# Certified Email

## Operating Manual of the provider Namirial S.p.A.

| | | | | |
|---|---|---|---|---|
| Category | **PEC** | Document Code | **NAM-PEC-MO** | **Namirial S.p.A.** |
| Prepared by | **Marina Pettinari** | Confidentiality Note | **Public Document** | The Legal Representative |
| Verified by | **Flavio Fanton** | Version | **2.2** | **Massimiliano Pellegrini** |
| Approved by | **Massimiliano Pellegrini** | Date of Issue | **07/07/2021** | |

**Signed by:** Massimiliano Pellegrini
**EMail:** m.pellegrini@namirial.com
**Signing time:** 08-07-2021 14:54:31
**IP address:** 93.38.49.150



**Namirial S.p.A.**

*Registered office, management and administration* 60019 Senigallia (AN) - via Caduti sul Lavoro, 4
Tax Code/Co. Reg. ANCONA No. 02046570426 - VAT No. IT02046570426 - Share capital €7,559,253.20 fully paid
Tel. 07163494 (switchboard) - info@namirial.com - www.namirial.com

**ISO 9001** - Certificate No. IT223776 | **ISO 27001** - Certificate No. IT280490

– This page has been intentionally left blank –

# CONTENTS

**1 Introduction 10**

1.1 Purpose and scope of the document 10

1.2 Definitions and Acronyms used in the document 10

1.3 Version of the Operating Manual and subsequent revisions(m) 12

1.4 Publication of the provider's Operating Manual(d) 13

1.5 Correspondence table 13

**2 The Provider 14**

2.1 Provider identification details(a) 14

2.2 Brief description of Namirial S.p.A. 15

2.3 Manager of the Service and of the Operating Manual(b) 16

2.4 Help Desk and customer support 16

2.5 Sales information 16

**3 Certified Email: general information 17**

3.1 Introduction 17

3.2 Certified Email: how it works 17

3.2.1 Details and special cases 18

3.2.1.1 Take-charge Receipt 18

3.2.1.2 Messages sent to non-certified email addresses 18

3.2.1.3 Messages from non-certified email addresses 18

3.2.1.4 Formally incorrect message 18

3.2.1.5 Presence of viruses 18

3.2.1.6 Maximum time limits exceeded 18

**4 The PEC service of Namirial S.p.A.(g) 20**

4.1 Features of the offer 20

4.2 Offer details, supply conditions and rates applied 20

4.3 Activation of the service through a sales partner 20

4.3.1 Local Registration Authority (LRA) 20

4.3.2 Obligations of the Local Registration Authority (LRA) 20

4.4 Identification 21

4.4.1 Parties authorised to carry out identification 21

4.4.2 Identification procedures 21

4.5 Domain names and mailbox names 21

4.6 Issue of PEC mailboxes 21

4.6.1 Mailbox activation request 22

4.6.2 Mailbox activation 22

4.6.2.1 Recommendations for users 22

4.7 Additional services 22

4.7.1 Acceptance of incoming conventional email or its forwarding 23

4.7.2 PEC receipt notification 23

4.7.3 Daily report by email and SMS 23

4.7.4 Archiving of PEC messages 23

4.7.5 Legally compliant retention of PEC messages 23

4.7.6 Mailboxes for bulk sending 23

4.7.7 Custom certified domains 24

4.7.8 Closed domain 24

4.8 Access to the service(i) 24

4.8.1 Access through email clients 24

4.8.2 Access via webmail 27

4.9 Loss of the system access credentials 27

4.10 Request and retrieval of message logs(h) 27

4.11 Request for closure of a PEC mailbox 28

4.12 Termination of the Certified Email service(l) 28

4.13 Help Desk service 28

4.13.1 Trouble ticketing 29

4.14 Service levels and quality indicators[j] 29

**5 Description of the solution 31**

5.1 Main features 31

5.2 Scalability and Reliability 31

5.3 Data security 31

5.4 System features 31

5.5 Time references 32

5.6 Archiving of Logs and of messages containing viruses, and their legally compliant retention 32

**6 Procedures and technological and security standards used 34**

6.1 Reference technological standards 34

6.2 Security standards 34

6.2.1 Signature devices (HSM) 34

6.3 Security measures 35

6.3.1 Human resources assigned to system management 35

6.3.2 Infrastructure security 35

6.3.3 Risk analysis and management 35

6.3.4 Actions to counter the spread of malicious content 36

6.3.4.1 Anti-malware technologies 36
6.3.4.2 Attachment analysis 36
6.3.4.3 Password policy 36
6.3.4.4 Systems for monitoring suspicious activity 37
6.3.4.5 Mutual assistance procedures between providers 37

6.3.5 Spam prevention 37

6.3.6 Monitoring of security levels 37

6.4 Operating procedures used in providing the service[e] 37

6.4.1 Staff organisation 37

6.4.2 Monitoring system 38

6.4.3 Problem management and resolution 38

6.5 Actions taken by the provider in the event of malfunctions 38

**7 Obligations and responsibilities 40**

7.1 Obligations and responsibilities of the Provider 40

7.2 Obligations and responsibilities of the Holders 40

7.3 Limitations and compensation 41

7.4 Insurance policy 41

**8 Personal data protection[(k)] 42**

8.1 Organisational structure of Namirial S.p.A. 42

8.2 Protection and rights of data subjects 42

8.3 Processing methods 42

8.4 Purposes of processing 42

8.5 Other forms of data use 42

8.6 Data security 42

## HISTORY OF CHANGES MADE

| VERSION | 2.2 |
|---|---|
| Date | 07/07/2021 |
| Reason | Update |
| Changes | §2.4 References updated<br>§3.2.1.3 Chapter updated and extended<br>§4.11 PEC mailbox closure flow revised<br>§6.3 Entire chapter updated and extended |

| VERSION | 2.1 |
|---|---|
| Date | 27/08/2020 |
| Reason | Update |
| Changes | §2.2 Section on the Provider's certifications revised and updated<br>§4.6.2.1 Recommendations for users<br>§4.8.1 Access parameters for email clients added<br>§4.8.2 Mandatory password change at first webmail access added |

| | |
|---|---|
| | §6.3.5 Attachment checks<br>§7.3 Limitations and compensation |

