anonimizzato.

SEND non effettua operazioni di update o delete sui record di log.

I log vengono conservati per un massimo di 10 anni. I log degli ultimi 120 giorni sono sempre presenti in DB per accesso rapido, i log vengono inoltre trasferiti giornalmente su file system e conservati con le stesse modalità utilizzate per le certificazioni opponibili a terzi.

I log di accesso a mezzo SPID o CIE (che contengono le informazioni relative a timestamp, source, spidRequestId, encryptedRequest, encryptedResponse) sono conservati per 24 mesi.

I log necessari per comprovare le informazioni contenute nelle certificazioni opponibili a terzi sono conservati per 10 anni.

Gli audit log che non sono necessari per comprovare le informazioni contenute nelle certificazioni opponibili a terzi sono conservati per 5 anni.
I log di sistema di SEND non necessari per comprovare le informazioni contenute nelle certificazioni opponibili a terzi sono conservati per 36 mesi.

17. ALTRI DATI - CONSERVAZIONE

I dati di navigazione, ovvero i record contenenti informazioni relative a browser, IP e device utilizzati durante le interazioni dell'Utente su SEND, sono conservati per 90 giorni.
I cookie sono conservati per 6 mesi.
I dati relativi alla configurazione delle utenze (ruoli, gruppi di appartenenza, ecc.) sono conservati per 2 anni dall'ultimo accesso.
I dati acquisiti a mezzo SPID e CIE ovvero nello specifico: nome, cognome, codice fiscale, ruolo del soggetto registrato quale Referente della PA Mittente sono conservati per 2 anni dall'ultima acquisizione.
Gli atti digitali originali depositati dalla PA sono conservati da SEND per 10 anni. Il destinatario può consultare e scaricare gli stessi in formato digitale accedendo alla piattaforma entro 120 gg dal perfezionamento della Comunicazione per il destinatario. Successivamente a tale termine dovrà inoltrare richiesta alla PA.

SEZIONE V: PROTEZIONE DEI DATI

18. VERIFICA DEI DATI IN INGRESSO

SEND garantisce la corretta attribuzione dei documenti informatici alla Comunicazione attraverso l'utilizzo di hash SHA-256. La PA - Mittente, nel momento in cui genera la richiesta di Invio, fornisce a SEND anche lo SHA-256 del documento. SEND calcola lo SHA-256 del documento ricevuto e lo confronta con ciò che la PA - Mittente ha fornito. Solo in caso di coincidenza tra le due hash la richiesta di Invio è accettata.

Inoltre, SEND verifica la validità dei CF forniti della PA mittente e la presenza dell'indirizzo fisico del/i destinatario/i per garantire la possibilità di effettuare la Comunicazione.

19. IMMODIFICABILITÀ DEI DOCUMENTI INFORMATICI MEMORIZZATI

I documenti informatici forniti dalla PA mittente vengono archiviati temporaneamente in un bucket S3 con legal hold e retention di 7 giorni. Legal hold rende i documenti immodificabili da parte di PagoPA fino allo scadere della retention, quando i documenti verranno eliminati automaticamente dal sistema. I documenti sono sottoposti a versioning.

Quando la PA - Mittente richiede di effettuare una Comunicazione, una volta generato lo IUN, i documenti, associati dalla PA - Mittente alla Comunicazione attraverso la lista di SHA-256, vengono associati logicamente alla Comunicazione appena creata. Sui documenti viene aggiornata la retention a 120 giorni. Alla data di perfezionamento della Ricezione per il destinatario, la retention viene nuovamente aggiornata a 120 giorni successivi a tale data.

Gli SHA-256 dei documenti vengono memorizzati nel record di Invio e nella certificazione opponibile a terzi di perfezionamento per il mittente. Il record di Invio contiene anche la versione esatta di ciascun documento.

Gli AAR e le certificazioni opponibili a terzi vengono create, sigillate elettronicamente e marcate temporalmente ed archiviate. Viene posto il legal hold e retention a 10 anni. La versione del documento viene memorizzata nel record di timeline corrispondente all'evento che lo ha generato. Entro un anno dalla creazione del documento, esso viene inviato alla conservazione a norma.

