# *Manuale Operativo*

*Posta Elettronica Certificata*

## UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

**(pagina lasciata intenzionalmente bianca)**

# VERSIONE DEL MANUALE E RESPONSABILITÀ

| | |
|---|---|
| *Versione* | 1.5 |
| *Emissione* | Allegato al DR 1614 del 11.05.2012 |
| *Redatto da* | Hilda Grasso – Responsabile Registrazione dei Titolari |
| *Verificato da* | Clelia Baldo – Direttore Tecnico CSI Area eGovernment (Riferimento del servizio UNINAPEC) |
| *Approvato da* | Vittorio Coti Zelati – Presidente del CSI (Responsabile della gestione del servizio UNINAPEC) |
| *Tipo di documento* | Documento Pubblico |

**(pagina lasciata intenzionalmente bianca)**

# INDICE

## INDICE DELLE FIGURE

**(pagina lasciata intenzionalmente bianca)**

# 1 – Introduzione

Il presente capitolo descrive lo scopo del documento e le modifiche ad esso apportate nel tempo; riporta, inoltre, una tabella di corrispondenza tra i contenuti della Circolare n.49 del CNIPA del 24 novembre 2005 ed i capitoli del documento, in modo da facilitarne la lettura.

## 1.1 Scopo del documento

Il **Manuale Operativo della Posta Elettronica Certificata (PEC)** illustra le caratteristiche del servizio di posta elettronica certificata (PEC) erogato, in qualità di gestore del servizio, dall'Università degli Studi di Napoli Federico II (nel seguito: UNINA o Gestore).

## 1.2 Registro delle modifiche

| | | | |
|---|---|---|---|
| **Versione.Release:** | 1.0 | **Data emissione:** | 15.07.2009 |
| **Descrizione modifiche:** | | | |
| **Motivazioni:** | Prima emissione | | |
| | | | |
| **Versione.Release:** | 1.1 | **Data emissione:** | 13.12.2010 |
| **Descrizione modifiche:** | 1. Modificato il codice release da “0” a “1” nel nome del documento e coerente aggiornamento del piè di pagina (all);<br>2. Modificata la descrizione del ruolo del Presidente del C.S.I. in “Responsabile della gestione del servizio UNINAPEC” (par. 2.1);<br>3. Aggiornato il nome del Presidente del C.S.I. (par.2.1);<br>4. Aggiornato il numero dei dipendenti dell’Ateneo ed, in particolare, dei docenti e ricercatori (par. 2.1);<br>5. Aggiornati i riferimenti normativi (par. 2.5);<br>6. Inserito il par. 5.1 con la descrizione dell’architettura dei domini gestiti da UNINAPEC e dei flussi che coinvolgono domini assegnati ad UNINA e ad altre PA;<br>7. Inserito il chiarimento relativo alla politica di definizione di ulteriori nuovi domini (par. 5.2);<br>8. Inserito il riferimento al dominio “gestorepec.unina.it” (par. 5.2);<br>9. Aggiornato il paragrafo sulla descrizione dell’assegnazione delle caselle (par. 5.3) ;<br>10. Inserito il riferimento ai moduli “Richiesta casella PEC di servizio” modulo “Richiesta casella PEC ospiti” (rispettivamente, parr. 5.4.1 e 5.4.4);<br>11. Inserito il riferimento al modulo per la “Richiesta LOG” (par. 5.7);<br>12. Inserita la descrizione del meccanismo per tenere sotto controllo l’occupazione di spazio della casella (par. 5.13);<br>13. Indicazione delle modalità di comunicazione (tramite pubblicazione su WEB) Gestore-Titolare (par. 5.13);<br>14. Modificato il par. 6.7.8;<br>15. Aggiornato il paragrafo 10. | | |
| **Motivazioni:** | Revisione della documentazione a seguito dell’avvio dell’esercizio del sistema UNINAPEC. | | |

| | | | |
|---|---|---|---|
| **Versione.Release:** | 1.2 | **Data emissione:** | 14.02.2012 |

| | |
|---|---|
| **Descrizione modifiche:** | 1. Modificato il codice release da “1” a “2” nel nome del documento e coerente aggiornamento del piè di pagina;<br>2. Invertito l’ordine dei capitoli 3, 4 e 5, nel seguente: 4, 5 e 3;<br>3. Aggiornato secondo la normativa [CAD] vigente il cap. 3;<br>4. Inserito il paragrafo 3.1.1 sui soggetti coinvolti nel servizio UNINAPEC;<br>5. Modificata la descrizione delle caselle personali e di quelle istituzionali (par. 3.2);<br>6. Aggiunto il paragrafo sulla Creazione di domini UNINAPEC (par. 3.4.1);<br>7. Aggiunto il paragrafo sulla Cessazione di domini UNINAPEC (par. 3.5.1);<br>8. Aggiornata la descrizione del meccanismo di modifica della titolarità delle caselle istituzionali (par. 5.4.1.2 nella versione 1.1, par. 3.4.2.2 nella presente) e del rilascio delle caselle agli studenti (par. 5.4.3 nella versione 1.1, par. 3.4.4 nella presente);<br>9. Aggiornato il paragrafo sulla descrizione della procedura di cessazione delle caselle (par. 5.6 nella versione 1.1, par. 3.5 nella presente);<br>10. Aggiornato il paragrafo 5.13 (nella versione 1.1, par. 3.6 nella presente) relativamente a:<br>a. descrizione del meccanismo di monitoraggio delle caselle e del sistema di notifica PEC su posta elettronica convenzionale;<br>b. indirizzo aggiornato per la pubblicazione degli avvisi di sospensione del servizio.<br>11. Modificato il paragrafo 9.3 relativamente alla copertura assicurativa del servizio. |
| **Motivazioni:** | Revisione periodica della documentazione del servizio UNINAPEC. |

| | | | |
|---|---|---|---|
| **Versione.Release:** | 1.3 | **Data emissione:** | 25.07.2012 |
| **Descrizione modifiche:** | 1. Modificato il codice release da “2” a “3” nel nome del documento e coerente aggiornamento del piè di pagina;<br>2. Nella tabella contenente la descrizione delle modifiche contenute nella versione 1.2 del Manuale Operativo, per i paragrafi modificati, inserita la doppia numerazione del paragrafo (riferita cioè sia alla versione 1.1 che 1.2 del Manuale);<br>3. Aggiornato il riferimento al nuovo Regolamento di Ateneo in materia di Posta Elettronica Certificata [UNINA-PEC];<br>4. Aggiunto il riferimento al "Regolamento per l’utilizzo del servizio di Posta elettronica @unina.it" [UNINA-PE];<br>5. Aggiunto il riferimento [Customer satisfaction] alle linee guida in materia di rilevazione della customer satisfaction di uno specifico servizio erogato in rete;<br>6. Aggiornato il paragrafo 3 con il riferimento al Regolamento [UNINA-PEC];<br>7. Aggiornati i parr. 3.4.2.1, 3.4.2.2, 3.4.3 e 3.4.5, con il riferimento al Regolamento [UNINA-PE];<br>8. Modificata nel par. 3.4.3 la procedura operativa per la comunicazione ai dipendenti in servizio della assegnazione della casella PEC: l’Università invia le comunicazioni agli interessati via posta elettronica istituzionale unina invece che per posta interna;<br>9. Aggiunto il paragrafo 3.6 “Accesso al servizio”;<br>10. Modificato il paragrafo 3.7 (3.6 nella versione 1.2), con particolare riguardo ai punti a), b) e d);<br>11. Nel paragrafo 3.7, inserito il punto relativo alla “Rilevazione della | | |

| | |
|---|---|
| | Customer Satisfaction";<br>12. Nel paragrafo 7.2, in accordo con il testo vigente del [DLgs 196/03] in materia di protezione dei dati personali, eliminato il riferimento al Documento Programmatico sulla Sicurezza. |
| **Motivazioni:** | Aggiornamento per l'entrata in vigore del nuovo Regolamento di Ateneo in materia di posta elettronica certificata.. |

| | | | |
|---|---|---|---|
| **Versione.Release:** | 1.4 | **Data emissione:** | 17.02.2014 |
| **Descrizione modifiche:** | 1. Aggiornata la descrizione sintetica del Gestore al punto 2.1, in modo coerente alla nuova organizzazione statutaria dell'Ateneo;<br>2. Aggiunto il riferimento al Regolamento di Ateneo in materia di posta elettonica@studenti.unina.it (par. 2.4);<br>3. Modificato il flusso per l'aggiornamento del Manuale Operativo del Servizio al punto 2.5.2;<br>4. Inserita la denominazione dell'AdID al punto 2.9.1;<br>5. Aggiornata l'informazione sull'ampiezza delle "caselle istituzionali", al punto 3.7.d);<br>6. Modificata la descrizione della procedura per la cessazione delle caselle PEC, mediante l'inserimento del riferimento ai Regolamenti di Ateneo in materia di posta elettronica (punto 3.5.2);<br>7. Modificato l'intervallo temporale di disponibilità giornaliera del servizio in voce del Contact Center (cap. 10). | | |
| **Motivazioni:** | Adeguamento al nuovo Statuto di Ateneo. | | |

| | | | |
|---|---|---|---|
| **Versione.Release:** | 1.5 | **Data emissione:** | 03.05.2016 |
| **Descrizione modifiche:** | 1. Aggiornato il nome del Presidente del C.S.I.;<br>2. Nei riferimenti normativi, aggiunto quello relativo al decreto di nomina del Presidente del C.S.I. (par. 2.4);<br>3. Riportate le nuove dimensioni massime delle diverse tipologie di casella PEC al punto 3.7, lettera d);<br>4. Nella tabella al punto 3.12, riportato il nuovo valore della dimensione massima del messaggio;<br>5. Adeguata la descrizione delle regole di impostazione della password per l'accesso al servizio alle policy contenute nel Regolamento [UNINA-PE] (par.6.7.1);<br>6. Inserito il chiarimento in merito all'uso dei canali di comunicazione riportati nel Manuale, da utilizzare "esclusivamente per esigenze connesse con l'utilizzo del servizio UNINAPEC" (cap.10). | | |
| **Motivazioni:** | Adeguamento al nuovo assetto organizzativo e ai nuovi requisiti per il servizio PEC forniti da AgID ai gestori. | | |

## 1.3 Tabella di corrispondenza

Si riporta di seguito la tabella di corrispondenza tra gli argomenti contenuti nella Circolare CNIPA n. 49 del 24 novembre 2005 [CNIPA/CR/49] e i paragrafi del presente documento.

| Manuale Operativo | Circolare CNIPA |
|---|---|

| Manuale Operativo | Circolare CNIPA |
|---|---|
| *Par. 2.1* | *Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo.*<br>***Punto a:***<br>*dati identificativi del Gestore* |
| *Par. 2.3* | *Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo.*<br>***Punto b:***<br>*indicazione del responsabile del manuale* |
| *Par. 2.4* | *Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo.*<br>***Punto c:***<br>*riferimenti normativi necessari per la verifica dei contenuti* |
| *Par. 2.5.1* | *Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo.*<br>***Punto d:***<br>*indirizzo del sito web del Gestore ove il manuale è pubblicato e scaricabile* |
| *Cap. 2.7* | *Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo.*<br>***Punto e:***<br>*indicazione delle procedure oltre che degli standard tecnologici e di sicurezza utilizzati dal Gestore nell'erogazione del servizio* |
| *Par. 2.9* | *Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo.*<br>***Punto f:***<br>*definizioni, abbreviazioni e termini tecnici* |
| *Cap. 3* | *Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo.*<br>***Punto g:***<br>*descrizione sintetica del servizio offerto* |
| *Par. 3.7 e Cap. 5* | *Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo.*<br>***Punto h:***<br>*descrizione delle modalità di reperimento e di presentazione delle informazioni presenti nei log dei messaggi* |
| *Par.3.1, 3.2 e 3.3* | *Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo.*<br>***Punto i:***<br>*indicazione del contenuto e delle modalità dell'offerta da parte del Gestore* |
| *Par. 3.4* | *Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo.*<br>***Punto j:***<br>*indicazione delle modalità di accesso al servizio* |
| *Par. 3.10 e 3.11* | *Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo.*<br>***Punto k:***<br>*indicazione del livelli di servizio e dei relativi indicatori di qualità di cui all'art. 12 del decreto del Ministero per l'Innovazione e le Tecnologie 2 novembre 2005* |
| *Par. 3.12* | *Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo.*<br>***Punto l:***<br>*indicazione delle condizioni di fornitura del servizio* |
| *Cap. 7* | *Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo.*<br>***Punto m:***<br>*indicazione delle modalità di protezione dei dati dei titolari* |

| Manuale Operativo | Circolare CNIPA |
|---|---|
| *Cap. 9* | *Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo.*<br>***Punto n:***<br>*indicazione degli obblighi e delle responsabilità che ne discendono, delle esclusioni e delle limitazioni, in sede di indennizzo, relative ai soggetti previsti all'art. 2 del DPR n.68/2005* |

# 2 – Informazioni di carattere generale

Il presente capitolo riporta i dati identificativi del Gestore e ne descrive sinteticamente le attività e gli ambiti operativi; contiene, inoltre, i riferimenti normativi in ambito di posta elettronica certificata.

## 2.1 Dati identificativi e descrizione sintetica del Gestore

Il servizio di Posta Elettronica Certificata viene erogato dall'Università degli Studi di Napoli Federico II attraverso il proprio Centro Servizi Informativi (C.S.I.), a ciò delegato dal Consiglio di Amministrazione dell'Ateneo. Di seguito, si riportano i dati identificativi del Gestore:

| Dati identificativi del Gestore | |
|---|---|
| *Ragione Sociale:* | Università degli Studi di Napoli Federico II – Centro Servizi Informativi di Ateneo (C.S.I.) |
| *Sede Legale:* | Corso Umberto I - 80138 Napoli |
| *Responsabile della gestione del servizio UNINAPEC:* | Presidente del C.S.I. |
| *Sede di erogazione del servizio:* | Complesso Universitario di Monte S. Angelo – Via Cinthia – 80126 Napoli |
| *Partita IVA:* | 00876220633 |
| *Siti web:* | http://www.unina.it |

L'Università degli Studi di Napoli Federico II è un'istituzione universitaria di diritto pubblico i cui fini primari sono l'elaborazione e la trasmissione delle conoscenze e la promozione della qualità dei processi formativi e della ricerca. Ciò viene perseguito promuovendo ed organizzando la ricerca e curando, con azioni coordinate, la formazione culturale e professionale, nonché la crescita civile degli studenti.

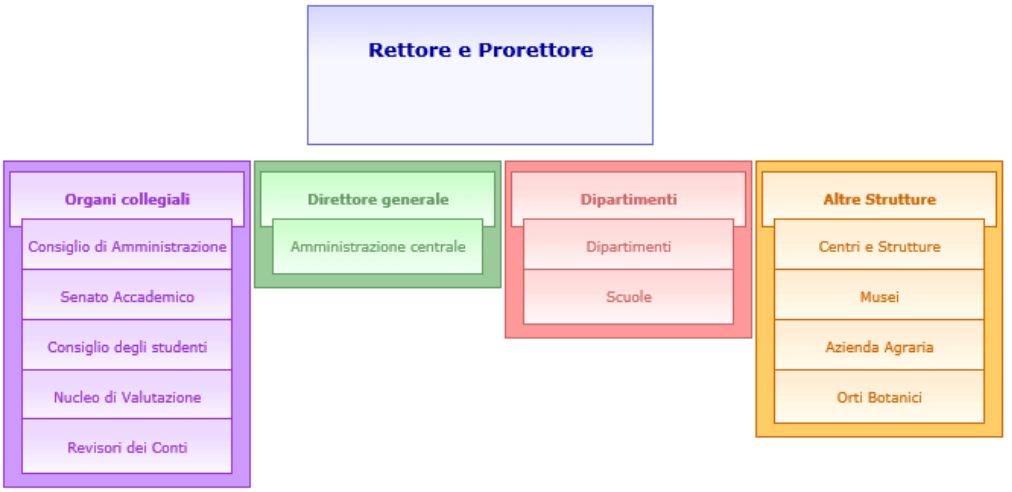


***Figura 1 – La struttura organizzativa UNINA***

L'Università degli Studi di Napoli Federico II è caratterizzata dalla presenza di circa 5.700 dipendenti, di cui circa 2.500 docenti e ricercatori, circa 86.000 studenti iscritti ed un numero commisurato di fornitori. Sul piano dell'organizzazione, ai sensi del proprio Statuto [UNINA-STA], l'Ateneo è articolato in Scuole, Dipartimenti, Centri di Ateneo, Centri di Eccellenza, Centri Interdipartimentali di Ricerca e di Servizio, Centri interuniversitari di ricerca, Scuole di Specializzazione, Centri Museali Biblioteche, Ripartizioni e Uffici amministrativi; il tutto in più sedi dislocate sul territorio.

## 2.2 Dati identificativi del documento

Il presente documento descrive le regole generali e le procedure seguite dall'Università degli Studi di Napoli Federico II per la gestione del proprio sistema di Posta Elettronica Certificata ed è identificato dal codice "UNINA-PEC-Manuale-Operativo-vx.n" dove i simboli "x" ed "n" individuano in modo univoco il livello di aggiornamento della versione e delle relativa release. Tale codice è riportato in ciascuna pagina del documento.

## 2.3 Responsabile del Manuale Operativo

Il responsabile del presente Manuale Operativo è Hilda Grasso, di cui si riportano di seguito i recapiti:

| | |
|---|---|
| *Email:* | hilda.grasso@unina.it |
| *Tel:* | 081.676641 |
| *Fax:* | 081.676628 |
| *Indirizzo:* | C.S.I. - Complesso Universitario di Monte S. Angelo – Via Cinthia – 80126 Napoli |

Per ogni comunicazione relativa al presente Manuale Operativo si può fare riferimento al Responsabile, inviando un messaggio di posta elettronica all'indirizzo sopra indicato.