| **VERSION** | **2.0** |
|---|---|
| Date | 14/10/2019 |
| Reason | Update |
| Changes | Ch 7 Added paragraph 7.3.5 Spam prevention<br>Ch 2.1 secondary service site updated; service email updated<br>Ch 2.4 help desk telephone reference updated<br>Ch 4.1 added the option of deleting PECs older than 30 days.<br>Ch 4.8 procedure for recovering access credentials changed<br>Ch 4.10 PEC mailbox closure method changed<br>Ch 4.11 PEC service termination plan added<br>Ch 4.13 maximum size of the message handled increased<br>Ch 5.7, Ch 5.8 changed the method of applying time stamps to LOGs and of their retention<br>Ch 6.4.3, Ch 6.4.4 changed the description of the monitoring system and of the actions taken when errors are found/reported.<br>Ch 7.4 information on the insurance policy updated. |

| **VERSION** | **1.9** |
|---|---|
| Date | 12/09/2014 |
| Reason | Update |
| Changes | General restructuring of the document.<br>Ch 2.2 Update of the brief description of the Provider<br>Ch 2.3 Change of the Manager of the Service and of the Operating Manual.<br>Ch 4.2 Paragraph deleted, its content merged into the Glossary of terms<br>Ch 5.1, Ch 5.2 Restructuring of the brief description of the service offered.<br>Ch 5.6.2.1 Password length and complexity adjusted<br>Ch 7.4.2 Update of Backup Management<br>Ch 8 Obligations and Responsibilities of the Provider and of the Holder merged into one chapter. |

| **VERSION** | **1.8** |
|---|---|
| Date | 14/10/2013 |
| Reason | Update |
| Changes | Ch 5.1.1, Ch 5.1.2, Ch 5.1.3 Definition of “bulk sending” supplemented and daily sending limits revised.<br>Ch 5.4.1 Service configuration parameters added.<br>Ch 5.4.2 Link to the webmail added.<br>Ch 8.2 Text changed from IGPEC to Public list of Providers, with the addition of the link for consulting it |

| **VERSION** | **1.7** |
|---|---|
| Date | 05/08/2013 |
| Reason | Update |

| | |
|---|---|
| Changes | Ch.5.1.1, Ch.5.1.2, Ch.5.1.3 Traffic limits have been introduced for the use of the PEC mailbox: limits on sending more than 1000 communications per day and limits on bulk sending of communications by PEC.<br>Ch.8.2 Obligations and responsibilities of holders supplemented, with an indication of the consequences for them in the event of breach. |

| **VERSION** | **1.6** |
|---|---|
| Date | 01/07/2011 |
| Reason | Update and restructuring of the document |
| Changes | The acronym CNIPA has been replaced with DigitPA where necessary.<br>Ch 5.1.7 After the amendments to the CAD, as per decree-law of 30 December 2010 no. 235, the duties of the Registration Office, which has changed its name, have been updated; all references in the manual have been updated.<br>Ch.5.1 The standard mailbox size has been increased to 1 Gigabyte<br>Ch.5.1.1, Ch.5.1.2, Ch.5.1.3 It has been specified that traffic limits apply only when the mailbox is used for bulk sending.<br>Ch. 5.1.4 It has been specified that use of the PEC mailbox request panel is allowed only to authorised persons (LRA/IR Resellers/Distributors)<br>Ch. 5.3 The procedure for activating PEC services by directly filling in the forms downloaded from the website has been added<br>Ch. 5.6 The availability on the website of the email address for requesting LOG files has been indicated<br>Ch.5.7 The notification to Holders of the closure of PEC mailboxes has been revised<br>Ch. 5.8.1 The image of the Trouble Ticketing program has been replaced with the new version<br>Ch. 6.9.2 The magnetic badge for access to the machine room has been replaced with a transponder key on a proximity reader<br>Ch.6.4 The OpenPec version has been updated<br>Ch.9.2 The personal data Processor has changed |

| **VERSION** | **1.5** |
|---|---|
| Date | 29/10/2009 |
| Reason | Update |
| Changes | Ch.2.1 Identification details: share capital changed from €1,000,000.00 fully paid to €6,500,000.00 fully paid<br>Ch.5.1.7 Registration Offices: the option for the Provider to use Registration Offices for the identification and validation of the documentation required for the provision of the PEC service has been added. |

| **VERSION** | **1.4** |
|---|---|
| Date | 10/12/2008 |
| Reason | Update |
| Changes | Ch.2.2 The description of the provider company has been made clearer.<br>Ch.4.3.1 The service for “forwarding” messages from non-certified mailboxes has been illustrated in detail.<br>Ch. 5.3 The option of sending the documentation by email and with a digital signature has been mentioned.<br>Ch.5.4.1 Access through email clients that meet the required requirements has been specified. |

| | |
|---|---|
| | Ch.5.7 A minimum period for the Provider to keep account/domain cancellation requests has been added.<br>Ch.6.9.2 The indication of the reference Class of the security doors and of the video surveillance system has been changed.<br>Ch.8.1 For greater completeness, further points on the provider's obligations have been added.<br>Ch.8.2 For greater completeness, further points on the holder's obligations have been added. |

| **VERSION** | **1.3** |
|---|---|
| Date | 19/05/2008 |
| Reason | Update |
| Changes | Ch. 4.3.1. The date of the UNI EN ISO 9001:2000 Quality Certification has been added<br>Ch. 4.3.1. A passage describing how Namirial handles messages from non-certified email addresses has been added.<br>Ch. 5.1 The option of purchasing basic 50 Mbyte mailboxes in addition to 100 Mbyte ones has been added<br>Ch. 7.4.2. The indication of backup management by Namirial has been updated. |

| **VERSION** | **1.2** |
|---|---|
| Date | 16/10/2007 |
| Reason | Update |
| Changes | Ch. 5.1.3 The bands for the minimum and maximum number of mailboxes that can be purchased have been changed.<br>Ch. 5.1.4 The additional space per mailbox increases from 50 Mbytes to 100 Mbytes |

| **VERSION** | **1.1** |
|---|---|
| Date | 28/12/2006 |
| Reason | First issue of the document. |
| Changes | --- |

# 1 INTRODUCTION

## 1.1 PURPOSE AND SCOPE OF THE DOCUMENT

This document is the Operating Manual of the certified email (PEC) service of the Provider Namirial S.p.A. and describes the processes and methods used by the provider to supply the certified email (PEC) service. The Operating Manual is a public document: it can therefore be freely downloaded from the provider's website at the following link: http://www.sicurezzapostale.it/docs/manualeoperativo.pdf.