20. GENERAZIONE DELLE CERTIFICAZIONI OPPONIBILI A TERZI

La certificazione opponibile a terzi viene generata a fronte di particolari eventi. Nel momento in cui l'evento si verifica viene prodotto un documento PDF con il contenuto descritto precedentemente. Al documento viene applicato il sigillo elettronico

qualificato di PagoPA e la marcatura temporale certificata. Questo garantisce l'immutabilità e non ripudiabilità del documento. Garantisce inoltre la data di generazione del documento stesso. Il documento viene quindi conservato come descritto precedentemente.

SEZIONE VI: PROTEZIONE DEI DATI PERSONALI

21. ORGANIZZAZIONE PRIVACY

I dati personali rilasciati dai soggetti che accedono al servizio SEND sono trattati conformemente a quanto previsto dal D.lgs. 101/2018 e dal Regolamento (UE) 2016/679 in materia di protezione dei dati personali.

Le figure a cui sono attribuiti specifici ruoli e responsabilità nel trattamento dei dati personali sono:

- Titolare;
- Responsabile;
- Incaricato.

Titolare è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente, o insieme ad altri, determina le finalità e i mezzi del trattamento.

Responsabile del Trattamento è la persona fisica o giuridica che tratta i dati personali in nome e per conto del Titolare del trattamento

Incaricato è il personale autorizzato al trattamento dei dati personali.

Il Modello Privacy di PagoPA è costituito dalle seguenti figure:

- Titolare del trattamento:
  Il titolare del trattamento è PagoPA S.p.A., con sede in Roma, Piazza Colonna 370, CAP - 00187, n. di iscrizione a Registro Imprese di Roma, CF e P.IVA 15376371009.
  E-mail: dpo@pagopa.it.
  Per ogni domanda inerente il trattamento di dati personali è possibile procedere tramite il form dedicato alla gestione delle richieste degli interessati.
- Responsabile Protezione Dati
  PagoPA S.p.A. ha nominato un proprio Responsabile della Protezione dei dati, ai sensi dell'art. 37 del Regolamento, che può essere contattato tramite apposito form di contatto.
  Il form è altresì disponibile sul sito web della Società nella sezione "Diritto alla protezione dei dati personali".
  Oppure tramite i seguenti recapiti:
  e-mail - dpo@pagopa.it;
  PEC - dpo@pec.pagopa.it;
  indirizzo - Via Sardegna n. 38 - 00187, ROMA (sede operativa della società).

22. MODALITA' DI PROTEZIONE DEI DATI

22.1. DATI PERSONALI

Ai sensi dell'art. 4 del Regolamento UE 2016/679 il «dato personale» è qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

I dati personali trattati in ragione delle attività oggetto del Contratto sono: dati comuni (es. nome, cognome, CF, ecc.); qualsiasi dato anche appartenente a categorie particolari contenuto nei documenti e messaggi trasmessi.

22.2. DIRITTI DEGLI INTERESSATI

PagoPA garantisce la tutela dei diritti degli interessati attraverso processi organizzativi e procedure che consentono di:

- fornire agli interessati adeguata informativa sul trattamento dei dati, ambiti e finalità;
- gestire le richieste degli interessati ai sensi degli articoli 15 e seguenti del Regolamento UE 2016/679;
- gestire i consensi richiesti all'interessato relativamente al trattamento dei propri dati personali nell'ambito di SEND.

22.3. SICUREZZA DEI DATI

Come previsto dalle norme, PagoPA adotta idonee e preventive misure di sicurezza al fine di ridurre al minimo:

- i rischi di distruzione o perdita, anche accidentale, dei dati, di danneggiamento delle risorse hardware su cui sono registrati e dei locali ove vengono custoditi;
- l'accesso non autorizzato ai dati stessi;
- modalità di trattamento non consentite dalla legge o dai regolamenti aziendali.