## 2.4 Riferimenti normativi

Le modalità attraverso le quali avviene lo scambio di messaggi di posta certificata e le regole per l'interoperabilità tra i gestori del servizio sono definite nel dettaglio da specifica normativa. Il servizio offerto dal Gestore è conforme a tale quadro giuridico, sintetizzato nella tabella seguente, ove si riportano anche i regolamenti interni dell'Ateneo e le abbreviazioni utilizzate nel testo del presente Manuale Operativo per riferimento:

| | |
|---|---|
| **[TUDA]** | **Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 –** Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (GU n. 42 del 20 febbraio 2001) e successive modifiche ed integrazioni. |

| | |
|---|---|
| **[CAD]** | **Decreto Legislativo 7 marzo 2005, n. 82 (e successive modifiche ed integrazioni) –** Codice dell'amministrazione digitale, recante le disposizioni in base alle quali lo Stato, le Regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale mediante le tecnologie dell'informazione e della comunicazione. |
| **[DPCM 2004]** | **Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 –** Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici (GU n. 98 del 27 aprile 2004) e successive modifiche ed integrazioni. |
| **[DPR 68/05]** | **Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 –** Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3. |
| **[DM 2/11/05]** | **Decreto 2 novembre 2005 della Presidenza del Consiglio dei Ministri Dipartimento per l'Innovazione e le Tecnologie**, recante Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata (GU n. 266 del 15 novembre 2005). |
| **[L. 2/2009]** | **Conversione in legge del D.L. 29.11.2008, n. 185**, recante le misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale (GU n. 22 del 28 gennaio 2009, suppl. ord. n.14). |
| **[C.1/2010/DDI]** | **Circolare n. 1 del 18 febbraio 2010** del Dipartimento per la Digitalizzazione della Pubblica Amministrazione e l'Innovazione Tecnologica recante uso della PEC nelle amministrazioni pubbliche. |
| **[C.2/2010/DDI]** | **Circolare n. 2 del 19 aprile 2010** del Dipartimento per la Digitalizzazione della Pubblica Amministrazione e l'Innovazione Tecnologica recante informazioni per la gestione delle caselle di PEC. |
| **[CNIPA RT]** | **Regole tecniche** del servizio di trasmissione di documenti informatici mediante posta elettronica certificata, allegate al DM 2/11/05. |
| **[CNIPA/CR/49]** | **Circolare CNIPA n. 49 del 24 novembre 2005**, recante Modalità per la presentazione delle domande di iscrizione nell'elenco dei gestori di posta elettronica certificata (PEC). |

| | |
|---|---|
| **[CNIPA/CR/51]** | **Circolare CNIPA n. 51 del 7 dicembre 2006**, recante Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell'elenco dei gestori di posta elettronica certificata (PEC). |
| **[DLgs 196/03]** | **Decreto Legislativo n. 196 del 30 giugno 2003 –** Codice in materia di protezione dei dati personali (GU n. 174 del 29 luglio 2003, suppl. ord. N. 123). |
| **[Customer satisfaction]** | Documento **"Linee Guida** per l'applicazione del modello di valutazione della **customer satisfaction** di uno specifico servizio erogato on line", emanato dal Ministro per la Pubblica Amministrazione ed Innovazione. |
| **[UNINA-PEC]** | **Regolamento di Ateneo UNINA** titolato "Regolamento in materia di Posta Elettronica Certificata", emanato con D.R. n. 1614 del 11.05.2012. |
| **[UNINA-PE]** | **Regolamento di Ateneo UNINA** titolato "Regolamento per l'utilizzo del servizio di Posta elettronica @unina.it", emanato con D.R. n. 4489 del 29.12.2010. |
| **[UNINA-PES]** | **Regolamento di Ateneo UNINA** titolato "Regolamento per l'utilizzo del servizio di Posta elettronica@studenti.unina.it", emanato con D.R. n. 4488 del 29.12.2010. |
| **[UNINA-Privacy]** | **Regolamento di Ateneo UNINA** titolato "Regolamento di attuazione del Codice di protezione dei dati personali utilizzati dall'Università degli Studi di Napoli Federico II", emanato con D.R. n. 5073 del 30.12.2005. |
| **[UNINA-STA]** | **Statuto dell'Ateneo**, emanato con D.R. n.1660 del 15 maggio 2012, pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana n.132 del 08/06/2012. |
| **[UNINA-NominaPresidenteCSI]** | **Decreto di nomina del Presidente del CSI**, emanato con DR n. 4353 del 14.12.2015. |

## 2.5 Reperibilità ed aggiornamento del Manuale Operativo

### 2.5.1 Reperibilità del manuale

Il manuale è pubblico e la sua versione aggiornata può essere consultata e scaricata in formato pdf all'indirizzo web del Gestore: http://www.unina.it/UNINAPEC.
Il Gestore si impegna a mantenere sul sito la versione aggiornata del manuale operativo.

### 2.5.2 Modifiche al manuale

Il Gestore si impegna a modificare il presente manuale ogni qual volta avvenga una variazione, di natura tecnica, procedurale o logistica, sul sistema di posta elettronica certificata, oppure a seguito di modifiche di norme di legge o di regolamenti interni di

Ateneo. Ogni eventuale modifica verrà sottoposta a verifica ed approvazione interna da parte del Gestore, pubblicato sul sito del Gestore e trasmesso alla Agenzia per l'Italia Digitale.
In funzione della tipologia di variazione, ciascuna edizione del manuale sarà caratterizzata da un proprio numero di versione.release, secondo la seguente regola: le modifiche con impatto rilevante sugli utenti comportano l'incremento del numero di versione del documento (con numero release pari a 0), mentre quelle con impatto meno rilevante determinano l'incremento del solo numero di release.

### 2.5.3 Elementi sulla verifica e sull'approvazione del documento

Il presente manuale, verificato dal Direttore dell'Area Tecnica eGovernment del C.S.I., è sottoposto a ratifica del Presidente del C.S.I.. Copia del presente manuale è depositata presso l'Agenzia per l'Italia Digitale.

## 2.6 Modalità di comunicazione del titolare con il Gestore

Oltre al riferimento di cui al paragrafo 2.3, il titolare può contattare il Gestore attraverso i canali specificati nel capitolo 10 titolato "Canali di comunicazione".

## 2.7 Standard tecnologici e di sicurezza di riferimento

- 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 2045 (Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies)
- RFC 2049 (Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples)
- 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 Hyper Text Transfer Protocol)
- RFC 2821 (Simple Mail Transfer Protocol)
- RFC 2822 (Internet Message Format)
- RFC 2849 (The LDAP Data Interchange Format (LDIF) – Technical Specification)
- RFC 3174 (US Secure Hash Algorithm 1 – SHA1)
- 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)
- RFC 3161 (TSP Time Stamp Protocol)

Per l'erogazione del servizio di posta elettronica certificata, UNINA adotta le linee guida ed i principi previsti dallo standard di sicurezza **ISO 27001:2005**, standard che sostituisce la norma di riferimento BS 7799 e che costituisce un modello per analizzare, progettare, realizzare, manutenere, controllare e migliorare il cosiddetto **Information Security Management System (ISMS**). In un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento, lo standard ISO 27001:2005 si pone l'obiettivo di proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne:

- l'**integrità** (accuratezza e completezza),
- la **riservatezza** (accessibilità ai soli individui autorizzati),
- la **disponibilità** (certezza che le informazioni siano sempre a disposizione del personale incaricato).

Lo standard enfatizza l'importanza di:

- capire i requisiti di sicurezza necessari e la necessità di definire policy adatte;
- realizzare ed eseguire i controlli sul sistema, allo scopo di analizzare e gestire i rischi di sicurezza;
- monitorare e effettuare review dell'ISMS;
- migliorare ed ottimizzare l'ISMS sulla base delle misurazioni effettuate.

Lo standard adotta, per tutti i processi dell'ISMS, il modello **PDCA** (**Plan-Do-Check-Act)** che può essere così schematizzato:

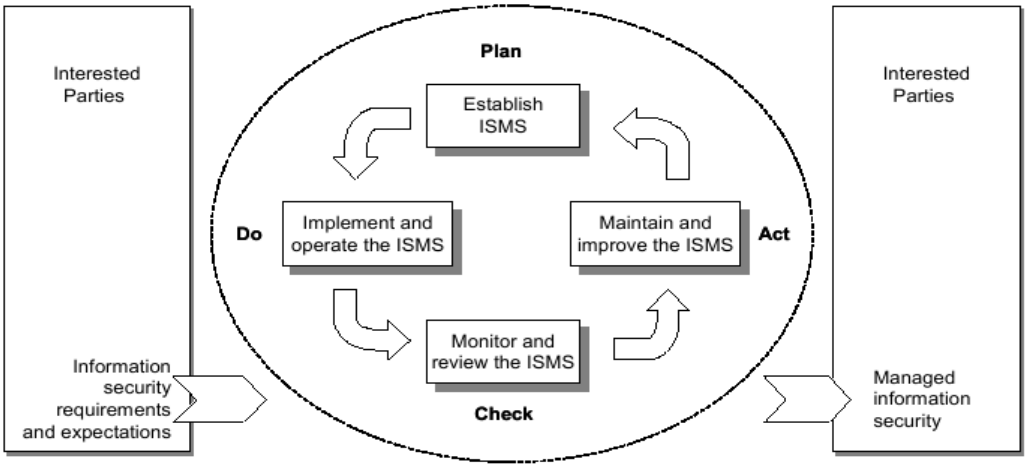


***Figura 2 – Il modello PDCA dello standard ISO/IEC 27001***

- **Plan**: stabilisce le policy, gli obiettivi, i processi e le procedure rilevanti per gestire il rischio e migliorare la sicurezza del sistema in accordo con le politiche e gli obiettivi complessivi dell'organizzazione.
- **Do**: implementa le policy, i processi e le procedure pianificate.
- **Check**: controlla e, ove possibile, misura le performance dei processi dell'ISMS documentando in opportuni report i risultati ottenuti.
- **Act**: intraprende azioni correttive e preventive sulla base dei risultati del controllo interno (vedi check) allo scopo di migliorare continuamente l'ISMS.

Nello standard sono fondamentali i concetti di:

- **analisi dei rischi**: individuazione punti deboli, studio delle possibili minacce e probabilità che si presentino, analisi degli eventuali impatti sul sistema;
- **gestione dei rischi**: monitor del sistema, rilevazione dei problemi e loro risoluzione, eliminazione punti deboli, riduzione dei rischi per l'intero sistema.

## 2.8 Sistema di Qualità

Per tutti i processi connessi al servizio di posta elettronica certificata, il Gestore imposta ed attua un sistema di gestione della qualità conforme ai requisiti stabiliti dalla UNI EN ISO 9001:2008.

## 2.9 Definizioni, abbreviazioni e termini tecnici

Di seguito vengono elencati i termini utilizzati nel corso del presente documento e, per ciascuno di essi, se ne fornisce descrizione.

### 2.9.1 Definizioni

| Termine | Descrizione |
|---|---|
| *PEC* | Posta Elettronica Certificata. |
| *CNIPA/DigitPA/AgID* | Centro Nazionale per l'Informatica nella Pubblica Amministrazione, attualmente Agenzia per l'Italia Digitale. |
| *UNINA* | Università degli Studi di Napoli Federico II. |
| *UNINAPEC* | Servizio PEC gestito da UNINA. |
| *Gestore di posta elettronica certificata* | Soggetto che gestisce uno o più domini di posta elettronica certificata con i relativi punti di accesso, di ricezione e di consegna, titolare della chiave usata per la firma delle ricevute e delle buste e che si interfaccia con altri gestori di posta elettronica certificata per l'interoperabilità con altri titolari. |
| *Indice dei Gestori di posta elettronica certificata* | Sistema che contiene l'elenco dei domini e dei gestori di posta elettronica certificata, con i relativi certificati corrispondenti alle chiavi usate per la firma delle ricevute, degli avvisi e delle buste, realizzato per mezzo di un server Lightweight Directory Access Protocol (LDAP), posizionato in un'area raggiungibile dai vari gestori di posta elettronica certificata e che costituisce, inoltre, la struttura tecnica relativa all'elenco pubblico dei gestori di posta elettronica certificata. |
| *Titolare* | Soggetto cui è assegnata una casella di posta elettronica certificata. |
| *Dominio di posta elettronica certificata* | Dominio, fully qualified domain name (FQDN), di posta elettronica certificata dedicato alle caselle di posta elettronica certificata. |
| *Casella di posta elettronica certificata* | Casella di posta elettronica definita all'interno di un dominio di posta elettronica certificata ed alla quale è associata una funzione che rilascia ricevute di avvenuta ricezione di messaggi di posta elettronica certificata. |
| *Punto di accesso* | Sistema che fornisce i servizi di accesso per l'invio e la lettura di messaggi di posta elettronica certificata, nonché i servizi di identificazione ed accesso dell'utente, di verifica della presenza di virus informatici all'interno del messaggio, di emissione della ricevuta di accettazione e di imbustamento del messaggio originale nella busta di trasporto. |

| Termine | Descrizione |
|---|---|
| *Punto di ricezione* | Sistema che riceve il messaggio all'interno di un dominio di posta elettronica certificata, effettua i controlli sulla provenienza e sulla correttezza del messaggio ed emette la ricevuta di presa in carico, imbusta i messaggi errati in una busta di anomalia e verifica la presenza di virus informatici all'interno dei messaggi di posta e delle buste di trasporto. |
| *Punto di consegna* | Sistema che compie la consegna del messaggio nella casella di posta elettronica certificata del titolare destinatario, verifica la provenienza e la correttezza del messaggio ed emette, a seconda dei casi, la ricevuta di avvenuta consegna o l'avviso di mancata consegna. |
| *Firma del gestore di posta elettronica certificata* | Firma elettronica avanzata, basata su un sistema di chiavi asimmetriche, che consente di rendere manifesta la provenienza e di assicurare l'integrità e l'autenticità dei messaggi del sistema di posta elettronica certificata; è generata attraverso una procedura informatica che garantisce la connessione univoca al gestore e la sua univoca identificazione, creata automaticamente con mezzi che garantiscano il controllo esclusivo da parte del gestore. |
| *Ricevuta di accettazione* | Ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del mittente, contenente i dati di certificazione, rilasciata al mittente dal punto di accesso a fronte dell'invio di un messaggio di posta elettronica certificata. |
| *Avviso di non accettazione* | Avviso, sottoscritto con la firma del gestore di posta elettronica certificata del mittente, emesso quando il gestore mittente è impossibilitato ad accettare il messaggio in ingresso, recante la motivazione per cui non è possibile accettare il messaggio e l'esplicitazione che il messaggio non potrà essere consegnato al destinatario. |
| *Ricevuta di presa in carico* | Ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, emessa dal punto di ricezione nei confronti del gestore di posta elettronica certificata mittente per attestare l'avvenuta presa in carico del messaggio da parte del sistema di posta elettronica certificata di destinazione, recante i dati di certificazione per consentirne l'associazione con il messaggio al quale si riferisce. |
| *Ricevuta di avvenuta consegna* | Ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, emessa dal punto di consegna ed inviata al mittente nel momento in cui il messaggio è inserito nella casella di posta elettronica certificata del destinatario; è ottenibile in tre formati con livelli di sintesi differenti secondo le successive definizioni. |

| Termine | Descrizione |
|---|---|
| *Ricevuta completa di avvenuta consegna* | Il formato più esteso di ricevuta; in tale formato sono contenuti i dati di certificazione ed il messaggio originale. |
| *Ricevuta breve di avvenuta consegna* | Il formato breve di ricevuta; in tale formato sono contenuti i dati di certificazione ed un estratto del messaggio originale. |
| *Ricevuta sintetica di avvenuta consegna* | Il formato sintetico di ricevuta; in tale formato sono contenuti i soli dati di certificazione. |
| *Avviso di mancata consegna* | Avviso, emesso dal sistema del destinatario, per indicare al mittente del messaggio originale che il gestore di posta elettronica certificata è stato impossibilitato a consegnare il messaggio nella casella di posta elettronica certificata del destinatario. |
| *Messaggio originale* | Messaggio inviato da un utente di posta elettronica certificata prima del suo arrivo al punto di accesso e consegnato al titolare destinatario per mezzo di una busta di trasporto che lo contiene. |
| *Busta di trasporto* | Busta creata dal punto di accesso e sottoscritta con la firma del gestore di posta elettronica certificata mittente; all'interno di tale busta sono inseriti il messaggio originale inviato dall'utente di posta elettronica certificata ed i relativi dati di certificazione. |
| *Busta di anomalia* | Busta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, nella quale è inserito un messaggio errato ovvero non di posta elettronica certificata e consegnata al titolare destinatario, evidenziando tale anomalia. |
| *Dati di certificazione* | Dati, quali ad esempio data ed ora di invio, mittente, destinatario, oggetto, identificativo del messaggio, che descrivono l'invio del messaggio originale e sono certificati dal gestore di posta elettronica certificata del mittente; tali dati sono inseriti nelle ricevute e sono trasferiti al titolare destinatario insieme al messaggio originale per mezzo di una busta di trasporto. |
| *Riferimento temporale* | Informazione, contenente la data e l'ora, associata ad un messaggio di posta elettronica certificata. |
| *Marca temporale* | Evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi secondo quanto previsto dal Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e dal Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, pubblicato nella Gazzetta Ufficiale n. 98 del 27 aprile 2004. |

| Termine | Descrizione |
|---|---|
| *Log dei messaggi* | Registro informatico delle operazioni relative alle trasmissioni effettuate mediante posta elettronica certificata tenuto dal gestore. |
| *Tamper evidence* | Sistema per segnalare qualsiasi tentativo di manomissione fisica del server che possa aver compromesso l'integrità del sistema e/o dei dati in esso contenuti; tipicamente realizzato tramite l'apposizione sulle macchine di sigilli, lucchetti, etichette autoadesive e/o qualsiasi altro mezzo di protezione il cui stato, in caso di accesso non autorizzato, risulti evidentemente compromesso ad un osservatore esterno. |
| *Tamper proof hardware* | Sistema di protezione fisica del server allo scopo di prevenire/impedire l'accesso e la manomissione del sistema dati da parte di soggetti non autorizzati. |

### 2.9.2 Abbreviazioni e termini tecnici

| Termine | Descrizione |
|---|---|
| *CC* | *Common Criteria*. Criteri per la valutazione della sicurezza nei sistemi informatici, con riconoscimento internazionale in quanto evoluzione dei criteri europei (ITSEC), americani (Federal Criteria) e canadesi (Canadian Criteria). |
| *GFS* | *Grandfather-Father-Son*. Strategia di backup. |
| *HSM* | *Hardware Security Module.* Dispositivo hardware per la generazione, la memorizzazione e la protezione sicura di chiavi crittografiche. |
| *HTML* | *Hyper Text Mark-Up Language*. Linguaggio usato per descrivere i documenti ipertestuali disponibili su Internet. Non è un linguaggio di programmazione, ma un linguaggio di markup, ossia descrive il contenuto, testuale e non, di una pagina web. |
| *HTTP* | *Hyper Text Transfer Protocol.* Protocollo di trasmissione che permette lo scambio di file (testi, immagini grafiche, suoni, video e altri documenti multimediali) su World Wide Web. |
| *HTTPS* | *Hyper Text Transfer Protocol (over) SSL.* Applicazione che si occupa di combinare l'interazione del protocollo HTTP attraverso un meccanismo di crittografia di tipo Transport Layer Security (SSL/TSL). |
| *IETF* | *Internet Engineering Task Force*. Comunità internazionale di professionisti dell'informatica che si occupa dell'evoluzione dell'architettura Internet. |

| Termine | Descrizione |
|---|---|
| *ISO* | *International Standards Organization.* Organizzazione internazionale per la standardizzazione, costituita da organismi nazionali provenienti da più di 75 paesi. Ha stabilito numerosi standard nell'area dei sistemi informativi. L'ANSI (American National Standards Institute) è uno dei principali organismi appartenenti all'ISO. |
| *ITSEC* | *Information Technology Security Evaluation Criteria.* Criteri europei per la valutazione della sicurezza nei sistemi informatici. |
| *LDAP* | *Lightweight Directory Access Protocol.* Protocollo applicativo utilizzato per la ricerca e la modifica di informazioni presenti su un Directory Server. Un directory server LDAP è un albero di entità costituite da attributi e valori. Un classico utilizzo di un directory server è la memorizzazione degli account email o degli utenti registrati ad un sito. |
| *LMTP* | *Local Mail Transport Protocol.* Protocollo applicativo in grado di indicare il successo o il fallimento dell'invio di un dato messaggio ad un dato destinatario. |
| *LOG* | Registrazione cronologica delle operazioni a mano a mano che vengono eseguite e, per estensione, il file su cui tali registrazioni sono memorizzate. |
| *MIME* | *Multipurpose Internet Mail Extensions.* Estensione del formato di posta elettronica standard che consente la trasmissione di contenuti binari con applicazioni specifiche. |
| *MTA* | *Mail Transfer Agent*. Componente software che ha il compito di effettuare lo smistamento dei messaggi di posta elettronica (invio e ricezione). |
| *NTP* | *Network Time Protocol.* Protocollo applicativo per la sincronizzazione degli orologi dei computer all'interno di una rete a commutazione di pacchetto. |
| *PUK* | *Personal Unblocking Key*. Chiave di sblocco personale. |
| *RFC* | *Request for Comments.* Definizioni scritte di protocolli o standard in uso su internet. |
| *S-MIME* | *Secure/MIME*. Versione "securizzata" del formato di posta elettronica MIME. Il formato MIME dei messaggi generati dal sistema di PEC è conforme a quanto definito nelle regole tecniche del servizio di trasmissione di documenti informatici mediante PEC. |

| Termine | Descrizione |
|---|---|
| *SNMP* | *Simple Network Management Protocol.* Protocollo utilizzato per la gestione ed il monitoraggio degli apparati di rete. |
| *SSL* | *Secure Socket Layer.* Protocollo per realizzare comunicazioni cifrate su Internet. Questo protocollo utilizza la crittografia per fornire sicurezza nelle comunicazioni su Internet e consentire alle applicazioni client/server di comunicare in modo tale da prevenire la manomissione dei dati, la falsificazione e l'intercettazione.<br>Scopo primario di SSL è fornire sistemi di crittografia per comunicazioni affidabili e riservate sul Web sfruttabili in applicazioni quali, ad esempio, posta elettronica e sistemi di autenticazione. |
| *TLS* | *Transport Layer Security.* Standardizzazione del protocollo *SSL* portata all'interno dello IETF, dove ha preso tale nome, e documentata nella RFC 2246. Il protocollo *TLS* non è legato al protocollo *HTTP* e può essere utilizzato con altre applicazioni come la posta elettronica. |
| *TSA* | *Time Stamping Authority.* Autorità "super partes" che realizza il servizio di marcatura temporale di documenti informatici. |

# 3 – Il servizio di Posta Elettronica Certificata di UNINA

Ai sensi di quanto prescritto dal Codice dell'Amministrazione Digitale [CAD], la PEC è un sistema per la trasmissione telematica di:

a. comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna;
b. documenti informatici la cui data ed ora di trasmissione e di ricezione siano opponibili ai terzi;
c. comunicazioni di documenti tra le pubbliche amministrazioni che soddisfano il requisito della forma scritta, valide ai fini del procedimento amministrativo e la cui trasmissione non deve essere seguita da quella del documento originale;
d. documenti informatici ed informazioni con i soggetti interessati che ne fanno richiesta e che hanno preventivamente dichiarato il proprio indirizzo di PEC.