## 1.2 DEFINITIONS AND ACRONYMS USED IN THE DOCUMENT

| TERM | MEANING |
|---|---|
| **PEC** | Certified Email |
| **CNIPA** | National Centre for Information Technology in Public Administration |
| **DigitPA** | National Agency for the Digitalisation of Public Administration (formerly CNIPA) |
| **AgID** | Agency for Digital Italy (formerly DigitPA) |
| **Certified Email Provider** | Party that manages one or more certified email domains with the related access, incoming and delivery points, and holds the key used to sign receipts and envelopes. This party interacts with other certified email providers for the interoperability of the mailboxes of all holders |
| **Holder** | Party to whom a PEC mailbox is assigned |
| **Certified Email Domain** | Certified email domain containing only certified email mailboxes, also called "certified domain" or PEC domain |
| **Index of Certified Email Providers** | System containing the list of certified email domains and providers, with the related certificates corresponding to the keys used to sign receipts, notices and envelopes, implemented by means of a Lightweight Directory Access Protocol server, hereinafter LDAP, located in an area accessible to the various certified email providers and which also constitutes the technical structure of the public list of certified email providers. Abbreviated as IGPEC. |
| **Certified Email Mailbox** | Email mailbox activated within a PEC domain and associated with a function that issues an acceptance receipt upon sending and a delivery receipt upon receipt of PEC messages by the recipient |
| **Time stamp** | Electronic evidence by which a time reference that can be relied upon against third parties is attributed to one or more electronic documents, as provided for by Presidential Decree no. 445 of 28 December 2000 and by the Decree of the President of the Council of Ministers of 13 January 2004, published in Official Gazette no. 98 of 27 April 2004. |
| **Time reference** | Information containing the date and time, associated with a certified email message |
| **Certification Data** | Data, such as the day and time of sending, sender, recipient, subject and message identifier, which describe the sending of the original message and are certified by the sender's certified email provider; these data are contained in the receipts and are transferred, by means of a transport envelope, to the recipient holder together with the original message |
| **Tamper evidence** | System for signalling any attempt to physically tamper with the server that may have compromised the integrity of the system and/or of the data it contains; typically implemented by applying to the machines seals, padlocks, self-adhesive labels and/or any other means of protection whose condition, in the event of unauthorised access, is clearly compromised to an outside observer. |
| **Tamper proof hardware** | Physical protection system for the server, designed to prevent/stop access to and tampering with the data system by unauthorised parties. |

| | |
|---|---|
| **MTA** | Acronym of Mail Transfer Agent. This is the module responsible for handling requests to send/receive ordinary and certified email messages |
| **LDAP** | Lightweight Directory Access Protocol. It is a network protocol used to search for and store information on a Directory Server. An LDAP directory server is a tree of entities made up of attributes and values. A typical use of a directory server is storing email accounts or the users registered on a website. |
| **LDIF** | Acronym of LDAP Data Interchange Format. It is a data interchange standard in text format, used to represent the contents of an LDAP directory and for requests to update them. |
| **SNMP** | Simple Network Management Protocol. It is a protocol used to manage and monitor devices as well as the structure of a network. |
| **HSM** | Hardware Security Module. It is a hardware device for the generation, storage and secure protection of a pair of signature keys. |
| **NTP** | Network Time Protocol. It is a protocol used to synchronise the clocks of computers within a packet-switched network, hence with variable and unreliable latency times |
| **LMTP** | Local Mail Transport Protocol. It is a protocol used to write PEC messages into the holders' mailboxes |
| **Secure Socket Layer (SSL)** | Protocol for encrypted communications over the Internet. This protocol uses cryptography to provide security in communications over the Internet and to allow client/server applications to communicate in such a way as to prevent 'tampering', falsification and interception of data. The primary purpose of SSL is to provide cryptographic systems for reliable, confidential communications on the Web that can be used in applications such as email and authentication systems. |
| **HTTPS** | The term HTTPS refers to the HTTP (Hyper Text Transfer Protocol) protocol used in combination with the SSL (Secure Socket Layer) layer. |
| **IR** | Party appointed by the Provider for the Identification, Registration and Support of Applicants/Holders of PEC mailboxes |
| **LRA** | Local Registration Authority: natural or legal person delegated by the Provider to carry out the Identification, Registration and Support operations for Holders of PEC mailboxes |
| **Personal data** | As defined in European Regulation 679/2016 (GDPR), personal data means "any information relating to a natural person, legal person, body or association, identified or identifiable, also by reference to any other information, including a personal identification number".<br>Personal data also include data relating to the user or to any third parties and contained in the information fields of the forms, in the electronic and/or paper archives of registration, of requests for suspension, reinstatement, revocation and change of personal details, and in the certificates referred to in this operating manual. |
| **Data controller** | Natural or legal person, public administration or any other body, association or organisation which, also jointly with another controller, is responsible for decisions regarding the purposes and methods of processing personal data and the tools used, including the security profile |
| **Data processor** | Natural or legal person, public administration or any other body, association or organisation appointed by the controller to process personal data |
| **Person in charge of data processing** | Natural person authorised by the data controller or processor to carry out data processing operations |
| **Data subject** | Natural or legal person, body or association to which the personal data refer |
| **Access Point (PdA)** | System that provides the access services for sending and reading certified email messages, as well as the services for user identification and access, checking for computer viruses in the message, issuing the acceptance receipt and enclosing the original message in the transport envelope |
| **Incoming Point (PdR)** | System that receives the message within a certified email domain, checks the origin and correctness of the message and issues the take-charge receipt, encloses incorrect messages in an anomaly envelope and checks for computer viruses in ordinary email messages and transport envelopes |