Le misure di sicurezza adottate assicurano:

- l'integrità dei dati, da intendersi come salvaguardia dell'esattezza dei dati, difesa da manomissioni o modifiche da parte di soggetti non autorizzati;

- la disponibilità dei dati, da intendersi come la certezza che l'accesso sia sempre possibile quando necessario; indica quindi la garanzia di fruibilità dei dati e dei servizi, evitando la perdita o la riduzione dei dati e dei servizi;
- la confidenzialità/riservatezza dei dati, da intendersi come garanzia che le informazioni siano accessibili solo da persone autorizzate e come protezione delle trasmissioni e controllo degli accessi stessi.
- Il Sistema di Gestione Qualità e Sicurezza delle Informazioni attuato in PagoPA è certificato secondo le norme ISO 9001:2015 e ISO 27001:2013, ed è stato strutturato per garantire la compliance normativa e tenere sotto controllo i possibili rischi sulla sicurezza dei sistemi informativi. Le procedure e le metodologie adottate ed applicate sono riferite all'intero ciclo di vita del Servizio di Recapito Certificato.

SEZIONE VII: COMUNICAZIONI

9 COMUNICAZIONE DI MODIFICHE SIGNIFICATIVE

Nel caso di modifiche significative nella prestazione dei propri servizi fiduciari qualificati aventi impatto sulla struttura organizzativa, sulle infrastrutture o sulla configurazione dei processi PagoPA provvederà a darne comunicazione al CAB in conformità al Regolamento dell'Organismo parte integrante del contratto stipulato con lo stesso e ad AgID.

Per modifica significativa si deve intendere:

- una variazione di configurazione dell'infrastruttura che abbia impatto sul servizio o sulla sicurezza delle informazioni;
- modifiche delle politiche di sicurezza e delle modalità tecniche per la loro applicazione;
- modifiche agli assetti organizzativi del sistema di gestione;
- una variazione del SOA o del SPS "Service Practice Statement",
- l'eliminazione di posizioni organizzative che hanno impatto sulla sicurezza etc.

Non sono da considerare modifiche significative:

- il normale turnover del personale;
- le normali operazioni di manutenzione che prevedano anche sostituzione di componenti;
- le revisioni delle valutazioni dei rischi, ove non comportino variazioni nell'applicazione dei controlli operativi o nella progettazione dei processi.

Ove richiesto, provvederà a fornire evidenza della valutazione dei rischi condotta a fronte del cambiamento per valutarne l'impatto sul servizio e sui relativi livelli di sicurezza.

La comunicazione evidenzierà anche se le modifiche abbiano richiesto anche la revisioni dei "Service Practice Statements" (SPS) e/o dello "Statement of Applicability" (Dichiarazione di Applicabilità) previsto dalla 27001.

10 COMUNICAZIONE DI CESSAZIONE ATTIVITÀ

La piattaforma SEND è l'ultima versione della "Piattaforma delle Notifiche Digitali - PND" istituita dall'art. 1, comma 402, della legge n. 160/2019 e disciplinata, in via generale, dall'art. 26 del Decreto-legge n. 76/2020 "Misure urgenti per la semplificazione e l'innovazione digitale" per consentire alle pubbliche amministrazioni di effettuare tramite piattaforma digitale l'invio di atti, provvedimenti, avvisi e comunicazioni ai cittadini.

In particolare, l'articolo 1, comma 402, della legge 27 dicembre 2019, n. 160 (Bilancio di previsione dello Stato per l'anno finanziario 2020 e bilancio pluriennale per il triennio 2020-2022) ha affidato alla Presidenza del Consiglio dei Ministri lo sviluppo, tramite la società PagoPA (interamente partecipata dallo Stato) di una piattaforma digitale per le Comunicazioni.

La piattaforma in questione e le sue modalità di funzionamento sono disciplinate dall'art. 26 del D.L. 16 luglio 2020, n. 76 Misure urgenti per la semplificazione e l'innovazione digitale (convertito con modificazioni dalla L. 11 settembre 2020, n. 120).

Il quindicesimo comma del citato art. 26 affida al potere regolamentare del Governo la definizione delle caratteristiche generali della piattaforma, individuando contenuti, principi e condizioni a cui essa deve conformarsi.

Alla luce di quanto sopra, PagoPA non ha facoltà autonoma di cessare l'attività collegata a SEND così come, non essendoci servizi fiduciari sostitutivi di SEND, non ha la possibilità di cedere l'attività a terzi.

Nel caso la cessazione dovesse essere decisa con atto governativo, PagoPA provvederà a comunicare i riferimenti dello stesso al CAB e ad AgID.

La cessazione del servizio avverrà in conformità a quanto definito nel "Piano di cessazione" cui si rimanda.

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