Le istanze e le dichiarazioni trasmesse dai cittadini alle pubbliche amministrazioni mediante la propria casella PEC, se effettuate da sistemi PEC coerenti con quanto previsto dal [CAD] per quanto attiene alle modalità di rilascio delle credenziali previa identificazione del titolare[1], sono valide e sono equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento.

Una breve sintesi delle caratteristiche generali di un sistema PEC, ai sensi della normativa vigente, è riportata nel par. 4 del presente manuale. Di seguito, si descrivono le principali caratteristiche tecnico-organizzative del servizio UNINAPEC gestito dall'Università degli Studi di Napoli, coerenti con la normativa vigente in materia di PEC e con il Regolamento di Ateneo [UNINA-PEC].

## 3.1 Caratteristiche principali del Servizio UNINAPEC

### 3.1.1 L'architettura dei domini gestiti da UNINA

Lo schema seguente riporta sinteticamente l'architettura dei domini gestiti da UNINAPEC. In esso, gli utenti UNINA sono identificati con: US1 e US2 se "strutture", con UP1 e UP2 se "dipendenti", con Upr1 e Upr2 se "studenti" o "esterni" (persone fisiche o giuridiche).
L'ulteriore dominio, definito "AltraPA", rappresenta, a titolo indicativo, uno o più domini attivati a servizio di altre PA che per il servizio PEC, ai sensi dell'art. 16 del DPR 68/05 e della nota integrativa n.ro 2 del 6/7/2007 contenuta in [CNIPA INT], chiedono di avvalersi del gestore UNINA attraverso apposita convenzione tra le parti in cui sia regolamentate le modalità di erogazione del servizio; le utenze di tali domini sono identificati con Upa1 e Upa2.

Le linee rosse tratteggiate evidenziano, coerentemente con quanto riportato dall'art. 16, comma 2, del [DPR 68/05], gli scambi di messaggi non ammessi.

[1] Secondo quanto specificato nell'art. 65 comma 1.c-bis) del [CAD].

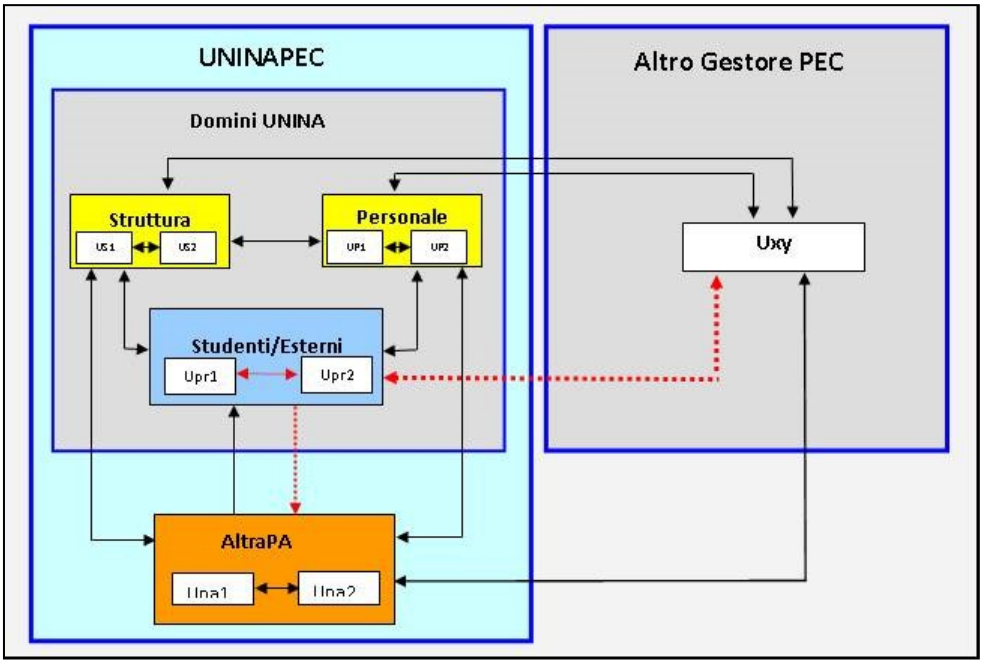


**Figura 3 – *I domini di PEC gestiti da UNINA***

### 3.1.2 Soggetti interessati

Agiscono nel Servizio UNINAPEC i seguenti soggetti:

a. "*Gestore UNINAPEC*", cioè l'Ateneo, in quanto gestore del Servizio UNINAPEC e titolare dei dati personali trattati in tale ambito;
b. *"Centro Servizi Informativi di Ateneo"* ("*CSI"*), in quanto delegato dall'Ateneo ad operare, mediante i propri "*addetti al servizio PEC*", come responsabile della gestione operativa del Servizio UNINAPEC;
c. *"Titolare di dominio PEC",* la pubblica amministrazione (l'Ateneo oppure "*Altra PA"*, definita più avanti) proprietaria del dominio che, in qualità di "terzo interessato" richiede ed autorizza assegnazione e rilascio di caselle PEC ai rispettivi titolari, purché sussistano i presupposti documentati che attestino – caso per caso – la legittimità di tale ruolo;
d. *"Titolare di casella PEC"*, inteso come:
   - assegnatario di una casella UNINAPEC personale,
   - o anche, assegnatario di una casella istituzionale, in qualità di responsabile pro-tempore di struttura o servizio,
   - oppure, delegato dalla propria società/ente ad utilizzare la casella stessa nel caso in cui la casella PEC sia attribuita ad una società/ente esterno al titolare del dominio;

e. *"Utilizzatore di casella PEC",* l'utente che si collega al sistema UNINAPEC per fruirne dei servizi. Coincide con il *titolare di casella PEC* nel caso di casella personale;
f. *"Altra PA",* l'amministrazione pubblica che, in accordo con la normativa vigente, ha richiesto di avvalersi dell'Ateneo quale gestore di posta elettronica certificata.

## 3.2 I flussi di comunicazione tra i domini assegnati ad UNINA

Le caselle di posta elettronica certificata utilizzate da UNINA sono distinte in:

- *caselle istituzionali*: assegnate a strutture, oppure a servizi del titolare del dominio. La titolarità della casella è assegnata al responsabile pro tempore della struttura o del servizio;
- *caselle personali*: assegnate a persone fisiche, ad esempio: dipendenti, studenti, laureati, collaboratori, professionisti, altri soggetti. Sono altresì titolari di caselle personali le persone fisiche che ricoprono incarichi istituzionali (ad esempio, i componenti degli Organi Collegiali dell'Ateneo), oppure i soggetti designati formalmente dal legale rappresentante dell'ente/società come titolari di casella PEC.

Le caselle appartengono, a seconda della finalità per la quale sono assegnate, ad uno dei seguenti domini in uso presso UNINA: "*pec.unina.it", "studentipec.unina.it", "personalepec.unina.it", "ospitipec.unina.it"* rispettivamente destinati a strutture e servizi, personale, studenti nonché soggetti esterni all'Ateneo, nell'ambito dei rapporti istituzionali che questi intrattengono con l'Università. Oltre ai citati, è attivo anche il dominio "*gestorepec.unina.it*", dedicato alle caselle di servizio utilizzate dagli amministratori del sistema UNINAPEC e regolato dalle stesse policy applicate al dominio "*pec.unina.it*".

Pertanto, UNINA utilizza – in qualità di titolare – più domini di PEC, ciascuno regolamentato da specifiche politiche di sicurezza, identificati nel modo seguente:

1. strutture e servizi UNINA: **pec.unina.it**
2. studenti: **studentipec.unina.it**
3. personale: **personalepec.unina.it**
4. esterni: **ospitipec.unina.it**
5. amministratori UNINAPEC: **gestorepec.unina.it**

Lo scambio di messaggi con altri gestori di PEC è consentito ai soli domini "*pec.unina.it", "personalepec.unina.it" e "gestore pec.unina.it"*. Per gli altri due domini (studenti ed ospiti), nel caso di flusso non abilitato, il sistema genera una ricevuta di mancata accettazione/mancata consegna, come di seguito dettagliato caso per caso.
I messaggi provenienti da caselle tradizionali o inviati a caselle tradizionali sono scartati.

Pertanto, rispetto alle limitazioni previste dalla normativa, UNINA inibisce anche l'invio di comunicazioni da utenti esterni (di altro gestore) verso le caselle appartenenti ai domini "*studentipec.unina.it"* e "*ospitipec.unina.it"*.

Tutte le regole vengono implementate a livello di dominio.

Nei paragrafi che seguono, i domini UNINAPEC assegnati ad altre PA sono identificati dalla denominazione "*altrapapec.unina.it*".

Per soddisfare specifiche esigenze di funzionamento dell'Ateneo o in forza di convenzioni stipulate con altri enti, potranno essere creati ulteriori domini.

### 3.2.1 Dominio per le strutture e servizi UNINA (pec.unina.it)

Il dominio "*pec.unina.it*" è riservato agli indirizzi di PEC assegnati alle strutture organizzative, didattiche e di ricerca dell'Ateneo, oppure a servizi. In esso sono anche attivate le caselle assegnate a persone fisiche se demandate all'adempimento di incarichi particolari (ad es. membri degli organi collegiali) ed anche a persone giuridiche che intrattengano particolari rapporti qualificati con l'Ateneo (ad es.: rappresentanze sindacali accreditate).
L'ambito della comunicazione istituzionale può essere sia verso e da utenti degli altri domini UNINA, sia verso e da utenti appartenenti a domini di altri gestori di PEC.
I flussi ammessi per tale dominio sono i seguenti:

| Domini | pec.unina.it invia a: | pec.unina.it riceve da: |
|---|---|---|
| Altri gestori PEC | **SI** | **SI** |
| pec.unina.it | **SI** | **SI** |
| personalepec.unina.it | **SI** | **SI** |
| studentipec.unina.it | **SI** | **SI** |
| ospitipec.unina.it | **SI** | **SI** |
| altrapapec.unina.it | **SI** | **SI** |
| Posta convenzionale | **NO** | **NO** |

Le caratteristiche e le modalità di attivazione delle caselle e di assegnazione di indirizzi di PEC del presente dominio sono definite nel paragrafo 3.4.2.

### 3.2.2 Dominio per i dipendenti (personalepec.unina.it)

Il dominio "*personalepec.unina.it*" è riservato agli indirizzi di PEC assegnati al personale docente, ricercatore e tecnico-amministrativo UNINA.
La finalità primaria della concessione di un indirizzo di PEC in tale dominio è correlata alla attività istituzionale svolta dall'assegnatario nel ruolo, mansioni, funzioni ad esso assegnate, nonché – ai sensi dell'art. 16 della legge [L.2/2009] – alla trasmissione delle comunicazioni al dipendente da parte dell'Università. I flussi ammessi per tale dominio sono i seguenti:

| Domini | personalepec.unina.it invia a: | personalepec.unina.it riceve da: |
|---|---|---|
| Altri gestori PEC | **SI** | **SI** |
| pec.unina.it | **SI** | **SI** |
| personalepec.unina.it | **SI** | **SI** |
| studentipec.unina.it | **SI** | **SI** (*) |
| ospitipec.unina.it | **SI** | **SI** |
| altrapapec.unina.it | **SI** | **SI** |
| Posta convenzionale | **NO** | **NO** |

(*) – Tale flusso potrà essere disabilitato su richiesta motivata del titolare della casella nel dominio personalepec, da inoltrare al Servizio Assistenza Utenti, attraverso uno dei canali riportati nel cap.10.

Le caratteristiche e le modalità di attivazione delle caselle e di assegnazione di indirizzi di PEC del presente dominio sono definite nel paragrafo 3.4.3.

### 3.2.3 Dominio per gli studenti (studentipec.unina.it)

Il dominio "*studentipec.unina.it"* è riservato agli indirizzi di PEC assegnati agli studenti di UNINA.
La finalità primaria della concessione di un indirizzo di PEC agli studenti deriva dalla necessità di comunicazione certificata tra le strutture didattiche e gli studenti, per gli aspetti relativi al rapporto tra UNINA e gli allievi, e tra questi ed UNINA, in merito ad atti ed informazioni precedentemente inviati attraverso posta raccomandata con avviso di ricevuta o ritiro/consegna presso gli sportelli di segreteria. I flussi ammessi per tale dominio sono i seguenti:

| Domini | studentipec.unina.it invia a: | studentipec.unina.it riceve da: |
|---|---|---|
| Altri gestori PEC | **NO** | **NO** |
| pec.unina.it | **SI** | **SI** |
| Personale pec.unina.it | **SI**(*) | **SI** |
| studentipec.unina.it | **NO** | **NO** |
| ospitipec.unina.it | **NO** | **NO** |
| altrapapec.unina.it | **NO** | **SI** |
| Posta convenzionale | **NO** | **NO** |

(*) – Tale flusso potrà essere disabilitato su richiesta motivata del titolare della casella nel dominio personalepec, da inoltrare al Servizio Assistenza Utenti, attraverso uno dei canali riportati nel cap.10.

Le caratteristiche e le modalità di attivazione delle caselle e di assegnazione di indirizzi di PEC del presente dominio sono definite nel paragrafo 3.4.4.

### 3.2.4 Dominio per gli esterni (ospitipec.unina.it)

Il dominio "*ospitipec.unina.it"* è riservato ad indirizzi di PEC concessi da UNINA a persone fisiche e/o giuridiche al solo scopo di rendere possibile una comunicazione certificata nell'ambito di procedimenti ed attività che interessano ambo le parti ed esclusivamente per la comunicazione relativa al rapporto che ha consentito l'assegnazione di tale indirizzo.
E' il caso, ad esempio, di: rapporti derivanti da convenzioni di ricerca tra UNINA e terze parti (pubbliche e/o private), rapporti di fornitura, prestazione d'opera, ecc. I flussi ammessi per tale dominio sono i seguenti:

| Domini | ospitipec.unina.it invia a: | ospitipec.unina.it riceve da: |
|---|---|---|
| Altri gestori PEC | **NO** | **NO** |
| pec.unina.it | **SI** | **SI** |
| personalepec.unina.it | **SI** | **SI** |
| studentipec.unina.it | **NO** | **NO** |
| ospitipec.unina.it | **NO** | **NO** |
| altrapapec.unina.it | **NO** | **SI** |
| Posta convenzionale | **NO** | **NO** |

Le caratteristiche e le modalità di attivazione delle caselle e di assegnazione di indirizzi di PEC del presente dominio sono definite nel paragrafo 3.4.5.

## 3.3 Titolarità delle caselle di PEC

Ogni casella rilasciata da UNINA è associata ad un **titolare** che ne ha la piena responsabilità ed i cui dati identificativi ed anagrafici sono contenuti nelle basi dati istituzionali UNINA per le strutture, i dipendenti e gli studenti, oppure, nell'anagrafica del servizio PEC per gli esterni e per le altre PA. L'identificativo del titolare PEC è costituito

dal suo codice fiscale. Nel caso di strutture/servizi la titolarità è assegnata al responsabile pro tempore della stessa.

## 3.4 Attivazione del servizio

### 3.4.1 Creazione di un dominio UNINAPEC

Su richiesta del *titolare di dominio PEC*, il Gestore UNINAPEC può creare nuovi domini PEC, le cui caratteristiche dipendono delle specifiche esigenze di servizio e di sicurezza da garantire. Nel caso in cui il servizio sia erogato al *Altra PA*, la creazione e la denominazione di un nuovo dominio è definita nell'ambito della convenzione stipulata tra le parti.

### 3.4.2 Caselle del dominio strutture e servizi UNINA (pec.unina.it)

La casella è assegnata alle strutture didattiche, di ricerca o di servizio UNINA, sulla base delle esigenze di servizio stabilite da UNINA.
Nel caso di caselle non di tipo personale, il titolare può, inoltre, incaricare, per iscritto, anche uno o più dipendenti afferenti alla propria struttura ad accedere alla casella di PEC, secondo le prassi operative vigenti in Ateneo per la nomina degli incaricati dei trattamenti dei dati personali mediante sistemi informatici centralizzati.