| | |
|---|---|
| **Delivery Point (PdC)** | System that delivers the message to the recipient holder's certified email mailbox, checks the origin and correctness of the message and issues, as the case may be, the delivery receipt or the non-delivery notice |
| **Certified Email Provider's Signature** | Advanced electronic signature, based on a system of asymmetric keys, which makes it possible to show the origin and ensure the integrity and authenticity of the messages of the certified email system; it is generated through a computer procedure that guarantees the unique connection to the provider and its unique identification, and is created automatically by means that guarantee the provider's exclusive control |
| **Acceptance Receipt (RdA)** | Receipt, signed with the signature of the sender's certified email provider, containing the certification data and issued to the sender by the access point upon the sending of a certified email message |
| **Non-acceptance Notice (AdNA)** | Notice, signed with the signature of the sender's certified email provider, which is issued when the sending provider is unable to accept the incoming message and which states the reason why the message cannot be accepted, together with the information that the message cannot be delivered to the recipient |
| **Take-charge Receipt (RPdC)** | Receipt, signed with the signature of the recipient's certified email provider and issued by the incoming point to the sending certified email provider, which certifies that the message has been taken charge of by the destination certified email system and carries the certification data so that it can be associated with the message to which it refers |
| **Delivery Receipt (RdAC)** | Receipt, signed with the signature of the recipient's certified email provider, issued to the sender by the delivery point when the message is placed in the recipient's certified email mailbox |
| **Full Delivery Receipt (full RdAC)** | Receipt containing the certification data and the original message |
| **Short Delivery Receipt (short RdAC)** | Receipt containing the certification data and an extract of the original message; |
| **Summary Delivery Receipt (summary RdAC)** | Receipt containing the certification data |
| **Non-delivery Notice (AdMC)** | Notice issued by the system to inform the sender of the anomaly of the original message, if the certified email provider is unable to deliver the message to the recipient's certified email mailbox |
| **Original Message** | Message sent by a certified email user, in the phase before it reaches the access point, and delivered to the recipient holder by means of a transport envelope containing it |
| **Transport Envelope (BdT)** | Envelope created by the access point and signed with the signature of the sending certified email provider, containing the original message sent by the certified email user and the related certification data |
| **Anomaly Envelope (BdA)** | Envelope, signed with the signature of the recipient's certified email provider, containing an incorrect message or a non-certified email message; it is delivered to a holder in order to notify the recipient of that anomaly |

*Table 1: definitions and Acronyms*

## 1.3 VERSION OF THE OPERATING MANUAL AND SUBSEQUENT REVISIONS(M)

The current version of the document is indicated on the first page; however, this Manual may be subject to changes as a result of modifications made to the system and dictated by the need for optimisation, regulatory adjustments or changes to the internal and external processes for the provision of the Certified Email service. The Provider undertakes to keep the document up to date and consistent with the installed system. Any future change to the document will be verified and approved by the service managers of the Provider Namirial S.p.A. and submitted for approval to the competent bodies (AgID). The Customer or the Holder is required to consult the most up-to-date version of the Operating Manual, published on the Provider's website referred to in § 1.4 below

## 1.4 PUBLICATION OF THE PROVIDER'S OPERATING MANUAL(D)

This manual is published on the Provider's website and can be downloaded from the following link: http://sicurezzapostale.it/docs/manualeoperativo.pdf. The Provider Namirial S.p.A. undertakes to publish its updated and approved version on the website.

## 1.5 CORRESPONDENCE TABLE

| Circular CNIPA/CR/56 of 21/05/2009 | § Operating Manual |
|---|---|
| a. Provider identification details | **2.1** |
| b. Name of the Operating Manual Manager | **2.3** |
| c. Regulatory references needed to verify the contents | **REFERENCES** |
| d. Address of the provider's website, where the Operating Manual is published and can be downloaded | **1.4** |
| e. Indication of the procedures and of the technological and security standards used by the Provider in providing the service | **6.4** |
| f. Definitions of abbreviations and technical terms | **1.2** |
| g. Description and methods of the service offered | **4** |
| h. Description of how the information in the message LOGs is retrieved and communicated | **4.10** |
| i. Methods of access to and supply of the service | **4.8** |
| j. Service levels with the related quality indicators, pursuant to article 12 of the Decree of the Minister for Innovation and Technologies of 2 November 2005 | **4.15** |
| k. Criteria for protecting the data of mailbox holders, resulting obligations and responsibilities, exclusions and any limitations in the event of compensation, concerning the parties provided for in article 2 of Presidential Decree no. 68/2005 | **7, 8** |
| l. Operating procedures to be implemented if the activity of certified email provider ceases | **4.12** |
| m. Version of the Operating Manual | **1.3** |

*Table 2: correspondence table between CNIPA/CR/56 and the Operating Manual*

# 2 THE PROVIDER

The Certified Email service is provided by Namirial S.p.A., whose identification details are given below together with a brief description of its activities and main areas of expertise.

## 2.1 PROVIDER IDENTIFICATION DETAILS[(A)]

| Provider identification details | |
|---|---|
| Company name: | Namirial S.p.A. |
| Registered office: | Via Caduti sul lavoro, 4<br>60019 - Senigallia (AN)<br>Tel: 071.63494<br>Fax: 071.60910 |
| Service provision site: | Via Caduti sul lavoro, 4<br>60019 - Senigallia (AN) - Italia<br>Tel: 071.63494<br>Fax: 071.60910 |
| Secondary sites (used to store backup copies of the data) | Digital Campus @ Milan<br>Via Monzoro, 101-105<br>20010 Cornaredo (MI) — Italia |
| VAT number: | IT02046570426 |
| Companies Register entry: | Ancona |
| REA: | 02046570426 |
| Share capital: | €7,559,253.20 fully paid |
| Service website: | http://www.sicurezzapostale.it |
| Provider's website: | http://www.namirial.com |
| Service email: | serviziopec@sicurezzapostale.it |
| Provider's email: | info@namirial.com |

*Table 3: Provider identification details*

## 2.2 BRIEF DESCRIPTION OF NAMIRIAL S.P.A.

Namirial S.p.A. is an IT and web engineering company operating specifically in the field of Information Technology, directing its software production towards the new and increasingly evident needs of the Italian production system to adapt to today's highly competitive and globalised economic scenarios. In a national economic landscape characterised mainly by small and medium-sized businesses, Namirial S.p.A. considers it essential to develop software solutions and services that are also accessible over the internet and able to respond professionally to emerging technological and innovation issues, while keeping operating costs very low. The company is based in a modern facility of more than two thousand square metres, which houses an *Internet Data Center* equipped with all the security systems needed to make the facility inviolable and able to assist users also with any hosting, housing and server farm needs in general.

**Namirial S.p.A. is:**

**eIDAS Qualified Trust Service Provider (Certificate No. IT269191)**

For the services of:

- issuing, verification and validation of qualified time stamps

- certification authority for issuing qualified electronic signature certificates and qualified electronic seals

according to the standards

- **ETSI EN 401**
- **ETSI EN 411 parts 1 and 2**
- **ETSI EN 421**
- **ETSI EN 422**
- **ETSI EN 319 412 as applicable.**

**PEC Provider, since 27/02/2007,** accredited with AgID (formerly DigitPA) and authorised to manage Certified Email **mailboxes** and **domains**.