#### *3.4.2.1 Attivazione di una nuova casella*

La richiesta di nuova casella PEC per una data struttura è comunicata al Gestore dagli uffici competenti, sulla base di specifiche disposizioni organizzative. La procedura di creazione della casella è attivata tramite il Servizio Assistenza Utenti del Gestore. La nuova casella è quindi attivata ed associata al responsabile (pro tempore) della struttura/servizio. Per quanto riguarda invece l'attivazione di caselle da assegnare ad uno specifico servizio, in conformità con quanto previsto in [UNINA-PEC], il responsabile della struttura di riferimento sottoscrive (eventualmente digitalmente) una richiesta di attivazione utilizzando modulo "Richiesta casella PEC" disponibile all'indirizzo http://www.unina.it/UNINAPEC, la protocolla informaticamente e la inoltra (esclusivamente in forma elettronica) al Gestore.
Il Gestore, al completamento dell'iter procedurale previsto per l'attivazione, invia al responsabile, in busta chiusa indirizzata al titolare: le credenziali per l'accesso ad UNINAPEC (costituite dall'indirizzo della casella completo dell'indicazione del dominio ("*pec.unina.it*") ed eventualmente da quelle relative all'identità digitale nel caso di nuova utenza) ed una minima informativa sul servizio PEC, con l'indicazione dell'indirizzo per reperire il presente Manuale Operativo. La busta è inviata presso la struttura di afferenza del titolare, oppure presso l'ufficio amministrativo richiedente, nel caso di rilascio di una casella a persona "avente titolo per ruolo".
Al primo collegamento al sistema PEC, nonché con periodicità non superiore a sei mesi, il responsabile è tenuto ad effettuare il cambio della password utilizzando l'apposita funzione disponibile sulla pagina di accesso al servizio PEC.
Nel caso di smarrimento della password, il titolare può effettuarne il reset, mediante l'omonima funzionalità anch'essa disponibile sulla pagina di accesso al servizio PEC, immettendo il proprio PUK personale di accesso ai servizi integrati di Ateneo, di cui è

provvisto ciascun dipendente UNINA. Nel caso di indisponibilità o smarrimento del PUK, il titolare può inoltrare richiesta di riemissione di tale codice al Servizio Assistenza Utenti del Gestore, secondo quanto previsto dal Regolamento di Ateneo [UNINA-PE].
La password impostata per l'accesso alla casella PEC di servizio non modifica la password personale del titolare, ma ha impatto sulla impostazione della password di accesso a tutti gli eventuali servizi associati allo specifico account attribuito alla struttura (ad esempio, la mail convenzionale).

#### *3.4.2.2 Cambio del titolare della casella*

Il Gestore effettua il cambio di titolarità della casella a seguito della ricezione – via Protocollo Informatico – della comunicazione istituzionale relativa alla nomina del nuovo responsabile pro-tempore effettuata dall'ufficio competente, oppure del nuovo responsabile per un servizio provvisto di casella PEC. Per le caselle assegnate a persone fisiche, "aventi titolo per ruolo", non è previsto il cambio di titolare della casella.
Al primo collegamento al sistema PEC, il nuovo titolare è tenuto ad effettuare il reset della password utilizzando il proprio PUK personale. La password va modificata dal titolare con periodicità non superiore a sei mesi.
Nel caso di indisponibilità o smarrimento del PUK, il titolare può inoltrare richiesta di riemissione di tale codice al Servizio Assistenza Utenti del Gestore, secondo quanto previsto dal Regolamento di Ateneo [UNINA-PE].

### 3.4.3 Caselle del dominio dipendenti (personalepec.unina.it)

Su tale dominio, UNINA assegna – su richiesta dell'Amministrazione UNINA – una casella PEC a ciascun dipendente, indipendentemente dalla carriera di afferenza. Nella fase iniziale di diffusione del servizio, visto che i dipendenti sono già abilitati all'utilizzo dei servizi integrati di Ateneo, la password di accesso alla casella è quella già in uso da parte del dipendente per l'accesso ai servizi integrati stessi ed il PUK è quello già in suo possesso. In tal caso, l'Università inoltra all'interessato, per posta elettronica istituzionale unina ed all'indirizzo della struttura alla quale il dipendente afferisce, una comunicazione che riporta esclusivamente l'indirizzo della casella completo di dominio ("*personalepec.unina.it*"), l'informativa per l'utilizzo del servizio PEC e le indicazioni per reperire il presente Manuale Operativo.
Il nuovo dipendente riceve, in busta chiusa, oltre alle credenziali (costituite dall'indirizzo della casella completo dell'indicazione del dominio "*personalepec.unina.it*" e dal PUK), anche l'informativa per l'utilizzo del servizio PEC con le indicazioni per reperire il presente Manuale Operativo ed è tenuto, al primo collegamento al sistema PEC, a definire la propria password, per mezzo dell'apposita funzione disponibile sulla pagina di accesso al servizio PEC, utilizzando il PUK personale.
In ogni caso, si raccomanda ai titolari di modificare la propria password con frequenza almeno semestrale.
Nel caso di smarrimento della password corrente, il reset può essere eseguito mediante l'omonima funzionalità disponibile sulla pagina iniziale del servizio PEC, immettendo il PUK personale.
Nel caso di indisponibilità o smarrimento del PUK, il titolare può inoltrare richiesta di riemissione di tale codice al Servizio Assistenza Utenti del Gestore, secondo quanto previsto dal Regolamento di Ateneo [UNINA-PE].
N.B.: La modifica o il reset della password modificano la password di accesso alla PEC ed a tutti gli ulteriori servizi integrati di Ateneo a cui è abilitato il titolare della casella.

### 3.4.4 Caselle del dominio studenti (studentipec.unina.it)

Ai fini della comunicazione istituzionale di tipo certificato, UNINA assegna a ciascuno studente una casella di PEC nel dominio *"studentipec.unina.it"*.
Il servizio è erogato, a partire dall'a.a. 2011/12, a tutti gli immatricolati al primo anno per mezzo della creazione ed attivazione automatica della casella al completamento del processo di immatricolazione on-line. Con successive disposizioni, il servizio verrà progressivamente esteso a tutti gli studenti attivi.
Alla casella è assegnata come password di prima connessione quella scelta dallo studente in fase di registrazione ai servizi di accesso ai corsi di studio. Il rilascio dell'indirizzo della casella prevede la sottoscrizione da parte dello studente di una dichiarazione in cui egli si impegna ad utilizzare l'indirizzo di posta elettronica certificata (PEC) assegnatogli dall'Università degli Studi di Napoli e di attenersi alle disposizioni riportate nell'informativa ricevuta dagli incaricati dell'Università.
L'indirizzo della casella ed una sintetica informativa, con il rimando al presente Manuale Operativo, sono rilasciati allo studente attraverso:

1. la procedura di immatricolazione on-line, che prevede anche la conferma di presa visione ed accettazione on-line da parte dello studente della suddetta dichiarazione;
2. la sottoscrizione di un "cartellino identificativo" presso l'Ufficio Segreteria Studenti, ove lo studente deve recarsi per il riconoscimento "de visu" da parte degli addetti di Segreteria. Nel "cartellino identificativo", oltre alla citata dichiarazione di accettazione delle regole di utilizzo della casella PEC, sono riportati, tra l'altro: la foto, il numero di matricola assegnato, il domicilio per le comunicazioni. Altre informazioni e documenti, tra i quali copia di documento di riconoscimento valido, costituiscono il fascicolo di iscrizione e sono già agli atti al momento della sottoscrizione del "cartellino identificativo".

Per gli studenti degli anni successivi al primo, è previsto che la firma di tale dichiarazione sia da essi apposta presso la Segreteria Studenti del proprio Dipartimento prima dell'attivazione della casella.
L'identificativo della casella PEC coincide con quello della mail convenzionale definita sul dominio "*studenti.unina.it*", anch'essa assegnata allo studente in fase di immatricolazione.
Nel caso di smarrimento della password, lo studente può utilizzare il proprio PIN e procedere, sempre dalla schermata iniziale di accesso al servizio PEC, ad effettuare il reset della password.
Infine, nel caso di smarrimento del proprio PIN, lo studente può rivolgersi all'Ufficio Segreteria Studenti del proprio Dipartimento.

### 3.4.5 Caselle del dominio esterni (ospitipec.unina.it)

UNINA, al fine di rendere giuridicamente valida la trasmissione di messaggi ed atti amministrativi inviati a soggetti terzi, ha la facoltà di dotarli di caselle di PEC. In tal caso, il Responsabile del procedimento amministrativo richiedente sottoscrive (eventualmente digitalmente) una richiesta di attivazione utilizzando modulo "Richiesta casella PEC ospiti" disponibile all'indirizzo http://www.unina.it/UNINAPEC, la protocolla informaticamente e la inoltra (esclusivamente in forma elettronica) al Gestore. In tutti i casi, il titolare di casella PEC è una persona fisica, eventualmente incaricata ad utilizzare la casella PEC per conto della persona giuridica esterna a cui afferisce, per un dato procedimento amministrativo.

In particolare, il Responsabile del procedimento amministrativo richiedente dovrà specificare, a seconda dei casi, le seguenti informazioni:

1) i dati del titolare di casella PEC:
   - nome e cognome
   - luogo e data di nascita
   - indirizzo di residenza: via, numero civico, città e CAP
   - codice fiscale
   - indirizzo e-mail non certificato per eventuali comunicazioni
   - un documento di identità o altra documentazione dalla quale si possa risalire all'identità della persona.

2) se è il caso, i dati della persona giuridica per conto della quale il titolare di casella PEC opera:
   - ragione sociale
   - sede legale: via, numero civico, città e CAP
   - codice fiscale
   - partita IVA (se differente dal codice fiscale)
   - indirizzo e-mail non certificato per eventuali comunicazioni
   - nome e cognome del legale rappresentante
   - codice fiscale del legale rappresentante
   - luogo e data di nascita del legale rappresentante
   - documentazione dalla quale si possa evincere l'identità del legale rappresentante.

A valle della creazione ed attivazione della casella, il Gestore, per ciascun titolare, inoltra al Responsabile del procedimento amministrativo richiedente, in busta chiusa intitolata al titolare, le credenziali e l'informativa da consegnare all'assegnatario della casella PEC. Il Responsabile del procedimento amministrativo provvede a custodire le ricevute di accettazione sottoscritte dagli interessati.
Nel caso di smarrimento delle credenziali, il titolare può inoltrare richiesta di riemissione delle stesse al Servizio Assistenza Utenti, secondo quanto previsto dal Regolamento di Ateneo [UNINA-PE].

## 3.5 Cessazione dei domini e delle caselle

### 3.5.1 Cessazione dei domini

La cessazione di un dominio, effettuata su richiesta del *titolare di dominio*, ovvero alla scadenza dell'accordo tra le parti, determina l'avvio della procedura di cessazione di tutte le caselle contenute nel dominio. A valle della cessazione definitiva di tutte le caselle contenute nel dominio, ne viene cancellato definitivamente l'indirizzo ed il contenuto di tutte le caselle.

### 3.5.2 Cessazione delle caselle

Una casella PEC viene a cessare, di norma, alla cessazione del titolo che ha originato il diritto della sua attivazione.
Per le strutture ed i servizi, ad esempio, la casella PEC cessa a seguito del provvedimento amministrativo di cessazione della struttura/servizio stesso. Per le cariche elettive, la casella cessa al completamento del mandato, ecc. Per i dipendenti e gli studenti, al pari, la casella PEC cessa a seguito dell'atto della risoluzione del rapporto con l'Università, secondo quanto prescritto dai Regolamenti di Ateneo [UNINA-PE] e [UNINA-PES], rispettivamente, per i dipendenti e per gli studenti. Di norma, tale periodo è pari a 1 anno (rinnovabile anno per anno su richiesta dell'interessato) per i dipendenti ed è pari a 4 anni

per gli studenti (tale periodo può essere eventualmente prolungato, su richiesta dell'interessato).
Le caselle attivate nel dominio "*ospitipec.unina.it"*, per contro, hanno una scadenza predefinita della durata di dodici mesi, fatto salvo il diritto del Responsabile del procedimento che ne ha richiesta l'attivazione di determinare tale validità per un periodo inferiore o di richiederne l'estensione oltre il limite citato.
La richiesta di variazione del termine di validità, se modifica quanto indicato nel modulo di attivazione, è inviata dal Responsabile del procedimento amministrativo al Servizio Assistenza Utenti, attraverso uno dei canali riportati nel cap.10.
In tutti gli altri casi, l'avvio della procedura di cessazione è operata alla emanazione del relativo provvedimento ovvero al termine del rapporto giuridico che ne ha dato titolo, conformemente ai regolamenti e disposizioni interni di Ateneo sopra citati.

A partire dal momento della richiesta di cessazione della casella:

- il titolare della casella PEC da cessare riceve dal Gestore un messaggio PEC in cui viene notificato l'avvio della procedura di cessazione;
- non è possibile utilizzare la casella per spedire o ricevere nuovi messaggi;
- viene automaticamente azzerata la quota di spazio assegnata alla casella;
- il titolare può accedere alla casella per i 185 giorni successivi alla ricezione del messaggio PEC di avvio della procedura cessazione. Entro i 10 giorni immediatamente precedenti lo scadere di tale termine, il titolare – ovvero il Responsabile del procedimento – può presentare al Gestore una richiesta motivata per la riattivazione della casella. Se la richiesta è autorizzata, ne vengono ripristinate funzionalità e contenuti;
- superato il termine dei 185 giorni, in assenza di richiesta di riattivazione autorizzata dal Gestore, la casella è cessata in modo definitivo: tutti i contenuti sono eliminati e l'indirizzo è reso potenzialmente disponibile per nuove attivazioni.

## 3.6 Accesso al servizio

Per poter accedere alla casella di posta certificata UNINA è sufficiente avere a disposizione un collegamento ad internet ed un browser (Internet Explorer, Firefox, ecc.) e connettersi all'indirizzo:

**https://webpec.unina.it**

immettendo, nei campi predisposti, le proprie credenziali di accesso. In particolare, nel campo "Nome utente" deve essere inserito l'indirizzo PEC assegnato al titolare, completo dell'indicazione del dominio (ad esempio: mario.rossi@studentipec.unina.it) e in quello "Password" la password adoperata per l'accesso alla corrispondente casella di posta convenzionale unina.

Per coloro che possono utilizzare i servizi integrati UNINA previo accesso all'**Area riservata**, disponibile all'indirizzo: http://www.unina.it, la connessione al servizio PEC può avvenire anche tramite l'apposito link ivi disponibile.

A valle della autenticazione, l'utente viene connesso con l'ambiente di fruizione del servizio ove consultare i contenuti della propria casella PEC ed inviare messaggi.

## 3.7 Caratteristiche del servizio offerto

Di seguito, un quadro di sintesi delle principali caratteristiche del servizio UNINAPEC.

**a. Il servizio per l'utilizzo delle caselle UNINAPEC**

UNINA consente l'utilizzo delle caselle di PEC **esclusivamente tramite webmail**, secondo le modalità di cui al par. 3.6. Tale La soluzione si caratterizza per la sua flessibilità e semplicità di utilizzo, non vincolando la disponibilità del servizio UNINAPEC alla configurazione di un client di posta.

**b. I domini e le relative regole**

In generale, le caselle UNINAPEC sono configurate in modo tale da rifiutare tutti i messaggi in ingresso di posta non certificata e da inibire l'inoltro verso indirizzi di posta non certificati.

Inoltre, così come esposto nei precedenti parr. 3.2.1, 3.2.2, 3.2.3 e 3.2.4, a ciascun dominio sono applicabili specifiche policy concordate con il titolare del dominio stesso, nel rispetto della normativa vigente in materia di PEC e del Regolamento di Ateneo [UNINA-PEC].

**c. Tipologie di ricevute**

Per ogni messaggio da inviare è possibile scegliere il tipo di ricevuta di avvenuta consegna. Tale ricevuta può essere:

- completa (contiene il messaggio originale completo),
- breve (contiene il messaggio originale con una codifica hash degli allegati),
- sintetica (contiene i soli dati di certificazione).

Ai fini di ridurre l'occupazione di spazio di ciascuna casella, la scelta proposta dal sistema di PEC UNINA è quella di ricevuta breve. Tale scelta è comunque modificabile, in qualsiasi momento e per ciascun messaggio, dall'utente stesso.

**d. Capacità delle caselle e meccanismi di salvataggio dei messaggi**

Le caselle hanno una capacità di: **120 MB** (domini *"studentipec.unina.it"* e *"ospitipec.unina.it"*), **300 MB** (dominio "*personalepec.unina.it*") e **500 MB**, estendibile, solo nel caso di struttura e su richiesta del titolare, a **2 GB** (dominio "*pec.unina.it*").

Onde evitare che il riempimento dello spazio a disposizione possa causare il rigetto di ulteriori messaggi e la loro conseguente perdita, il titolare si impegna ed è tenuto a svuotare periodicamente la casella, cancellandone i contenuti. A tal fine, l'ambiente offre semplici funzionalità per la copia e l'archiviazione sul proprio computer o altro supporto di messaggi singoli o di intere cartelle di messaggi. Peraltro, al fine di facilitare il controllo dell'occupazione fisica della casella, la % di quota impegnata è indicata da una barra indicatrice colorata posta a margine destro in alto (nel menu laterale di navigazione). Il colore della barra indicatrice varia nel modo seguente:

- verde: occupazione < 70%
- giallo/arancio: occupazione compresa tra 70% e 90%
- rosso: occupazione maggiore 90%

**e. Il servizio di notifica su Posta Elettronica non certificata**

Per migliorare l'utilizzo del servizio, la ricezione di un messaggio PEC è notificabile anche su una casella di posta elettronica ordinaria scelta dal titolare. Nel caso degli studenti e dei dipendenti, il servizio di notifica è attivato in automatico, in fase di

creazione della casella, verso il corrispondente indirizzo di posta elettronica convenzionale assegnato a ciascun titolare.
Alla ricezione della notifica, è opportuno che l'interessato si colleghi tempestivamente alla propria casella PEC per visualizzare, eventualmente salvare il messaggio ricevuto provvedendo se del caso anche alla sua cancellazione per liberare lo spazio occupato.
Il titolare può in qualsiasi momento disabilitare il "servizio di notifica", oppure modificare l'indirizzo della mail convenzionale verso la quale inviare le notifiche.
La mancata consegna di un messaggio di notifica può avvenire per differenti cause anche non dipendenti dalla responsabilità del Gestore e non pregiudica gli effetti e l'efficacia legale del sistema PEC: l'utente è quindi comunque tenuto alla periodica consultazione ed alla diligente gestione della propria casella.

**f. Il controllo dell'esito dell'invio di un messaggio a destinatari multipli**

Nel caso di invio a più destinatari, è possibile attivare la funzionalità detta "micro-mailing list (MML)" che consente, in modo agevole, di monitorare l'esito complessivo della trasmissione visualizzando un rapporto sintetico che evidenzia la avvenuta ricezione o meno delle singole ricevute di consegna, oltre che di quella di accettazione.

**g. La rilevazione della Customer Satisfaction**

Ai sensi dell'art. 63 comma 2 del [CAD], UNINAPEC mette a disposizione dei propri utenti un sistema di rilevazione della Customer Satisfaction, teso a migliorare il grado di soddisfazione degli utilizzatori del Servizio.
Il sistema, realizzato in conformità alle specifiche ed alle raccomandazioni ministeriali in materia [Customer satisfaction], è fruibile direttamente a partire dalla pagina di accoglienza UNINAPEC.

**h. La comunicazione tra il Gestore ed i titolari di casella PEC**

Eventuali comunicazioni da parte degli amministratori UNINAPEC ai titolari avverranno esclusivamente tramite pubblicazione di annunci (ad esempio: la autosospensione del servizio a fronte di anomalie gravi) all'indirizzo: http://www.unina.it/UNINAPEC.

## 3.8 Richiesta dei log dei messaggi

I registri di LOG, il cui trattamento effettuato dal Gestore è diffusamente descritto nel successivo cap. 5, contengono la registrazione di tutte le attività inerenti le trasmissioni di messaggi di PEC ed hanno la stessa validità legale delle ricevute inviate attraverso il sistema di PEC. Nel caso in cui ne abbia esigenza, il titolare può richiedere al Gestore, attraverso il Servizio Assistenza Utenti, un estratto dei file di LOG **solo relativamente a comunicazioni relative alla casella di cui è titolare, quale mittente o destinatario dei messaggi**.

Per richiedere un estratto dei registri di LOG, il titolare deve inviare al Gestore i seguenti dati:

- nome e cognome del titolare, ovvero dati identificativi della struttura;
- indirizzo di PEC assegnato;
- indirizzo di PEC del mittente del messaggio;
- indirizzo di PEC del destinatario del messaggio;
- data di riferimento del messaggio da ricercare;

- oggetto del messaggio da ricercare (opzionale);
- identificativo del messaggio (opzionale);
- indirizzo di PEC per l'inoltro dell'estratto richiesto.

La richiesta, redatta sul modulo "Richiesta LOG PEC" disponibile all'indirizzo http://www.unina.it/UNINAPEC, deve essere firmata dal titolare, con allegata una fotocopia di un documento di identità valido e può pervenire utilizzando uno dei canali (fax o raccomandata A/R) indicati nel capitolo 10. Laddove si intenda inviare la richiesta via PEC, la richiesta deve essere firmata digitalmente dal titolare senza allegare copia di documento identificativo, oppure vanno allegati al messaggio PEC le immagini scansionate del modulo firmato (con firma autografa) e la copia del documento di identità. Se una richiesta proviene da un responsabile di struttura, può essere inoltrata anche via protocollo informatico (codice 1-7-33-1-0) e con oggetto: "SERVIZIO PEC".
La richiesta è elaborata nel primo giorno lavorativo successivo alla ricezione.
Verificati i dati comunicati dal richiedente, il Gestore provvede ad ottenere l'estratto dei registri di log e ad inviarli al titolare attraverso un messaggio di PEC.

## 3.9 Servizio di Assistenza Utenti

Di seguito, viene descritta l'organizzazione del Gestore atta a garantire un diretto, efficace e tempestivo supporto all'utenza sia per quanto attiene i processi di gestione delle anomalie e dei reclami sia per la gestione della comunicazione con il titolare che abbia avanzato richiesta di dati e di informazioni.

### 3.9.1 Il Contact Center

L'organizzazione della struttura del Gestore prevede un **Contact Center multicanale** che fornisce il servizio di contatto all'utente, organizzando e gestendo, mediante l'adozione di idonee procedure, un insieme di risorse umane e di infrastrutture specializzate. Il Contact Center gestisce diversi possibili canali di comunicazione con l'utente sia in entrata (inbound) sia in uscita (outbound). I canali di comunicazione previsti sono illustrati nel Capitolo 10.
Il servizio di assistenza in voce è disponibile dal lunedì al venerdì, dalle ore 8:30 alle ore 17:30 (escluso i festivi). Le segnalazioni pervenute oltre tale orario o in giorno festivo attraverso gli ulteriori canali, sono prese in carico nel primo giorno lavorativo successivo.
Il Contact Center, in base alla tipologia ed alla specificità di segnalazione, provvede al coinvolgimento delle risorse specialistiche del Gestore preposte alla risoluzione dello specifico problema. In particolare, per le anomalie, è attivato il Team di risoluzione, secondo quanto descritto più dettagliatamente nel paragrafo 8.2.
Il Servizio di Assistenza Utenti del Gestore, nel suo complesso:

- fornisce informazioni, delucidazioni e supporto all'utilizzo della PEC nelle fasi di attivazione, cancellazione ed accesso;
- gestisce e coordina l'iter delle segnalazioni di anomalie/disservizi e delle segnalazioni di reclami, assicurando la corretta e tempestiva chiusura di tutte le segnalazioni attivate;
- gestisce ed effettua il monitoraggio dell'iter di ricezione, espletamento e risposta delle richieste di log, di attivazione e di cessazione delle caselle.

Il Servizio di Assistenza Utenti ha anche in carico la verifica del livello di soddisfazione degli utenti della PEC e la raccolta di tali informazioni.

### 3.9.2 Il Sistema di gestione delle segnalazioni

Il Servizio di Assistenza Utenti del Gestore utilizza un sistema applicativo che offre supporto all'operatività delle risorse coinvolte e, tramite il quale, il Gestore tiene traccia di tutte le comunicazioni intercorse con i propri utenti, consentendo anche analisi e documentazione delle attività svolte.
Il sistema di gestione delle segnalazioni consente, in via generale, le seguenti funzionalità:

- apertura di un nuovo ticket su segnalazione da parte dell'utente attraverso uno dei canali illustrati nel capitolo 10 (Canali di comunicazione);
- monitoraggio da parte dell'utente di tutti i vari passaggi di stato del ticket (aperto, confermato, risolto, sospeso, attesa dati utente, inoltrato ad esterno, chiuso);
- notifica degli aggiornamenti del ticket con eventuali annotazioni degli operatori del Contact Center, degli addetti alla risoluzione del problema o dell'utente;
- risoluzione e chiusura del ticket.

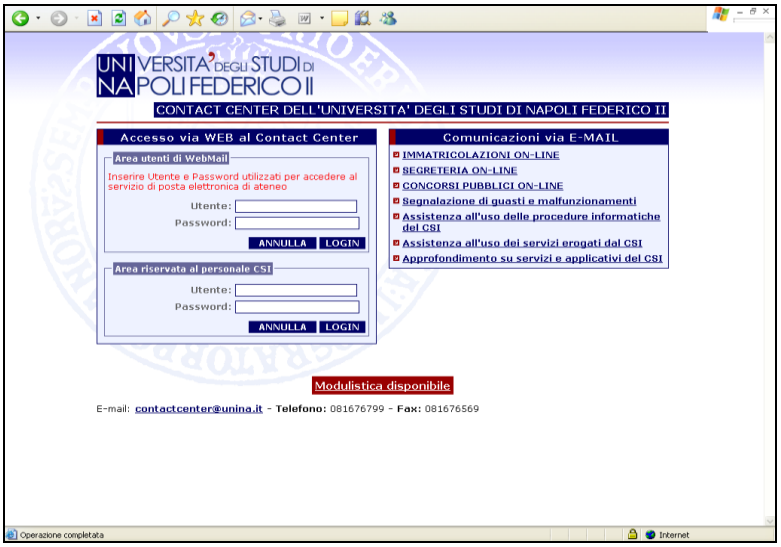


***Figura 4 – Il sistema di gestione delle segnalazioni***

## 3.10 Raccomandazioni per gli utenti

La casella di PEC è uno strumento molto semplice ma, al tempo stesso, molto potente e ciò potrebbe indurre dei malintenzionati ad utilizzarlo per scopi illegali. Pertanto, UNINA raccomanda a tutti i suoi utenti di considerare la propria casella di posta certificata alla stregua di un documento di identità e di adottare una serie di accorgimenti in grado di rendere l'uso del servizio più corretto e sicuro.

In particolare, UNINA raccomanda di:

1. Utilizzare la casella di PEC per inviare comunicazioni o per spedire documentazioni che necessitano di una ricevuta di avvenuta consegna con validità legale.
2. Utilizzare una comune casella di posta elettronica per le altre comunicazioni (che non necessitano di una ricevuta di avvenuta consegna con validità legale).
3. Controllare frequentemente la casella: i messaggi di PEC vengono considerati consegnati a destinazione non appena depositati nella mailbox. A tal fine, si suggerisce di attivare la funzionalità precedentemente descritta di "notifica PEC su

Posta Elettronica non certificata" (v. par. 3.7), in modo tale da ricevere sulla propria casella email non PEC l'alert di arrivo di un messaggio sulla casella PEC.

4. Controllare periodicamente l'occupazione della propria casella di PEC e provvedere all'eliminazione dei messaggi più vecchi in modo che non venga mai raggiunta la capienza massima (con conseguente mancata consegna dei messaggi).
5. Proteggere il computer utilizzato per accedere alla casella di PEC con software antivirus e firewall.
6. Definire la password di accesso utilizzando criteri non banali (ad esempio evitare di inserire il proprio nome, la propria data di nascita o il nome e la data di nascita dei familiari stretti).
7. Modificare periodicamente la propria password (non oltre sei mesi) per aumentare il grado di sicurezza.
8. Usare password di lunghezza superiore agli 8 caratteri e composta da caratteri alfabetici e numerici opportunamente combinati tra loro.
9. Conservare con cura e segretezza le proprie credenziali di accesso.

## 3.11 Interoperabilità con gli altri sistemi di PEC

UNINA si impegna a garantire l'interoperabilità del proprio sistema di PEC con i sistemi degli altri gestori presenti nell'Indice Pubblico dei Gestori (IGPEC).

Per semplificare il controllo dell'interoperabilità, UNINA mette a disposizione degli altri gestori, su richiesta, una casella di posta certificata da utilizzare per i test di interoperabilità.

## 3.12 Livelli di servizio

UNINA assicura il rispetto dei livelli di servizio previsti dalla normativa vigente:

| Livelli di Servizio rispettati dal sistema di PEC UNINA | |
|---|---|
| Numero massimo di destinatari contemporanei accettati in un singolo messaggio | 200 |
| Dimensione massima di ogni singolo messaggio (intesa come prodotto tra il numero dei destinatari e la dimensione del messaggio) | 100 MB |
| Disponibilità nel tempo di riferimento del servizio PEC | ≥ 99,8% nel quadrimestre |
| Durata massima di ogni evento di indisponibilità del servizio PEC | ≤ 50% del totale previsto nel quadrimestre |
| Tempo massimo per il rilascio della ricevuta di accettazione nel periodo di disponibilità del servizio (calcolato escludendo i tempi di trasmissione) | 30 min |

## 3.13 Indicatori di qualità del servizio

UNINA garantisce l'erogazione del servizio di PEC nel rispetto dei seguenti indicatori di qualità:

| Indicatori di qualità del servizio di PEC UNINA |
|---|

| Indicatori di qualità del servizio di PEC UNINA | |
|---|---|
| Disponibilità del servizio (invio e ricezione email) | H24 – 365 gg/anno |
| Disponibilità del servizio di richiesta di attivazione | H24 – 365 gg/anno |
| Tempo massimo per l'esecuzione di interventi di manutenzione che causino il fermo servizio | 2 ore |
| Disponibilità del servizio di richiesta da parte del titolare della traccia delle comunicazioni effettuate (log) | H24 – 365 gg/anno |
| Accesso ai file di log da parte del personale di Università Federico II | Orario di ufficio (*) |
| Tempo massimo per l'invio delle informazioni relative ai file di log dietro richiesta del titolare | 30 giorni |
| Sistema di monitoring con invio di messaggi di alert via email ed sms al presentarsi di malfunzionamenti e situazioni critiche | H24 – 365 gg/anno |
| Assistenza in voce tramite Contact Center | Orario di ufficio (*) |

(*) Per orario di ufficio si intende dal lunedì al venerdì dalle ore 8:30 alle ore 17:30 (escluso i festivi)

# 4 – Descrizione del servizio di Posta Elettronica Certificata

Il presente capitolo descrive le caratteristiche generali di un sistema di PEC, ai sensi della normativa vigente in materia.

## 4.1 Generalità

La Posta Elettronica Certificata (PEC) è un sistema di comunicazione moderno, veloce e sicuro nato con lo scopo di sostituire la tradizionale **Raccomandata con ricevuta di ritorno (o raccomandata A/R)**. In pratica, si tratta di un sistema posta elettronica che aggiunge alcune importanti caratteristiche, prima fra tutte, la prova legale dell'invio e della consegna di documenti informatici.
A chi invia un messaggio di PEC viene recapitata una ricevuta di avvenuta consegna non appena il proprio messaggio giunge a destinazione (viene cioè depositato nella mailbox del destinatario). Tale ricevuta ha validità legale esattamente come avviene per l'avviso di ricevimento di una tradizionale raccomandata.
La PEC può essere utilizzata per inviare ogni tipologia di informazioni (testo, immagini, video, ecc.).
A garanzia del servizio, la normativa prevede l'istituzione dell'**Indice Pubblico dei Gestori di Posta Certificata (IGPEC)**. Si tratta di un elenco di aziende private ed enti pubblici che hanno ottenuto l'accreditamento da parte del CNIPA (oggi AdiD) e, pertanto, possono erogare il servizio cioè fornire singole caselle di PEC, domini certificati, ecc. I gestori hanno l'obbligo di erogare il servizio nel pieno rispetto della normativa vigente, mentre AdID ha il compito di vigilare sul loro operato ed intervenire qualora ravvisi comportamenti scorretti.
Ai sensi di quanto disposto dal D.P.R. 68/2005, le pubbliche amministrazioni possono erogare il servizio di PEC ai propri utenti, per consentire lo scambio di messaggi la cui data ed ora di invio, la trasmissione e la consegna siano opponibili ai terzi.
Le caselle di posta certificata rilasciate ai privati da una pubblica amministrazione iscritta nell'elenco pubblico dei gestori presentano, in base al suddetto decreto, la seguente limitazione: l'utilizzo delle stesse risulta valido unicamente per i rapporti intrattenuti tra i privati con l'amministrazione che le ha rilasciate.
La comunicazione viene realizzata attraverso l'interscambio di messaggi, ricevute ed avvisi che vengono inviati:

- all'utente da parte dei server di posta certificata,
- tra i diversi server di posta certificata.

Ogni messaggio, avviso o ricevuta viene marcato con un riferimento temporale, in modo da certificare in modo esatto gli istanti in cui le comunicazioni sono avvenute.
Tra i compiti di un gestore di PEC vi è anche quello di conservare, per un periodo di 30 mesi, i LOG del sistema che tracciano le comunicazioni avvenute all'interno del proprio sistema. Tali LOG, infatti, hanno la stessa validità legale delle ricevute e possono essere richiesti dagli utenti finali in qualsiasi momento.

## 4.2 Funzionamento di un sistema di Posta Elettronica Certificata

Dal punto di vista dell'utente finale, la casella di PEC è una normale casella di posta elettronica con alcune caratteristiche aggiuntive. In particolare, il sistema prevede la presenza di una serie di ricevute che vengono recapitate al proprietario della casella.
Per ogni messaggio inviato e consegnato, il mittente riceve una **ricevuta di accettazione** ed una **ricevuta di avvenuta consegna**:

- la **ricevuta di accettazione** è un messaggio di posta che ha per oggetto il prefisso "Accettazione:" seguito dall'oggetto originale e che nel testo indica che il messaggio in partenza è corretto ed è stato accettato dal sistema. La ricevuta di accettazione viene inviata dal server di PEC del mittente.
- la **ricevuta di avvenuta consegna** è un messaggio di posta che ha per oggetto il prefisso "Avvenuta consegna:" seguito dall'oggetto originale e che nel testo indica che il messaggio è giunto a destinazione. La ricevuta di avvenuta consegna viene generata dal server di PEC del destinatario; contiene, in allegato, un file xml con i dati di certificazione e può contenere il messaggio originale, completo di allegati.

Il destinatario riceve un **documento di trasporto**, cioè un messaggio di posta che ha per oggetto il prefisso "Posta certificata:" seguito dall'oggetto del messaggio originale e che, nel testo, indica che si tratta di un messaggio di PEC. Il messaggio viene generato dal server di PEC del gestore e contiene, in allegato, la mail originale completa degli eventuali allegati.
Le anomalie – in caso di cattiva formattazione delle mail, presenza di virus, ritardi di consegna ed altri casi particolari – vengono trattate attraverso lo scambio di ricevute ed avvisi particolari. Anche in questi casi, le ricevute hanno un oggetto costituito da un prefisso esplicativo seguito dall'oggetto originale.
Nella figura che segue è descritto – a grandi linee – il funzionamento di un sistema di Posta Elettronica Certificata:

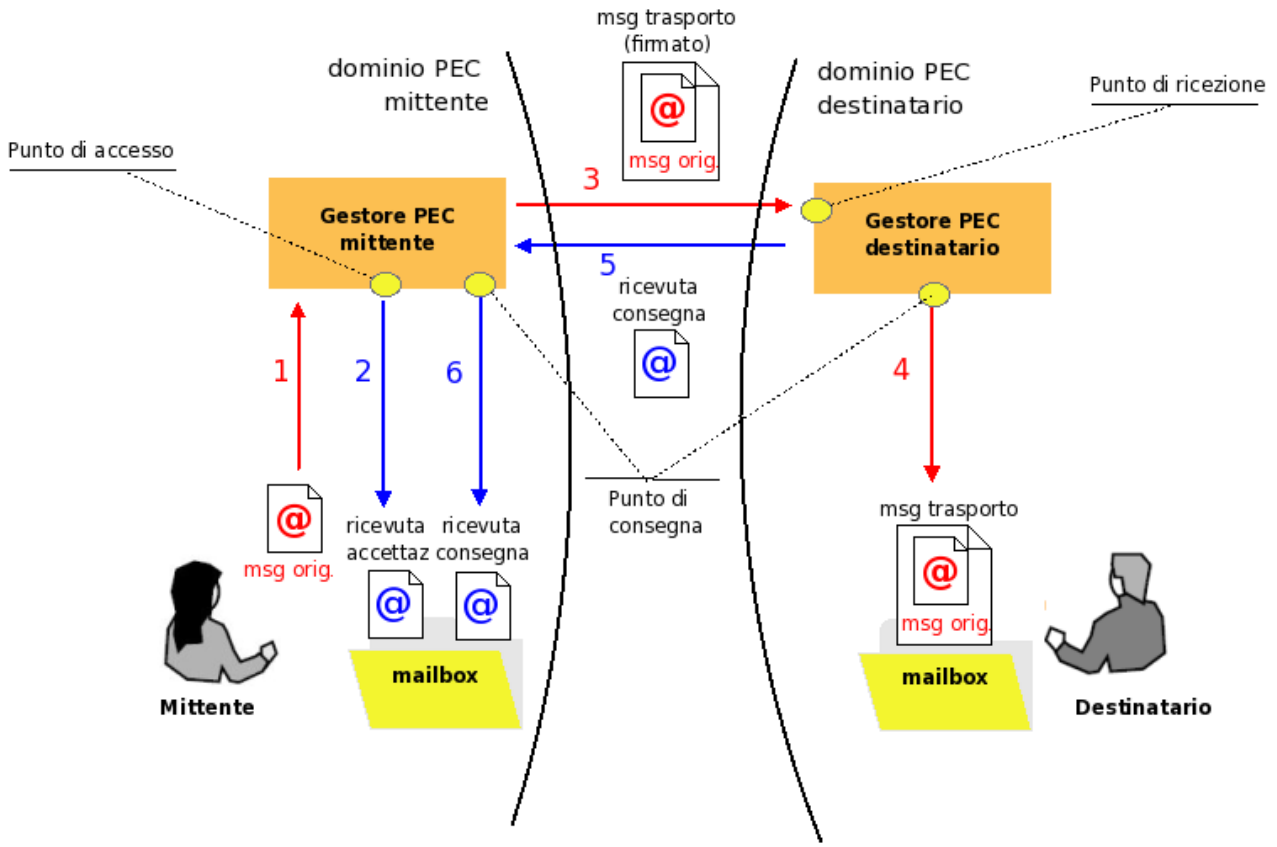


***Figura 5 – Funzionamento di un sistema di PEC***

Nello schema sono visualizzati 2 utenti ciascuno appartenente al proprio dominio di posta elettronica certificata.
Con la stessa numerazione utilizzata nel disegno, si descrive di seguito cosa accade quando il mittente spedisce un messaggio di PEC al destinatario.