**Accredited Identity Provider** with AgID for issuing digital identities in compliance with the Prime Ministerial Decree (DPCM) of 24 October 2014, the technical requirements of Commission Implementing Regulation (EU) 2015/1502 and Art. 24 of Regulation (EU) 910/2014 eIDAS (Certificate No. IT273825)

**Accredited Retention Provider** with AgID for the retention of electronic documents referred to in article 44-bis, paragraph 1, of Legislative Decree no. 82 of 7 March 2005 (Certificate No. IT277150).

**ISO 9001 certified.** Namirial has obtained certificate no. 223776 issued by **Bureau Veritas Italia S.p.A.**

**ISO/IEC 27001 certified (with extensions 27017/27018).** Namirial has obtained certificate no. IT280490 issued by **Bureau Veritas Italia S.p.A.**

**Certified by Adobe**. Since June 2013 Namirial has been a **member of the AATL** (Adobe Approved Trust List).

*Table 4: certifications of the Provider*

## 2.3 MANAGER OF THE SERVICE AND OF THE OPERATING MANUAL(B)

The Manager of this operating manual is:

**Flavio Fanton**

The Manager can be contacted at the following addresses:

telephone: +39 071.63494
email: serviziopec@sicurezzapostale.it
address: Via Caduti sul lavoro, 4 - 60019 Senigallia (AN)

The Managers responsible for verifying and approving the document are named on the first page.

## 2.4 HELP DESK AND CUSTOMER SUPPORT

To obtain information on the service and receive assistance if malfunctions are detected, please refer to the page https://support.namirial.com/it/supporto-tecnico

## 2.5 SALES INFORMATION

To receive sales information on the offers of Namirial S.p.A., it is possible to contact the Provider by telephone, email or web at the following addresses:

telephone: 071-63494
email: commerciale@sicurezzapostale.it
web: www.sicurezzapostale.it

# 3 CERTIFIED EMAIL: GENERAL INFORMATION

## 3.1 INTRODUCTION

Certified email (PEC) is an email system in which the sender is given, in electronic format, legal proof of the sending and delivery of electronic documents. PEC was created to replace, through modern means of communication, the **Registered letter with return receipt**, or registered letter A/R. As with the registered letter A/R, the sender receives a receipt certifying the delivery of their message to the recipient. PEC messages may contain any type of information and attachment. Communication takes place through a series of messages (called envelopes), receipts and notices which are sent:

- to users (sender and recipient), by the certified email servers;
- between the various certified email servers.

Every envelope, receipt or notice is marked with a time reference that certifies exactly the moments at which the communications take place.
To guarantee the lawfulness, transparency and correctness of the system, AgID has set up a **Public Index of Certified Email Providers (IGPEC)**. This is a list of public bodies or private companies which, once accredited by an AgID examining committee, may act as Provider, supply PEC mailboxes to third parties and, more generally, provide the service. One of the tasks of a PEC Provider is also to keep, for a period of 30 months, the system LOGs, which contain the record of the communications that have taken place. These LOGs have the same legal validity as registered letter receipts and may be requested at any time by users who are mailbox holders.

## 3.2 CERTIFIED EMAIL: HOW IT WORKS

To outline how a Certified Email system works, consider the drawing shown in the following figure.

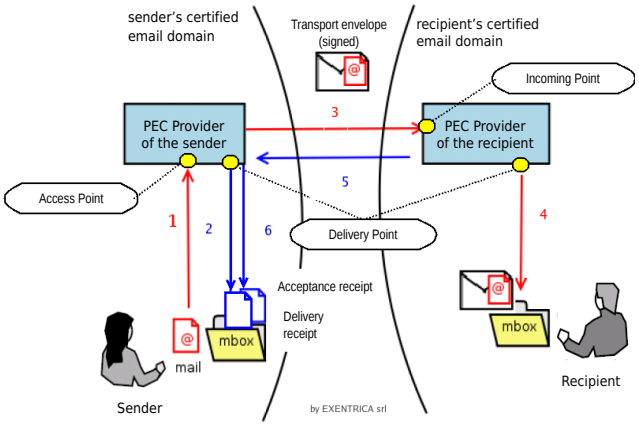



*Figure 1: How the PEC system works*

The diagram shows 2 users (Sender and Recipient), each of whom belongs to a Certified Email domain:

1) The original message reaches the Access Point of the Sender's PEC Provider.
2) The Sender's PEC Provider, after carrying out the formal checks and verifying that the message does not contain viruses, issues the Acceptance Receipt and sends it to the Sender.
3) The original message is enclosed in a Transport Envelope, which is signed by the Sender's Provider by means of a dedicated device and then sent to the Incoming Point of the Recipient's PEC Provider.
4) The Recipient's PEC Provider receives the Transport Envelope at the Incoming Point, verifies the reliability of its signature, checking that it has not been altered in transit, and delivers it to the recipient's mailbox (delivery point).

5) As soon as the message has been delivered, the recipient's PEC provider creates a delivery receipt, signs it and sends it to the sender.

6) The sender's PEC provider receives the delivery receipt, verifies its correctness and integrity and delivers it to its user (the sender) through the delivery point.

The delivery receipt can be:

- **full**: this is the default receipt in the webmail. In addition to the certification data, it contains as an attachment the original message, complete with any attached files it originally contained;
- **short**: in addition to the certification data, it contains as an attachment the original message in which any attached files originally present are replaced by their hash code;
- **summary**: it contains only the certification data, without the original message attached.

### 3.2.1 DETAILS AND SPECIAL CASES

The communication shown in Figure 1 describes a typical exchange between Sender and Recipient. However, communication between users is accompanied by a series of receipts, envelopes and notices between user and Provider and between Providers, which serve to guarantee correct transmission, detect any anomalies and/or handle the special cases described below.

#### 3.2.1.1 TAKE-CHARGE RECEIPT

To maintain the traceability of Transport Envelopes, the Recipient's PEC Provider sends the Sender's Provider a Take-charge Receipt whenever it receives a Transport Envelope from a certified domain outside the Recipient's Provider itself.