1. Il messaggio arriva al **punto di accesso** nel sistema di PEC del server mittente.
2. Il server del mittente, verificato il corretto formato del messaggio, invia una **ricevuta di accettazione** al mittente.
3. Il messaggio viene racchiuso in una busta di trasporto e firmato dal Gestore mittente; in pratica, il messaggio originale viene allegato al messaggio di trasporto.
4. Il server di PEC del destinatario raccoglie il messaggio di trasporto **nel punto di ricezione**, controlla l'attendibilità della firma e verifica che il messaggio non abbia subito alterazioni durante il percorso; dopo aver effettuato tali verifiche deposita il messaggio nella casella del destinatario (**punto di consegna**).
5. Non appena consegnato il messaggio, il server di PEC del destinatario crea una **ricevuta di avvenuta consegna**, appone la firma elettronica del Gestore destinatario e la invia al mittente.
6. Il server di PEC del mittente raccoglie la ricevuta di avvenuta consegna, controlla l'attendibilità della firma, verifica che la ricevuta non abbia subito alterazioni e la consegna al proprio utente (mittente) attraverso il **punto di consegna**.

I gestori di PEC si scambiano dei messaggi "di servizio" allo scopo di garantire la tracciabilità dei messaggi di PEC in transito ed in modo da avere – in qualsiasi istante – la certezza di chi ha in carico un particolare messaggio. Questi tipi di messaggi si chiamano ricevute di **presa in carico**; quando il server di PEC del destinatario riceve la busta di trasporto invia al server di PEC mittente la ricevuta di presa in carico con la quale si prende la responsabilità del messaggio.

La ricevuta di **avvenuta consegna** può essere di 3 tipi:

- **completa**: oltre ai dati di certificazione contiene, sotto forma di allegato, il messaggio originale completo di eventuali allegati;
- **breve**: oltre ai dati di certificazione contiene, sotto forma di allegato, il messaggio originale nel quale gli eventuali allegati vengono sostituiti dallo loro codifica hash;
- **sintetica**: contiene solamente i dati di certificazione senza il messaggio originale.

Generalmente viene utilizzata la ricevuta completa in quanto fornisce al mittente il maggior numero di informazioni possibile: con tale ricevuta infatti il mittente non solo è certo dell'avvenuta consegna del proprio messaggio, ma può anche controllare che quanto consegnato a destinazione corrisponda esattamente a quanto spedito.
La ricevuta breve è stata introdotta per minimizzare l'occupazione di memoria e la dimensione delle email in transito mentre quella sintetica è stata introdotta per poter introdurre procedure automatiche di invio e ricezione di messaggi di PEC.

## 4.3 Alcuni casi particolari

Meritano un approfondimento i casi particolari di seguito descritti.

### 4.3.1 Messaggio formalmente non corretto

Nel caso in cui il messaggio inviato dal mittente sia formalmente non corretto, ossia non rispetti i vincoli formali previsti dalla normativa, il gestore invia al proprio utente (mittente) un **avviso di mancata accettazione per errori formali**. E', ad esempio, il caso in cui la busta di trasporto non è conforme alle specifiche riportate nell'allegato tecnico al [DM

2/11/2005], con particolare riguardo alle specifiche sul formato del messaggio internet [RFC 2822].

### 4.3.2 Presenza virus

Nel caso in cui il gestore del mittente rilevi la presenza di un virus nel messaggio, invia al proprio utente un **avviso di mancata accettazione per virus**.
Nel caso in cui sia il gestore del destinatario a rilevare il virus, il punto di ricezione invia al gestore del mittente un **avviso di rilevazione virus**. Il gestore mittente, alla ricezione di un avviso di rilevazione virus, invia al mittente del messaggio un **avviso di mancata consegna per virus**.

### 4.3.3 Ritardi di consegna

Nel caso in cui il gestore del mittente non riceva alcuna ricevuta di presa in carico nelle 12 ore successive alla spedizione, invia al mittente un **primo avviso di mancata consegna per superamento limiti di tempo**. Con tale avviso il gestore avverte il proprio utente che il messaggio ***potrebbe non arrivare a destinazione***.
Nel caso in cui dopo ulteriori 12 ore non sia stata ancora recapitata la ricevuta di presa in carico, il gestore del mittente invia al proprio utente un **secondo avviso di mancata consegna per superamento limiti di tempo**. Con questo secondo avviso il gestore comunica che la spedizione deve considerarsi ***non andata a buon fine***.

# 5 – Modalità di generazione, conservazione, reperimento e presentazione dei log dei messaggi

In questo capitolo sono descritte le modalità che il Gestore adotta per la gestione dei log e dei messaggi contenenti virus in termini di: generazione, conservazione, reperimento e presentazione delle informazioni al titolare che ne faccia richiesta.

## 5.1 Generazione dei log

Durante le fasi di trattamento dei messaggi, il sistema mantiene traccia delle operazioni svolte memorizzando tutte le attività in registri (LOG) contenenti i seguenti dati:

- codice identificativo univoco assegnato al messaggio originale;
- data e ora dell'evento;
- mittente del messaggio originale;
- destinatario/i del messaggio originale;
- oggetto del messaggio originale;
- tipo di evento (accettazione, ricezione, consegna, emissione ricevute, avvisi, anomalie, ecc.);
- codice identificativo dei messaggi correlati generati (ricevute, avvisi, ecc.);
- gestore mittente.

Gli effettivi dati registrati sui singoli LOG dipendono dalla tipologia dell'operazione tracciata (ricezione di un messaggio, generazione ricevute, ecc.). UNINA garantisce la possibilità di fornire all'interessato che lo richieda (secondo le modalità specificate nel par. 3.8), entro il periodo di 30 mesi dall'invio del messaggio, gli elementi – opponibili a terzi – relativi all'iter del messaggio ed all'esito della trasmissione dello stesso.

## 5.2 Conservazione dei log e apposizione della marca temporale

I registri di LOG prodotti dai sistemi che costituiscono l'architettura tecnica del servizio (descritta nel cap. 6) sono ruotati con frequenza giornaliera, sono "marcati temporalmente", secondo le specifiche riportate nel par. 6.5, sono quindi sottoposti a conservazione sostitutiva, come da [DPCM 2004] e sue successive modificazioni ed integrazioni. Tale procedimento consiste nella generazione, per ciascun log, di un'evidenza informatica che viene sottoscritta digitalmente dal Responsabile della conservazione sostitutiva UNINAPEC ed infine salvata nel sistema di backup UNINA, con storicizzazione dei dati salvati pari a 30 mesi. Durante la fase di apposizione della marca temporale e di conservazione sostitutiva a norma dei file di LOG, un processo provvede ad estrarre le informazioni necessarie per il reperimento dei dati da fornire al titolare. Tali informazioni sono registrate in un database relazionale in cui sono organizzate ed indicizzate per consentirne il successivo rapido ed efficace recupero. In particolare, sono memorizzate:

- Tipo di messaggio: trasporto, consegna, avviso, virus ecc.;
- Message-ID del messaggio originale;
- Message-ID dei messaggi generati correlati al messaggio originale;
- Mittente del messaggio originale;
- Destinatario del messaggio originale;
- Gestore mittente;
- Contenuto completo del messaggio (postacert.eml): solamente in caso di sospetta presenza di virus, come previsto dalla normativa;
- Data ed ora dell'evento;
- Oggetto del messaggio originale.

## 5.3 Reperimento e presentazione dei log

A valle della ricezione della richiesta del titolare, il Gestore effettua il reperimento dei dati mediante ricerca sul database contenente i dati estratti dai registri di LOG dei sistemi. Poiché si opera sui dati indicizzati presenti su tabelle del database, le fasi di identificazione dei LOG sono molto veloci ed efficaci anche nel caso si conoscano solamente pochi elementi relativi alla trasmissione.
L'estrazione dei LOG richiesti, quindi, viene effettuata mediante accesso ai server o agli archivi WORM, dai quali si reperiscono i file di LOG identificati.

Al fine di predisporre il documento da consegnare al titolare che ne ha fatto richiesta, UNINA provvede ad effettuare:

1. copia ed assemblaggio dei log richiesti in un unico archivio;
2. apposizione sull'archivio della firma digitale del responsabile sicurezza dei log dei messaggi (art. 21, comma 1, lettera e) del [DM 2/11/05]);
3. registrazione di protocollo dell'archivio firmato presso il Gestore;
4. trasmissione dell'archivio firmato all'indirizzo di PEC dichiarato nella richiesta dal richiedente.

## 5.4 Conservazione dei messaggi contenenti virus e relativa informativa al mittente

La soluzione UNINA soddisfa i requisiti previsti dalla normativa in merito al comportamento in caso di presenza di virus nei messaggi di PEC inviati o ricevuti dal sistema stesso.
Come per i LOG, anche i messaggi, oppure, le buste di trasporto contenenti virus sono sottoposti a conservazione sostitutiva, in modo tale che possano essere in ogni caso esibiti per un periodo di almeno 30 mesi, anche in caso di disastro.

# 6 – Descrizione della soluzione tecnica

Il presente capitolo definisce l'architettura della soluzione di posta elettronica certificata di UNINA, ne elenca i componenti e descrive l'infrastruttura della server farm del Gestore e le politiche di sicurezza adottate.

## 6.1 Principali caratteristiche tecniche

Dal punto di vista dell'architettura tecnica, il sistema di PEC messo in opera da UNINA ha le seguenti caratteristiche:

1. è pienamente conforme alla normativa vigente in materia di posta elettronica certificata;
2. rispetta i requisiti funzionali previsti dalle regole tecniche del servizio;
3. rispetta i requisiti di interoperabilità previsti dalle regole tecniche del servizio;
4. rispetta i requisiti di sicurezza previsti dalle regole tecniche del servizio per:
   - l'hardware,
   - il software,
   - la rete,
   - le procedure ed i processi utilizzati per erogare il servizio,
   - il personale utilizzato (responsabile, qualificato, preventivamente istruito),
   - la cura e la gestione dei dati sensibili;
5. è scalabile ed estensibile;
6. è perfettamente compatibile con i client di posta che soddisfano i requisiti minimi stabiliti dalle regole tecniche (Outlook, Outlook Express, Thunderbird, ecc.);
7. rispetta lo standard internazionale RFC3161 per quanto concerne la marcatura temporale dei registri di LOG e mediante qualsiasi Time Stamping Authority accreditata;
8. è integrabile con le tipologie di rete più diffuse sul mercato;
9. usa dispositivi hardware ad alta sicurezza per la gestione e il mantenimento delle chiavi di firma;
10. usa dispositivi hardware ad alta sicurezza per la firma e verifica dei messaggi.

## 6.2 Scalabilità ed Affidabilità

Il sistema di PEC UNINA presenta delle caratteristiche di scalabilità che ne consentono la semplice e rapida estensione nel caso in cui ciò si ritenga necessario. Il sistema, infatti, è modulare e consente di suddividere i moduli software su apparecchiature hardware diverse per venire incontro ad esigenze di traffico e di carico.
Il sistema è, inoltre, altamente affidabile e prevede la ridondanza di ogni dispositivo hardware e di ogni modulo software.

## 6.3 Architettura del sistema

La soluzione PEC UNINA si basa sul prodotto **OpenPEC versione 2 (OpenPEC 2)**.
OpenPEC (www.openpec.org) è un progetto Open Source nato con lo scopo di realizzare un sistema di Posta Elettronica Certificata conforme alle linee guida indicate dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA, oggi AdID).

L'architettura di seguito riportata descrive l'architettura tecnica di massima del sistema di posta certificata UNINA. Lo schema e la descrizione che seguono non hanno lo scopo di essere esaustivi circa il numero o la tipologia dei server coinvolti.

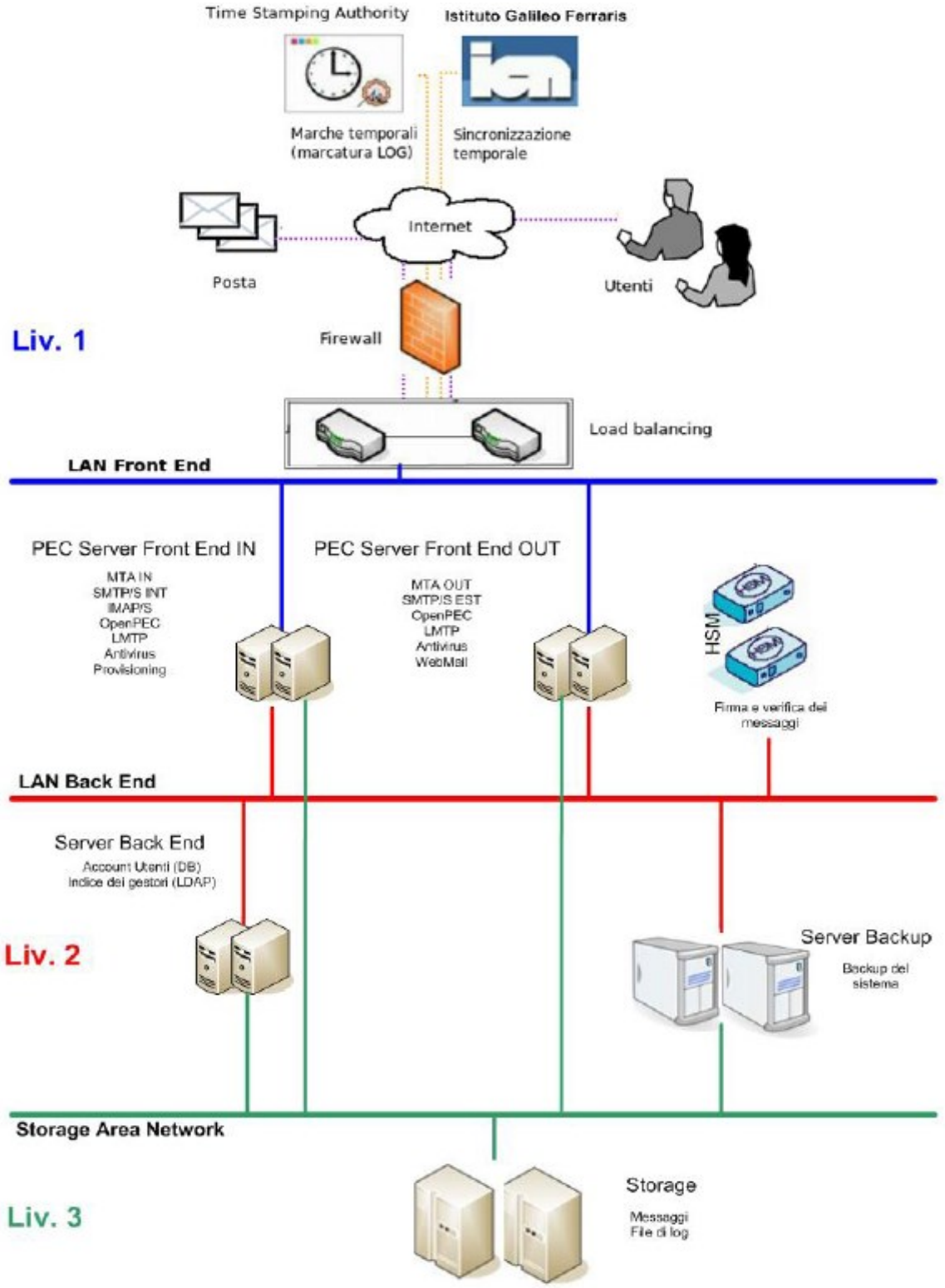


***Figura 6 – Architettura della soluzione***

L'architettura tecnica della soluzione, come si evince dallo schema sopra riportato, può essere suddivisa in 3 livelli:

- **Primo livello.** Il primo livello è costituito dagli apparati di rete (router, switch), dal modulo firewall per la protezione del sistema da accessi indesiderati, ed i load balancer che si occupano di suddividere il carico tra le varie macchine.
- **Secondo livello.** Il secondo livello rappresenta il modulo **PEC**, cioè il centro di elaborazione principale e l'interfaccia verso i dispositivi di memorizzazione.
  Contiene 5 gruppi di macchine: **PEC server Front End IN**, **PEC server Front End Out, server Back End, server Backup** e **HSM.**
  - **PEC server Front End IN**
    Il gruppo di macchine PEC server Front End IN si occupa delle mail in ingresso. Sulle macchine è installato il modulo **MTA** che si incarica del mail routing, il modulo antivirus, il nucleo centrale del sistema **OpenPEC**, il server **IMAP** (per l'accesso alla casella di posta tramite browser) ed il sistema di provisioning (per la creazione e gestione degli account e dei domini di PEC). All'interno di questo gruppo di macchine è inoltre implementata la sincronizzazione con l'Istituto Galileo Ferraris di Torino mediante protocollo NTP e l'interfaccia con una Time Stamping Authority, allo scopo di effettuare la marcatura giornaliera dei log.
  - **PEC server Front End OUT**
    Il gruppo Front End OUT si occupa delle mail in uscita. Oltre ai moduli **MTA**, **OpenPEC** e **antivirus**, sulle macchine è installato il server **SMTP** (per la spedizione delle mail) ed il modulo di **web mail** (per l'accesso alla casella di posta attraverso un comune browser web).
    All'interno di questo gruppo di macchine è inoltre implementata la sincronizzazione con l'Istituto Galileo Ferraris di Torino mediante protocollo NTP e l'interfaccia con una Time Stamping Authority allo scopo di effettuare la marcatura giornaliera dei log.
  - **Server Back End**
    Il gruppo di macchine **server back end** contiene il database degli account ed il mirror dell'indice pubblico dei gestori tenuto da AdID, memorizzato su server LDAP.
  - **Server Backup**
  - Il gruppo di macchine **Server backup** effettua il backup dei dati previsti dalla normativa vigente in materia di PEC, nonché tutte le informazioni necessarie a garantire l'alta disponibilità del sistema.
  - **HSM**
    I moduli HSM (Hardware Security Module) si occupano della firma e della verifica dei messaggi inviati e ricevuti.
- **Terzo livello:** Il terzo livello rappresenta il **data store** del sistema e contiene le mailbox degli utenti ed i file di log memorizzati all'interno di uno storage condiviso.

## 6.4 Principali componenti della soluzione

Di seguito si riporta uno schema che descrive i principali componenti della soluzione:
Come rappresentato in esso, esiste un nucleo centrale del sistema (OpenPEC) che si interfaccia con tutti gli altri moduli:

- il Mail Transfer Agent (MTA) che si incarica del "dispatching" delle mail,
- il modulo Antivirus,
- il server LDAP (che contiene gli account ed il mirror dell'indice dei gestori),
- il server LMTP,
- i moduli HSM utilizzati per la firma dei messaggi,
- lo storage (file system),

- il server POP-IMAP,
- il modulo di provisioning (per la creazione/modifica degli account) richiamabile attraverso interfaccia SOAP,
- il modulo di web mail.

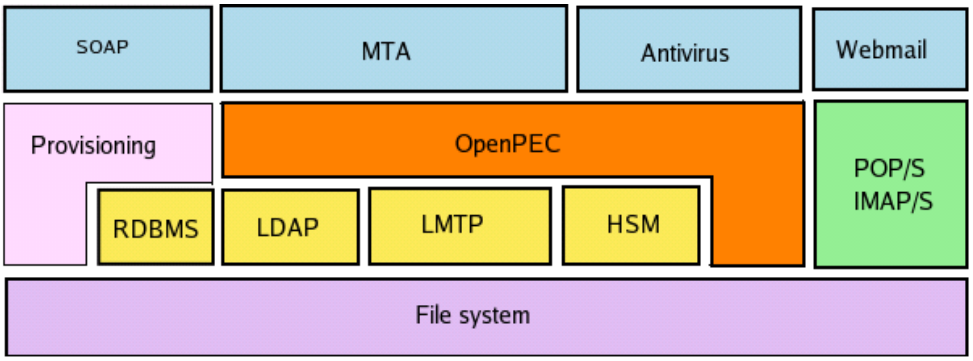


***Figura 7 – Componenti del sistema***

Tutti i componenti utilizzati per l'erogazione del servizio UNINAPEC sono prodotti open source, in linea con le strategie adottate da UNINA nella scelta delle nuove piattaforme tecnologiche di riferimento per l'evoluzione dei propri servizi informatici.