#### 3.2.1.2 MESSAGES SENT TO NON-CERTIFIED EMAIL ADDRESSES

Every original message sent to non-certified email addresses will reach its destination contained in a Transport Envelope.

#### 3.2.1.3 MESSAGES FROM NON-CERTIFIED EMAIL ADDRESSES

Every PEC Provider can choose how to handle messages from non-certified email addresses – ordinary email messages.
The Provider Namirial S.p.A. allows the user to choose whether to reject such messages, forward them automatically to a second address or deliver them enclosed in an Anomaly Envelope. The option is available in the *Settings* section of the webmail.
In the latter case, these messages are analysed by the antispam system, which merely alerts the user through appropriate notices and moves messages considered unwanted or dangerous to a dedicated folder.
The antispam service of Namirial S.p.A. operates in full compliance with current legislation and acts on the ordinary email traffic entering the PEC mailbox.

#### 3.2.1.4 FORMALLY INCORRECT MESSAGE

The Provider sends its user (the Sender) a **Non-acceptance Notice** whenever it detects, in the original message sent by that Sender, malformations and/or non-compliance with the regulations, such as the presence of the Bcc field.

#### 3.2.1.5 PRESENCE OF VIRUSES

A virus contained in the text or in the attachments of a certified email may be detected by the Sender's PEC Provider or by that of the Recipient.
If the Sender's PEC Provider detects the virus, the Sender receives a **Non-acceptance Notice for Virus**.
If the Recipient's Provider detects the virus at its Incoming Point, it sends the Sender's Provider a virus detection notice. As soon as it receives a virus detection notice, the latter Provider issues and delivers to its user (i.e. the sender of the original message) a **Non-delivery Notice for Virus**.
Messages containing viruses are kept by the Provider for a period of not less than 30 months.

#### 3.2.1.6 MAXIMUM TIME LIMITS EXCEEDED

After a Transport Envelope has been sent by the Sender's Provider, the Recipient's Provider may be unable to exchange information with the Sending Provider (Take-charge Receipt, Delivery Receipt, Non-delivery Notice, etc). If this situation continues beyond 12 and 24 hours after sending, the Sender's Provider is required to inform the sender by sending information on the outcome of their message.
In such cases, the protocol is as follows:

- after 12 hours from sending, during which there has been no news of the Transport Envelope (i.e. no communication in the form of receipts has arrived from the Recipient's Provider), the Sender's Provider issues and sends its user a **Non-delivery notice for maximum time exceeded**. The notice states that the signed message *"has not been delivered in the first twelve hours after it was sent"* but does not rule out that this may happen in the following 12 hours.

- after a further 12 hours from the first notice (24 in total from sending), without any information having been received from the Recipient's Provider, the Sender's Provider issues and sends its user a second **Non-delivery notice for maximum time exceeded**. The notice informs the Sender that the signed message *"has not been delivered in the twenty-four hours after it was sent. The sending is to be considered unsuccessful*".

# 4 THE PEC SERVICE OF NAMIRIAL S.P.A.(G)

The PEC service of the Provider Namirial S.p.A. is outlined below, together with a description of its main features.

## 4.1 FEATURES OF THE OFFER

The certified email offer of Namirial S.p.A. is aimed at private individuals, professionals, public bodies and businesses throughout Italy
Please note that, under current legislation, messages are to be considered received when they are delivered to the user's mailbox and not when the user downloads and/or reads them.
Obviously, once the capacity limit of the PEC mailbox has been reached, further messages are rejected and not delivered. That said, the Provider advises and recommends **regularly downloading** the messages of the Certified Email mailbox.
The Provider reserves the right to permanently delete PEC messages that remain in the Recycle Bin of the Holder's PEC mailbox for a period of more than 30 days.
The Provider reserves the right to change over time the features of the offer, set out below.

## 4.2 OFFER DETAILS, SUPPLY CONDITIONS AND RATES APPLIED

For details and costs of the various services described below, as well as how to subscribe to them, please refer to the website http://www.sicurezzapostale.it

## 4.3 ACTIVATION OF THE SERVICE THROUGH A SALES PARTNER

Namirial S.p.A. also uses sales partners to distribute its PEC service. The sales partner collects the information needed to identify the customer (the so-called Applicant) who has asked to subscribe to the service, as well as information on: offer, number of mailboxes, any optional services requested.
Once this information has been acquired and its correctness and completeness verified, **the customer enters into a contract directly with the Service Provider**. All the contractual documentation, containing the conditions of the service purchased, is in fact prepared by the Provider Namirial S.p.A..

### 4.3.1 LOCAL REGISTRATION AUTHORITY (LRA)

The Provider uses Registration Offices located throughout the country (LRA), which, directly or through their appointed persons (IR), carry out the following intermediate activities between the Provider and the Applicant:

- Identification and pre-registration of the Applicant;
- Checking that the documentation required to request the certified email account is in order;
- Support to the Holder and the Provider in the renewal, revocation and suspension of accounts.

The LRAs are activated by the Provider after adequate training of their staff assigned to identification and, where applicable, registration functions. The Provider checks that the procedures used by the LRA and by the operators (IR) responsible for Registration comply with the provisions of this manual.

### 4.3.2 OBLIGATIONS OF THE LOCAL REGISTRATION AUTHORITY (LRA)

The LRA, in the person of the Registration Officer (IR), is required to guarantee:

- the verification of the Applicant's identity and the registration of their data;
- that the Applicant is expressly informed of the need to protect the secrecy of the password;
- the communication to the Provider of all the data and documents acquired during identification, in order to start the procedure for activating the PEC account;
- the verification and forwarding to the Provider of the request for closure
- of the PEC mailbox;
- that the activities entrusted by the Provider to the LRA are carried out according to the rules and procedures described in this Operating Manual;
- the compliance of its data security system with the security measures for the processing of personal data, as described in §8.6 in accordance with the provisions of the GDPR.

## 4.4 IDENTIFICATION

Before issuing the PEC account, the Provider verifies the Applicant's identity. The identification procedure requires the Applicant to be personally recognised by the parties referred to in § 4.4.1, who verify their identity by checking their Identity Card or an equivalent document (cf. art. 35, paragraph 2, of Presidential Decree no. 445 of 28 December 2000), which must be valid.

### 4.4.1 PARTIES AUTHORISED TO CARRY OUT IDENTIFICATION

The Applicant's identity may be established by one of the following parties:

- the Provider, also through its appointed persons (IR);
- an LRA, also through its appointed persons (IR);
- a Public Official.

### 4.4.2 IDENTIFICATION PROCEDURES

The party carrying out the identification verifies the Applicant's identity by checking one of the following documents, valid and not expired, as provided for by art. 35, paragraph 2, of Presidential Decree no. 445 of 28 December 2000:

- Identity Card;
- Passport;
- Driving licence;
- Boat licence;
- Pension book;
- Licence to operate heating systems;
- Firearms licence.

In addition to those listed, other identity cards are accepted, provided that they bear a photograph and a stamp and are issued by a State Administration.
Identification by Public Officials may also be carried out on the basis of the rules governing their activities, including the provisions of Decree-Law no. 143 of 3 May 1991, as amended and supplemented.

## 4.5 DOMAIN NAMES AND MAILBOX NAMES

The names of the domains and of the mailboxes are chosen and indicated by the customer. However, the Provider reserves the right to refuse them if it considers them offensive, disrespectful or harmful to third parties.

## 4.6 ISSUE OF PEC MAILBOXES

The following figure outlines a diagram, illustrative and not exhaustive, of the flow describing the issue of a certified email mailbox.

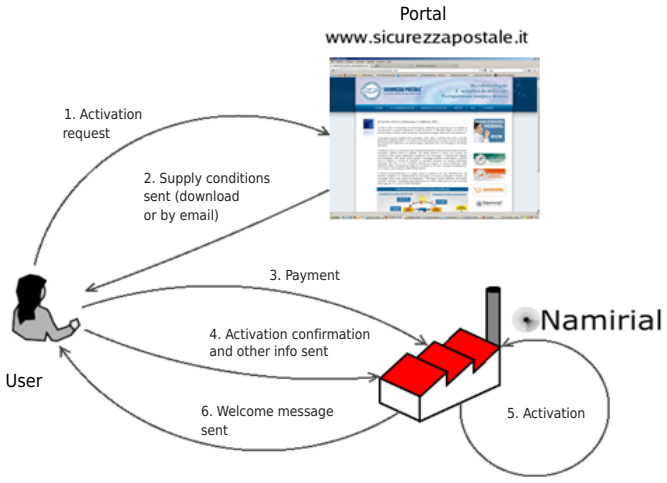



*Figure 2: PEC mailbox activation flow*

### 4.6.1 MAILBOX ACTIVATION REQUEST

To activate a PEC mailbox, the Applicant must download the following forms (steps 1 and 2 of Figure 2), available on the Service website:

- "Subscription request";
- "General terms and conditions";
- "Privacy notice on the processing of personal data";

After reading the "General terms and conditions" and the "Privacy notice on the processing of personal data", the applicant fills in the "Activation Request" form with their personal data and, where applicable, address details (depending on whether the applicant is a natural person, a company, a body, etc.), signs the request by hand or digitally and sends it to the Provider, together with a copy of a valid identity document (if the request is signed by hand) and a copy of the payment made, as provided for in the request itself (step 3 of Figure 2).
The "Activation Request" form can be sent to the Provider in the following ways (step 4 of Figure 2):

- **Fax**
- **Registered letter with return receipt**
- **PEC or PEO**
- **Online channels set up by the Provider or by its LRAs**

### 4.6.2 MAILBOX ACTIVATION

After verifying the correctness and plausibility of the information sent by the customer, the Provider activates the mailbox and any domains requested (step 5 of Figure 2). Then, to confirm the activation, the Provider sends the applicant a welcome email (step 6 of Figure 2) containing all the details of the service provided. In particular, the following system access parameters are sent:

- login;
- password;
- smtp server;
- pop/imap server;
- webmail address;
- information on retrieving LOGs, requesting assistance, changing the password, etc.

#### 4.6.2.1 RECOMMENDATIONS FOR USERS

In addition to the provisions of § 7.2, a vademecum is provided below with some suggestions for the correct and secure use of certified email and for the management of the PEC mailbox of the Provider Namirial S.p.A.:

- the PEC mailbox should be used for official communications and not for normal correspondence, for which it is advisable to use an ordinary email mailbox;
- since certified emails are deemed received as soon as they are delivered to the recipient's mailbox, the holder is invited to check their mailbox frequently. If necessary, it is advisable to save and then delete older messages, so as always to have space available and thus prevent PEC messages from being rejected because the mailbox is full. The Provider reserves the right to permanently delete PEC messages that remain in the recycle bin for more than 30 days;

- the user is required by the system to change the password at first access. The new password must comply with the format and security policies indicated, and it cannot be reused for a period set by the Provider. It is advisable to change the password at least every 90 days.
- it is advisable to configure the workstation so as to meet the minimum security requirements.

## 4.7 ADDITIONAL SERVICES

Namirial S.p.A. offers its customers a range of additional services to enrich the basic offer:

- Acceptance of incoming conventional email or its forwarding to a conventional email chosen by the mailbox holder
- PEC receipt notification
- Daily report by email and SMS
- Archiving of PEC messages

- Legally compliant retention of PEC messages
- Mailboxes for bulk sending
- Custom certified domains
- Closed domain

### 4.7.1 ACCEPTANCE OF INCOMING CONVENTIONAL EMAIL OR ITS FORWARDING

By default, conventional email is not allowed into the PEC mailbox. This is a deliberate choice of the Provider Namirial S.p.A., dictated by the advisability of protecting the content of the mailbox from incoming messages with no legal value.
This rule can however be changed, through the "Settings" panel of the webmail, in the following ways:

- Accept non-certified messages into the mailbox as well. The system will handle them in accordance with the technical rules, therefore delivering them inside an anomaly envelope.
- Forward messages from conventional email addresses to a conventional email address chosen by the holder; non-certified messages will not enter the webmail but will be redirected to that address.

### 4.7.2 PEC RECEIPT NOTIFICATION

The PEC receipt notification is a function that allows the holder to receive a specific conventional email message, at an address of their choice, whenever they receive a PEC (transport envelope).
The notification contains the key elements of the PEC email just received and can be configured in the "Settings" section of the webmail.
ATTENTION: the provider shall not be held responsible for failure to receive the notification which, being delivered to a non-certified email address, does not enjoy the full technical and legal certainty of delivery. The holder is therefore responsible for checking their PEC mailbox, regardless of whether notifications are received.