## 6.5 Riferimenti temporali e Marche temporali di UNINA

### 6.5.1 Riferimenti temporali

In base all'art.10 del [DPR 68/2005] e sulla base di quanto riportato nel [DM 2/11/05], il Gestore appone un **riferimento temporale** su tutti gli eventi che costituiscono la transazione di elaborazione di un messaggio di PEC (generazione di ricevute, buste di trasporto, log, ecc.). Il riferimento temporale può avere uno scarto non superiore ad 1 minuto secondo rispetto alla scala di riferimento UTC (Coordinated Universal Time).
Allo scopo di avere un riferimento temporale coerente in tutte le macchine, il sistema si interfaccia con un pool di server NTP tra i quali l'Istituto Elettrotecnico Nazionale Galileo Ferraris (IEN) di Torino.
Il formato della data è ***gg/mm/aaaa*** dove:

*gg* sono le 2 cifre del giorno,
*mm* le 2 cifre del mese e
*aaaa* le 4 cifre dell'anno.

Il formato dell'ora è ***hh:mm:ss*** dove:

*hh* sono le 2 cifre delle ore (su 24 ore),
*mm* le 2 cifre dei minuti,
*ss* le 2 cifre dei secondi.

Nei riferimenti temporali è riportata inoltre, tra parentesi, la differenza, in ore e minuti dell'ora legale locale con il riferimento UTC (Coordinated Universal Time). Il valore di tale differenza è preceduto da un segno + o – che indica la differenza positiva o negativa rispetto ad UTC.
Ad esempio:

*22/03/2007 10:22:06 (+0100)*
indica il 22 marzo 2007, ore 10, 22 minuti, 6 secondi,
1 ora avanti rispetto al riferimento UTC.

### 6.5.2 Marche temporali

Il [DM 2/11/05] stabilisce, tra l'altro, che ogni sistema di posta elettronica certificata deve eseguire, senza soluzione di continuità, il salvataggio dei registri di log dei messaggi con un intervallo di tempo non superiore alle 24 ore. Per fissare in maniera inequivocabile l'istante in cui il registro viene archiviato, UNINA utilizza le **marche temporali**, ossia riferimenti temporali che vengono validati da una terza parte fidata, la cosiddetta **Time Stamping Authority** (**TSA**).
La validazione temporale di un documento informatico consiste nella generazione di una firma digitale, così da poter attribuire al documento in oggetto un riferimento temporale (data ed ora) sicuro e verificabile. L'interfacciamento tra il sistema di PEC e la TSA avviene secondo lo standard RFC 3161 (http://www.ietf.org/rfc/rfc3161.txt).

## 6.6 Descrizione della server farm UNINA

Il servizio di PEC erogato dal Gestore si basa sull'utilizzo di una piattaforma fortemente integrata nell'architettura tecnologica ed applicativa UNINA, ove tutte le risorse hardware e software, connesse ed interoperabili attraverso la rete di Ateneo, sono installate presso i due CED (ubicati presso le sedi CSI del Centro Storico e di Monte S. Angelo) ed ospitano i sistemi istituzionali di Ateneo per la gestione della didattica, della ricerca, del personale, della contabilità e finanza, del protocollo informatico, delle biblioteche digitali, del portale di Ateneo e della posta elettronica (convenzionale e PEC). Le tecnologie utilizzate sono eterogenee e multivendor, con una progressiva standardizzazione – soprattutto per quanto concerne sistemi operativi e software di base – verso l'utilizzo di prodotti open source.

### 6.6.1 La rete UNINA

L'infrastruttura di rete, realizzata completamente in fibra ottica G.652 e completamente gestita in proprio dall'Ateneo, prevede l'interconnessione delle sedi dell'Università e di principali enti di ricerca presenti sul territorio ai nodi di trasporto o GigaPoP Metropolitani, che costituiscono il primo livello topologico della rete metropolitana *(componente di trasporto o core).* A tali GigaPoP sono collegate tutte le sedi dell'Università o di altri enti costituenti i Punti di Accesso metropolitani.

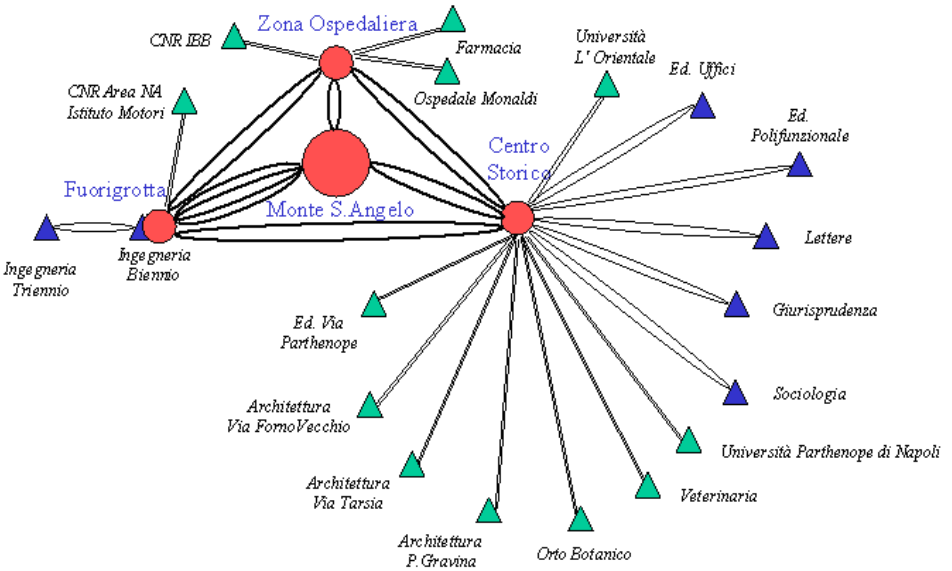


***Figura 8 – Schema dei collegamenti in fibra ottica della rete UNINA***

Come si può notare dalla figura, sono stati realizzati quattro punti principali di erogazione, che individuano i GigaPOP, fra loro completamente magliati, uno dei quali assume un ruolo privilegiato di centro della rete (il POP di Monte S. Angelo, che ospita i collegamenti verso Internet e i peering verso le altre reti che partecipano all'iniziativa). Sfruttando la magliatura completa è stato possibile realizzare 4 anelli logici che garantiscono multipli collegamenti fra i GigaPOP. Inoltre, al fine di aumentare la tolleranza dell'intero sistema rispetto ai guasti e renderlo già pronto ad una gestione dinamica ottimizzata dei path (collegamenti logici con specifici requisiti di banda, affidabilità e QoS) direttamente dagli apparati di trasporto/distribuzione, si è ritenuto opportuno duplicare tutti i collegamenti tra le diverse sedi.
La topologia realizzata consente in maniera intrinseca di aumentare la disponibilità della rete, riducendo drasticamente i tempi di fermo in caso di guasto della fibra ottica anche in casi estremi come il tranciamento accidentale dell'intero cavo (in conseguenza, per es., di una trivellazione errata) in un punto dell'anello.
La connettività "internet commodity" è realizzata attraverso 4 collegamenti 1Gbps Ethernet direttamente terminati sul polo GARR di Napoli, di cui 2 destinati al calcolo scientifico.

### 6.6.2 Descrizione dei locali della sede di erogazione

I sistemi che costituiscono l'architettura tecnica del servizio di PEC sono ubicati presso il CED del CSI a Monte S. Angelo. Tale struttura è collegata, tramite la rete di trasporto metropolitana illustrata nel paragrafo precedente, al CED CSI del Centro Storico, che funge da sito per gestire il recovery del servizio.

### 6.6.3 Accesso agli ambienti e standard di sicurezza adottati

Il CED di Monte S. Angelo è dotato dei seguenti sistemi di sicurezza di tipo logistico:

| Funzione di sicurezza di tipo logistico | Meccanismo |
|---|---|
| Sistemi di controllo accessi fisici | ○ Porta di accesso unica con badge e lettore biometrico<br>○ Impianto antintrusione<br>○ Videosorveglianza |
| Sistemi di rilevazione passiva | ○ Rilevatore incendio<br>○ Rilevatore di fumo |
| Infrastrutture | ○ Estintori<br>○ Condizionamento ambiente e segnalazione anomalie<br>○ Quadro elettrico chiuso a chiave |
| Sistemi di continuità di alimentazione | ○ Sistema UPS<br>○ Inverter per stabilizzazione<br>○ Gruppo elettrogeno |
| Armadi specifici per i server di PEC | ○ Dislocazione dei server adibiti all'erogazione del servizio di PEC in appositi armadi chiusi a chiave |

## 6.7 Misure di sicurezza informatiche

Il sistema reso disponibile da UNINA soddisfa tutti i requisiti di sicurezza previsti dalla normativa vigente, con particolare riguardo a quella in materia di gestione del servizio di posta elettronica certificata e di protezione dei dati personali. Riportiamo, nei seguenti paragrafi, una breve descrizione delle misure di sicurezza adottate. Tali misure sono dettagliate in modo approfondito nel **Piano di Sicurezza**, un documento riservato, custodito presso AdID, redatto in base alle disposizioni della circolare [CNIPA/CR/49]. Tale documento è coerente con quanto riportato nel DPS UNINA, contenente l'analisi delle vulnerabilità e dei rischi incombenti sui dati personali trattati con strumenti elettronici da UNINA, in attuazione del [D.lgs. 196/2003].

### 6.7.1 Identificazione e autenticazione

Il servizio di PEC utilizza un sistema centralizzato basato su tecnologia LDAP per la verifica dell'identità dichiarata da un utente che vuole accedere al sistema.
L'identificazione e l'autenticazione sono effettuate prima di ulteriori interazioni tra il sistema e l'utente e sono basate sull'utilizzo di credenziali (userid/password) dell'utente. La password deve essere lunga almeno 8 caratteri. Per consentirne il cambio, oppure il reset, da parte dell'utente, il Gestore ha reso disponibili due apposite funzionalità sull'interfaccia di presentazione di accesso al servizio.

### 6.7.2 Controllo autorizzazione

Il sistema garantisce la possibilità di associare, sulla base delle credenziali immesse dall'utente, la tipologia di dominio (e quindi, di politiche e di sicurezza da applicare). Inoltre, è assicurata la riservatezza dei messaggi: ciascun utente può infatti accedere esclusivamente alla propria mailbox.

### 6.7.3 Tracciamento

Ciascuna operazione di firma dei messaggi, avvisi e ricevute svolte dal sistema di posta elettronica certificata UNINA viene tracciata in un registro di controllo (registro di LOG) al quale viene associata, con frequenza almeno giornaliera, una marca temporale.

### 6.7.4 Sistemi che evidenziano eventi anomali

Lo stato del sistema viene costantemente controllato mediante un sistema di controllo e gestione eventi anomali che si preoccupa di controllare la disponibilità dei servizi e di allertare:

1. mediante segnalazioni visive sulle postazioni in una sala ad accesso controllato;
2. mediante mail e SMS al personale dedicato alla gestione del sistema.

### 6.7.5 Oscuramento dati d'archivio

Le password degli utenti, custodite su LDAP, sono crittografate con algoritmo SHA-1, in modo tale da garantirne la riservatezza. In caso di perdita/dimenticanza della password, l'utente provvede autonomamente al reset della stessa tramite le funzionalità messe a disposizione e secondo le modalità illustrate al paragrafo 3.4 in funzione della categoria di utenza.

### 6.7.6 Rilevazione e ripristino affidabilità software

I server dedicati all'erogazione del servizio sono aggiornati tempestivamente non appena è annunciata la disponibilità di nuove "patch", al fine di renderli meno vulnerabili in caso di errori o di tentativi di attacco fraudolento. Inoltre, sui server sono installati prodotti per

l'analisi del software al fine di identificare, segnalare e correggere violazioni dell'integrità. Fra tali funzioni vi sono quelle di identificazione ed eliminazione dei virus, bombe logiche e "cavalli di troia", analisi del codice per verificare l'integrità degli eseguibili, la correttezza delle chiamate ai dati, ecc.

### 6.7.7 Qualità dei dati

Il sistema è realizzato in modo tale da garantire la qualità dei dati gestiti, in termini di: *accuratezza* (garanzia che il contenuto di ogni dato, in ciascuno dei suoi attributi, sia dettagliato in maniera significativa e priva di errori); *completezza* (garanzia che un determinato dato sia previsto nello schema strutturale e sia valorizzato in tutti i suoi elementi in base ai requisiti informativi); *conformità* (garanzia che il contenuto del dato sia in armonia col contenuto degli altri dati, rispettando l'insieme dei vincoli logici e referenziali che legano i dati tra loro); *interpretabilità* (garanzia che il valore del dato sia comprensibile per tutti i possibili utenti, senza adito ad alcuna ambiguità); *tempestività* (garanzia che il valore del dato risulti aggiornato al momento in cui viene reso disponibile all'utente finale in ragione delle esigenze di utilizzo).

### 6.7.8 Duplicazione dati/risorse

L'architettura del servizio prevede la ridondanza delle risorse, al fine di garantire l'efficace e tempestivo ripristino in caso di malfunzionamenti. L'architettura di sistema è configurata in alta disponibilità, prevedendo l'utilizzo di apparati e di sistemi ridondati (alimentazione, rete, server, dischi, ambienti applicativi, ecc.).

Per quanto riguarda i dati, sono sottoposti a procedura di salvataggio le seguenti risorse: i log del sistema, i log dei messaggi PEC, i messaggi contenenti virus marcati temporalmente, gli account ed i profili utente e l'indice dei gestori PEC.

Il back-up di tali dati è eseguito quotidianamente mediante creazione di copie di salvataggio incrementali su disco, presso il CED C.S.I. di Monte S. Angelo, e loro storicizzazione in modalità GFS su nastro, custodito presso il CED C.S.I. del Centro Storico, con retention di 15 giorni. Gli stessi backup vengono effettuati, in modalità "FULL", con cadenza settimanale.

In particolare, i log dei messaggi PEC ed i messaggi contenenti virus sono sottoposti a conservazione sostitutiva, con retention non inferiore a 30 mesi.

### 6.7.9 Controllo interscambio dati

UNINA garantisce l'utilizzo di meccanismi atti ad assicurare la sicurezza nelle trasmissioni di dati attraverso: autenticazione e controllo delle autorizzazioni dell'originatore, integrità e riservatezza del contenuto del messaggio, non ripudio dell'originatore e del destinatario.
Di seguito, si descrivono i meccanismi utilizzati da UNINA, dando particolare risalto all'utilizzo degli apparati HSM per la firma elettronica avanzata dei messaggi.

#### *6.7.9.1 Meccanismi generali*

In particolare, mediante l'utilizzo di router di rete, viene svolto il controllo perimetrale di anti-intrusione. Inoltre, presso la sede del CED di Monte S. Angelo, è installato un firewall, che svolge funzioni di packet filtering e proxy server. I server che compongono l'architettura del servizio di PEC sono dotati di certificati elettronici qualificati di tipo "Global

Trust" rilasciati da GARR, di cui UNINA è Registration Authority, garantendo così, mediante l'uso di protocolli e connessioni sicure (HTTPS, FTPS, SMTP/S, ecc.), che un'entità di pari livello in una comunicazione è quella che dichiara di essere. La riservatezza dei messaggi è garantita mediante l'utilizzo, da parte dell'utente, di certificati elettronici qualificati S/MIME.
Infine, l'utilizzo di certificati elettronici qualificati di firma digitale rilasciati da AdID garantisce l'autenticità e la non ripudiabilità dei messaggi inviati mediante il sistema di PEC UNINA. A tale scopo, UNINA memorizza i certificati e le chiavi crittografiche in idonei dispositivi di firma HSM, di seguito dettagliatamente illustrati.

#### *6.7.9.2 Dispositivi di firma (HSM)*

La generazione e la gestione delle chiavi e dei certificati di firma viene svolta all'interno di appositi dispositivi chiamati **HSM**, **Hardware Security Module**. Le stesse apparecchiature vengono inoltre usate per la firma dei messaggi di PEC e per la loro successiva verifica.
Lo standard del **National Institute of Standards and Technology** (**NIST**) indica i requisiti di sicurezza che devono essere rispettati dai moduli crittografici utilizzati in sistemi che trattano dati sensibili. I requisiti di sicurezza riguardano le interfacce e le regole di autenticazione, nonché il livello fisico ed il processo di gestione delle chiavi e dei certificati.

UNINA ha scelto di utilizzare dei moduli HSM con certificazione **FIPS 140-2 level 3** che presentano caratteristiche di sicurezza tali da evidenziare tentativi di accesso non autorizzato e da eliminare le chiavi presenti nel caso di tentativi di manomissione.

## 6.8 Organizzazione del personale

Coerentemente con quanto previsto dal [DM 2/11/05], UNINA ha individuato e nominato i seguenti responsabili del servizio UNINA:

- Riferimento del Servizio,
- Responsabile della Registrazione dei Titolari,
- Responsabile dei Servizi Tecnici,
- Responsabile delle Verifiche e delle Ispezioni (auditing),
- Responsabile della Sicurezza, dei Log dei messaggi e del Sistema di riferimento temporale,
- Responsabile del Contact Center.

Tutto il personale coinvolto nell'erogazione del servizio è in possesso delle conoscenze e dell'esperienza necessaria a svolgere i compiti assegnati ed è coinvolto dal CSI in un percorso di formazione ed aggiornamento continuo sulle tecnologie e sulle applicazioni gestite.
Ogni responsabile si avvarrà del supporto del direttore tecnico del CSI della propria area di afferenza, in modo tale da individuare, ciascuno per quanto di propria competenza, le soluzioni tecnico-organizzative più idonee per garantire il funzionamento a norma del servizio "UNINAPEC" ed assicurare il rispetto delle procedure operative previste dal Sistema Gestione Qualità del Servizio.

# 7 – Protezione dei dati personali

Il presente capitolo descrive i processi e le modalità operative adottate da UNINA, in qualità di titolare del trattamento dei dati personali, nello svolgimento della propria attività di gestore del servizio di PEC.
Le informazioni personali dei titolari vengono trattate, conservate e protette in conformità a quanto previsto nel [DLgs 196/03], nel Regolamento di Ateneo [UNINA-Privacy], nonché nel Regolamento di Ateneo [UNINA-PEC].

## 7.1 Definizioni

| Definizioni in materia di trattamento dei dati personali | |
|---|---|
| Dato personale | Ai sensi dell'art. 1 comma 2 lett. B) del D.lgs, per dato personale si intende: qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. Pertanto, sono dati personali anche i codici identificativi forniti dal gestore.<br>Dati personali sono anche quelli relativi all'utente ovvero ad eventuali terzi e contenuti nei campi informativi presenti sui moduli e negli archivi – elettronici e/o cartacei – di registrazione, di richiesta di sospensione, di riabilitazione, di revoca, di cambio anagrafica e nei certificati di cui al presente manuale operativo. |
| Trattamento | Qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati. |
| Titolare del trattamento dati | Persona fisica, giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. |
| Responsabile del trattamento | Persona fisica, giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare, al trattamento dei dati personali. |
| Incaricato del trattamento | Persona fisica autorizzata a compiere operazioni di trattamento dal titolare del trattamento dati o dal responsabile. |
| Interessato | Persona fisica, persona giuridica, ente o associazione cui si riferiscono i dati personali |

## 7.2 Attuazione della normativa

Il Titolare del trattamento dei dati personali utilizzati in tutte le fasi di gestione del servizio di PEC è il Gestore del servizio, cioè l'Università degli Studi di Napoli Federico II, con sede in Corso Umberto I - 80138 Napoli. Per ulteriori informazioni sul tema del trattamento dei dati personali si può fare riferimento a quanto indicato sul sito dell'Università all'indirizzo: http://www.unina.it/ateneo/attiNorme/sicurezza.
In ottemperanza a quanto disposto dal [D.lgs. 196/2003] e dai propri regolamenti di Ateneo, UNINA definisce le politiche di sicurezza per la tutela dei dati personali trattati ed individua i meccanismi di sicurezza da implementare, al fine di minimizzare il rischio di perdita dell'integrità, della riservatezza e della disponibilità dei dati.
All'interno di UNINA i dati personali sono trattati da personale UNINA nominato, a seconda del ruolo e dei compiti assegnati, quale responsabile, incaricato oppure amministratore di sistema. Eventualmente, UNINA si può avvalere di altre società per la manutenzione dei sistemi informatici e, in tal caso, nomina, a seconda dei casi, i responsabili, gli incaricati del trattamento o gli amministratori di sistema tra il personale di tali società. I nominativi di tali soggetti sono a disposizione degli interessati che ne facciano richiesta.

## 7.3 Tutela e diritti degli interessati

Ai sensi del [Dlgs 196/2003], UNINA garantisce che i dati personali degli interessati saranno trattati secondo i criteri di liceità, di necessità, di non eccedenza, di pertinenza e di correttezza, nel rispetto della normativa vigente e dei regolamenti emanati dall'Università.

Il conferimento dei dati personali è facoltativo, salvo che sia richiesto da specifiche normative.

L'eventuale rifiuto di conferire i propri dati comporta l'impossibilità per UNINA di erogare il servizio in oggetto.

Ai sensi dell'art. 13 del citato [D.lgs. 196/2003], UNINA fornisce agli interessati tutte le informazioni necessarie in relazione a: titolare del trattamento, finalità e modalità del trattamento, diritti di accesso ai dati personali ed ambito di comunicazione dei dati dell'interessato.

L'interessato può esercitare i diritti previsti dall'art. 7 del [D.lgs. 196/2003], di seguito riportato, chiedendo di conoscere i nominativi dei responsabili del trattamento dei dati, di accedere ai propri dati per conoscerli, verificarne l'utilizzo o, ricorrendone gli estremi, farli correggere, chiederne l'aggiornamento, la rettifica, l'integrazione, la cancellazione od opporsi al loro trattamento, rivolgendo richiesta scritta all'indirizzo riportato al Capitolo 10. Alla richiesta deve essere allegata copia di un documento identificativo valido del titolare della casella.

Le richieste sono prese in carico nel primo giorno lavorativo successivo alla loro ricezione.

| D. Lgs. 196/2003, Art.7 – Diritto di accesso ai dati ed altri diritti |
|---|
| 1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile. |

2. L'interessato ha diritto di ottenere l'indicazione:
   a) dell'origine dei dati personali trattati;
   b) delle finalità e modalità del trattamento;
   c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
   d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma2, del D. Lgs. 196/2003;
   e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
   a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
   b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
   a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
   b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.



## 7.4 Finalità del trattamento

Il trattamento cui saranno sottoposti i dati personali richiesti o acquisiti è diretto esclusivamente all'espletamento da parte di UNINA delle finalità attinenti all'esercizio delle attività di erogazione del servizio di posta elettronica certificata ed altri servizi correlati, nonché per adempiere ad eventuali obblighi previsti dalla legge, dai regolamenti o dalla normativa comunitaria.
I dati personali vengono trattati, nell'ambito delle finalità istituzionali dell'Università e per l'erogazione del servizio di PEC, per consentire: l'espletamento di procedimenti amministrativi dell'Ateneo, lo svolgimento di procedimenti amministrativi connessi con la didattica ovvero con i rapporti di lavoro o contrattuali tra UNINA ed i dipendenti, oppure, tra UNINA e terze parti. Il trattamento è obbligatorio, in quanto costituisce condizione necessaria ed indispensabile per consentire l'adempimento delle proprie funzioni istituzionali da parte del Gestore. L'eventuale rifiuto di fornire tali dati e di consentirne il trattamento comporterebbe, quindi, l'impossibilità di adempiere a dette funzioni.

## 7.5 Modalità del trattamento

I dati personali acquisiti dagli interessati sono successivamente trattati esclusivamente dai responsabili e dagli incaricati designati da UNINA tra il personale in servizio presso le strutture e gli uffici dell'Università.
Tutte le informazioni personali raccolte durante l'erogazione del servizio di PEC vengono trattate dal Gestore con tutte le misure di sicurezza descritte all'interno del presente manuale allo scopo di prevenirne la perdita, evitarne usi illeciti o accessi da parte di personale non espressamente autorizzato.

Il trattamento dei dati personali acquisiti da UNINA viene eseguito:

- in modalità automatizzata (gestione dei dati mediante utilizzo di strumenti informatici);

- in modalità cartacea (raccolta, registrazione, conservazione, utilizzo dei documenti mediante fascicoli, schede, raccoglitori e archivi).

I dati in formato elettronico vengono mantenuti in appositi data server adibiti allo scopo e su supporti magnetici conservati in armadi protetti.
I dati in formato cartaceo sono conservati negli archivi cartacei presso la sede di erogazione del servizio, cui avranno accesso solo gli incaricati espressamente autorizzati.
Le operazioni di trattamento previste sono: la registrazione, l'elaborazione, la conservazione, la cancellazione/distruzione, la comunicazione.
Con particolare riguardo a quest'ultima operazione di trattamento, i dati raccolti non verranno comunicati a terze parti per usi commerciali, di marketing o per statistiche ed indagini di mercato.
I dati personali possono essere comunicati, per le medesime finalità previste dal servizi UNINAPEC, agli altri Certificatori e Gestori attivi iscritti nei relativi elenchi pubblici tenuti dal AdID (ex CNIPA) in caso di cessazione della attività da parte di UNINA e al solo fine di assicurare la continuità del servizio.
I dati potranno essere trasferiti al di fuori del territorio nazionale alle condizioni e con le garanzie di cui al [Dlgs 196/2003], nonché comunicati a soggetti pubblici, quali forze dell'ordine, Autorità pubbliche e autorità Giudiziaria, per lo svolgimento delle attività di loro competenza e per motivi d'ordine pubblico, nel rispetto delle disposizioni di legge per la sicurezza e difesa dello Stato, per la prevenzione, accertamento e/o repressione dei reati.
I dati potranno altresì essere comunicati o resi accessibili ad altre società che si occupano della manutenzione dei sistemi informatici, in qualità di responsabili di UNINA. I nominativi di tali soggetti sono a disposizione degli interessati che ne facciano richiesta.
I dati personali non sono soggetti a diffusione.

## 7.6 Sicurezza dei dati personali

Come previsto dalle norme, il Titolare del trattamento dati adotta idonee e preventive misure di sicurezza (descritte al par. 6.7) al fine di garantire l'integrità e la riservatezza dei dati. In particolare, il Titolare del trattamento dei dati si impegna a:

- ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati;
- ridurre al minimo i rischi di danneggiamento a risorse hardware, infrastrutture di rete, locali fisici presso i quali sono custodite le informazioni;
- impedire l'accesso a dati personali alle persone non autorizzate;
- trattare i dati solamente con modalità consentite dalla legge o dai regolamenti di Ateneo.

# 8 – Analisi dei rischi e procedure di ripristino

Il presente capitolo elenca i rischi ai quali il sistema è esposto e descrive le misure adottate dal Gestore per evitare il loro verificarsi, riservando al documento "Piano per la Sicurezza" i dettagli. Il capitolo descrive, inoltre, i servizi di emergenza e le procedure adottate dal Gestore per la gestione delle anomalie riscontrate e per il ripristino, nel più breve tempo possibile, del corretto funzionamento del sistema.

## 8.1 Analisi dei rischi

I rischi di malfunzionamento possono essere catalogati nelle seguenti categorie:

- Furti,
- Frodi o malversazioni (computer crime),
- Danneggiamento,
- Manipolazioni di dati e/o programmi,
- Perdita riservatezza,
- Errori sui dati e programmi,
- Utilizzo di software illecito,
- Divulgazione di dati e programmi,
- Utilizzo illegale di risorse,
- Indisponibilità dei sistemi,
- Inagibilità dei locali.

Per contrastare le suddette minacce e ridurre la possibilità che esse si presentino, il Gestore adotta una serie di misure e strumenti di sicurezza di tipo logistico (sistemi di controllo accessi, aree protette), informatico (ridondanza dei servizi, duplicazione delle informazioni, oscuramento dei dati critici, monitoraggio delle funzionalità principali) ed organizzativo (ruoli e responsabilità, formazione, procedure di gestione del sistema).
I meccanismi di sicurezza informatici, organizzativi e logistici adottati da UNINA per la protezione dei trattamenti effettuati nell'ambito della gestione del sistema di PEC, già descritti nei precedenti capitoli, sono descritti nel Piano della Sicurezza depositato presso AdID.
Nel Piano della Sicurezza sono anche dettagliate le procedure di ripristino adottate.

## 8.2 Gestione delle anomalie

La gestione delle anomalie avviene secondo la seguente organizzazione:

- Il Contact Center del Servizio Assistenza Utenti prende in carico la segnalazione che può arrivare:
  - dall'esterno ad opera di un utente,
  - dall'interno ad opera di un addetto al servizio PEC,
  - dal sistema di monitoraggio a seguito del presentarsi di un evento anomalo.
- In tutti e tre i casi, un operatore di Contact Center prende in carico la segnalazione e la inoltra, mediante il sistema di gestione delle segnalazioni, al Team di Risoluzione preposto alla gestione del servizio PEC.
- Il Team di Risoluzione prende in carico la segnalazione, la studia, verifica che il problema sussista realmente e che sia risolvibile.
- Il Team di Risoluzione individua le possibili soluzioni e ne sceglie la migliore in termini di minore impatto sul servizio e velocità di applicazione.
- Se necessario, il Team di Risoluzione richiede il supporto di terzi (risorse interne o esterne).

- Il Team di Risoluzione effettua l'operazione di risoluzione del problema. Nel caso in cui sia stato previsto il supporto di personale esterno all'azienda, il Team di Risoluzione lo assiste durante tutte le attività svolte e ne controlla l'operato.
- Il Team di Risoluzione testa la soluzione prima di metterla in produzione.
- Terminato l'intervento, il Team di Risoluzione chiude la segnalazione, con annotazioni sulla tipologia di soluzione adottata e/o eventuali informazioni da fornire all'utente.
- Il Contact Center verifica che il problema è stato risolto e comunica la soluzione a chi ha effettuato la segnalazione.

## 8.3 Servizi di emergenza

UNINA garantisce il ripristino delle funzionalità minime del sistema previste dalla normativa a seguito di danni causati da eventi catastrofici (partendo cioè dalla installazione ex-novo di tutti i componenti hardware e software che costituiscono l'architettura di servizio a partire dalle copie di backup) presso il CED CSI del Centro Storico, predisposto per il recovery del sistema ed il ripristino del servizio entro 5 giorni lavorativi.

# 9 – Obblighi e responsabilità

Il presente capitolo descrive gli obblighi e le responsabilità del Gestore di posta elettronica certificata e dei titolari del servizio.

## 9.1 Obblighi e responsabilità del Gestore

Il Gestore si impegna a rispettare la normativa vigente e le Regole Tecniche contenute nel [DM 2/11/2005]. In particolare, si impegna a:

- garantire i livelli di servizio previsti;
- assicurare l'interoperabilità con gli altri gestori accreditati;
- informare i titolari sulle modalità di accesso al servizio e sui necessari requisiti tecnici;
- fornire al mittente la ricevuta di presa in carico, accettazione e di avvenuta consegna del messaggio di posta elettronica certificata (salvo nel caso di eventi disastrosi improvvisi);
- adottare misure atte ad evitare inserimento di codici eseguibili dannosi nei messaggi (virus);
- rilevare la presenza di virus o eccezioni formali nei messaggi mediante avviso di non accettazione;
- effettuare la corretta trasmissione dal mittente al destinatario conservando l'integrità del messaggio originale nella relativa busta di trasporto (salvo nel caso di eventi disastrosi improvvisi);
- rilasciare avviso di mancata consegna per superamento dei tempi massimi previsti (salvo nel caso di eventi disastrosi improvvisi);
- apporre su ogni messaggio un riferimento temporale, sia esso la busta di trasporto, una ricevuta o un avviso (salvo nel caso di eventi disastrosi improvvisi);
- apporre la relativa marca temporale ai log dei messaggi generati dal sistema;
- registrare ed associare un riferimento temporale ad ogni fase di trasmissione del messaggio sui file log, conservare e rendere disponibili detti log per gli usi e nelle modalità previste dalla legge;
- prevedere procedure e servizi di emergenza che assicurino il completamento della trasmissione anche in caso di incidenti (ad esclusione di eventi disastrosi improvvisi quali terremoti, attentati, ecc);
- agire nel rispetto delle norme previste dal Decreto legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali;
- garantire la riservatezza, integrità e inalterabilità nel tempo dei file di log;
- assicurare la segretezza della corrispondenza trasmessa attraverso il proprio sistema;
- conservare i messaggi contenenti virus informatici per il periodo previsto dalla normativa;
- conservare le informazioni relative agli accordi stipulati con gli utenti nel rispetto della normativa vigente;
- effettuare la disattivazione di una casella di PEC dopo aver verificato l'autenticità della richiesta;
- fornire informazioni sulle modalità di richiesta, reperimento e presentazione all'utente dei log dei messaggi;
- utilizzare protocolli sicuri allo scopo di garantire la segretezza, l'autenticità, l'integrità delle informazioni trasmesse attraverso il sistema di PEC;

- attivare la procedura di sostituzione dei certificati elettronici relativi alle proprie chiavi di firma con una tempistica tale da non causare interruzioni di servizio;
- richiedere la revoca dei certificati relativi alle chiavi utilizzate per la firma dei messaggi e per la connessione sicura al sito AdID in caso di loro compromissione;
- operare in modo che non sia consentita la duplicazione abusiva e incontrollata delle chiavi private di firma o dei dispositivi che le contengono;
- consentire l'esportazione cifrata delle chiavi private di firma in modo da non diminuirne il livello di sicurezza;
- non consentire l'utilizzo delle chiavi private per scopi diversi dalla firma dei messaggi previsti dalla normativa;
- comunicare tempestivamente ai propri utenti l'eventuale cessazione o interruzione del servizio;
- consentire l'accesso logico e fisico al sistema alle sole persone autorizzate;
- utilizzare un sistema di riferimento temporale che garantisca stabilmente una sincronizzazione delle macchine coinvolte con uno scarto non superiore al minuto secondo rispetto alla scala di Tempo Universale Coordinato UTC;
- utilizzare dispositivi di firma conformi con la normativa.

## 9.2 Obblighi e responsabilità dei titolari

Il titolare del servizio ha l'obbligo di:

- fornire a UNINA tutte le informazioni necessarie ad identificare la persona ed attivare il servizio, garantendo, sotto la propria responsabilità, la veridicità dei dati comunicati;
- custodire gelosamente le proprie credenziali di accesso al sistema;
- utilizzare in modo sicuro il sistema e non rivelare ad alcuno le proprie credenziali di accesso;
- utilizzare il servizio per i soli usi consentiti dalla legge;
- essere a conoscenza dei contenuti del presente Manuale Operativo;
- adottare misure atte ad evitare inserimento di codici eseguibili dannosi nei messaggi (virus);
- informare le persone abilitate all'utilizzo delle caselle sulle tematiche di sicurezza concernenti il loro uso onde evitare un uso non autorizzato.

Inoltre, il titolare:

- ha la piena responsabilità del contenuto dei messaggi inviati e relativi allegati;
- ha la responsabilità di conservare copia dei messaggi inviati o spediti e delle relative ricevute;
- solleva il gestore da ogni responsabilità in merito ai contenuti dei messaggi.

## 9.3 Limitazioni ed indennizzi

UNINA non risponderà in alcun caso:

- dei danni causati direttamente o indirettamente dagli utilizzatori del servizio imputabili ad un utilizzo improprio del sistema ed al mancato rispetto delle regole e degli obblighi contenuti nel presente manuale;
- dei danni causati da malfunzionamenti, ritardi o interruzioni purché rientranti nei livelli di servizio descritti nel presente manuale.

Inoltre, UNINA:

- non potrà in alcun modo essere ritenuta responsabile, a titolo esemplificativo ma non esaustivo, per danni derivanti da cause di forza maggiore, caso fortuito, eventi

catastrofici (incendi, terremoti, esplosioni) o comunque non imputabili al Gestore che provochino ritardi, malfunzionamenti o interruzioni del servizio;

- non assume alcun obbligo riguardo la conservazione dei messaggi inviati e trasmessi attraverso le proprie caselle di PEC. Tale responsabilità viene assunta unicamente dal titolare;
- non ha alcuna responsabilità sui contenuti dei messaggi inviati e ricevuti attraverso le proprie caselle di PEC.

Qualsiasi contestazione dell'utente, relativa all'erogazione del servizio, dovrà essere comunicata al Gestore, pena decadenza, entro 30 giorni dalla data dell'evento mediante raccomandata con ricevuta di ritorno.

La copertura dei rischi dell'attività e dei danni causati a terzi dovuti al mancato rispetto dei livelli di servizio descritti nel presente manuale è garantita dalla polizza stipulata da UNINA per l'assicurazione della "Responsabilità civile patrimoniale della Pubblica Amministrazione".

UNINA si riserva la facoltà di modificare il presente manuale nel caso in cui vengano apportate modifiche tecniche al sistema o adeguamenti normativi.

## 10 – Canali di comunicazione

Di seguito vengono riportati i numeri di telefono, i fax e gli indirizzi email da utilizzare per comunicare con il Gestore, esclusivamente per esigenze connesse con l'utilizzo del servizio UNINAPEC:

| | |
|---|---|
| ***email:***<br>contactcenter@unina.it | ***pec:***<br>contactcenter@pec.unina.it |
| ***Fax:***<br>081.676569 | ***telefono*:***<br>081.676799 |
| ***protocollo informatico:***<br>http://www.protocollo.unina.it<br>(codice destinatario: 1-7-33-1-0<br>oppure, solo per le richieste di attivazione caselle: 1-7-33-5-0 ) | ***web:*** https://www.contactcenter.unina.it<br>(immettendo le proprie credenziali di accesso alla posta convenzionale UNINA) |
| ***Indirizzo:***<br>CSI – Servizio PEC<br>Complesso Universitario di Monte S. Angelo<br>Via Cinthia – 80126 Napoli | |
| *Il servizio in voce è attivo dal lunedì al venerdì nelle seguenti fasce orarie: dalle 11:00 alle 13:30 e dalle 14:30 alle 16:30. | |

Università degli Studi di Napoli Federico II
Centro Servizi Informativi di Ateneo (C.S.I.)

f.to digitalmente: Il Presidente