### 4.7.3 DAILY REPORT BY EMAIL AND SMS

The report consists of a daily notification, by email or by SMS, summarising what has been received in the PEC mailbox in the last 24h.
The report is sent, to the contact details and at the time indicated by the holder, if new notices, receipts or certified messages have been received in the last 24h.
ATTENTION: the provider shall not be held responsible for failure to receive the report which, being delivered through non-certified channels, does not enjoy the full technical and legal certainty of delivery. The holder is therefore responsible for checking their PEC mailbox, regardless of whether the report is received.

### 4.7.4 ARCHIVING OF PEC MESSAGES

The PEC archive makes it possible to save automatically, in a separate and secure area, a copy of incoming messages and of receipts.
To make it easier to consult, the archive can be accessed both from the webmail and through email clients.
Space for archiving can be freed by deleting messages or folders through the webmail; however, the utmost care must be taken during deletion, as it is irreversible.
On the other hand, it is not possible to delete or, in general, modify the archive through the email client.
In the "Settings" section of the webmail, the holder can decide the type of messages to be archived, choosing among the options offered and thus being able to limit the space occupied in the archive.

### 4.7.5 LEGALLY COMPLIANT RETENTION OF PEC MESSAGES

StrongPEC is the legally compliant digital Retention service for PEC messages of the provider Namirial S.p.A.
It can be activated on any PEC mailbox and automatically places a copy of incoming messages in legally compliant retention.
Once retained, messages are accessible through the webmail; to guarantee the integrity of the system, it is not possible to free space or make changes to the service.
The space available for Retention and the space used are updated in the webmail.
In the "Settings" section of the webmail, the holder can decide the type of messages to be retained, choosing among the items offered and thus being able to limit the space occupied in the service.

### 4.7.6 MAILBOXES FOR BULK SENDING

The bulk sending service of Namirial S.p.A. consists in providing PEC mailboxes with guaranteed performance, both in terms of sending/receiving and of consultation.

It is a service designed to meet the needs of large companies that require PEC systems with guaranteed response times and high traffic volumes.

### 4.7.7 CUSTOM CERTIFIED DOMAINS

Namirial provides custom services on PEC domains and DNS management; in particular, it supplies:

- **PEC Domain Certification**
  PEC certification of the domain chosen by the customer
- **PEC Domain management and certification**
  Registration, DNS management and domain certification
- **PEC Domain management and certification and interface customisation**
  Registration, DNS management and domain certification, graphic customisation of the webmail and of its access points.

### 4.7.8 CLOSED DOMAIN

A Closed PEC Domain is a domain, certified by the provider Namirial, whose mailboxes are intended for certified correspondence exclusively with other PEC mailboxes of the same provider registered in advance.
In other words, Namirial offers the opportunity to request the activation of PEC mailboxes on a dedicated domain, which can receive, or send and receive, exclusively with other PEC mailboxes identified in advance.
In particular, when a user tries to send an email to a mailbox that has not been registered, a blocking window appears with a notice that the email cannot be sent. If a message is sent to a mailbox with a closed domain from an unregistered PEC or from a conventional email, it is blocked and the sender receives a notice stating that the destination mailbox is intended exclusively for communication with specific mailboxes and therefore cannot receive from the sending address. The Closed PEC Domain service of Namirial S.p.A. fully complies with the relevant regulations.

## 4.8 ACCESS TO THE SERVICE[(I)]

The PEC mailbox can be used both through the web, using the webmail, and through the most common email clients. Guides for configuring and using the PEC mailbox on clients are available on the website of the Provider's Service.

### 4.8.1 ACCESS THROUGH EMAIL CLIENTS

The holder can access the mailbox through the most common email clients (such as Thunderbird, Outlook Express, Outlook) that meet the requirements for verifying the Provider's signatures, described in paragraph 9.2 of the annex to [V] "Technical rules for the service of transmitting electronic documents by certified email." The welcome message, sent to the mailbox holder after its activation, lists all the configuration parameters needed to access the system through email clients, and in particular:

**Basic access parameters:**

| **IMAPS** | |
|---|---|
| **IMAP server address** | **imaps.sicurezzapostale.it** |
| **Account name** | certified email address |
| **Password** | the password assigned to the mailbox |
| **Use SSL** | enabled |
| **Port** | 993 |

| **POPS** | |
|---|---|
| **POP server address** | **pops.sicurezzapostale.it** |
| **Account name** | certified email address |
| **Password** | the password assigned to the mailbox |
| **Use SSL** | enabled |
| **Port** | 995 |

| **SMTPS** | |
|---|---|
| **SMTP server address** | **smtps.sicurezzapostale.it** |
| **Account name** | certified email address |
| **Password** | the password assigned to the mailbox |
| **Use SSL** | enabled |
| **Port** | 465 |

**Pro access parameters:**

| **IMAPS** | |
|---|---|
| **IMAP server address** | **pro-imaps.sicurezzapostale.it** |
| **Account name** | certified email address |
| **Password** | the password assigned to the mailbox |
| **Use SSL** | enabled |

| | |
|---|---|
| **Port** | 993 |
| | |
| **POPS** | |
| **POP server address** | **pro-pops.sicurezzapostale.it** |
| **Account name** | certified email address |
| **Password** | the password assigned to the mailbox |
| **Use SSL** | enabled |
| **Port** | 995 |
| | |
| **SMTPS** | |
| **SMTP server address** | **pro-smtps.sicurezzapostale.it** |
| **Account name** | certified email address |
| **Password** | the password assigned to the mailbox |
| **Use SSL** | enabled |
| **Port** | 465 |

Once the email client has been configured, the holder can use the PEC mailbox like an ordinary mailbox. The only differences concern the formats of the messages and receipts delivered. In fact, for each message sent and delivered without anomalies, the sender receives:

- an **Acceptance Receipt sent by their PEC Provider**; the acceptance receipt is an email message with the subject "ACCETTAZIONE:" (acceptance receipt), followed by the subject of the original message sent, and containing a text indicating that the outgoing message is correct, has been accepted by the system and has been addressed to the recipients in the original message (distinguishing certified recipients from non-certified ones).
- a **Delivery Receipt for each certified recipient in the original message**. The delivery receipt is sent by the Provider of the recipient's PEC mailbox and is an email message with the subject "CONSEGNA:" (delivery receipt), followed by the subject of the original message, and containing a text indicating that the message has been delivered to the recipient's mailbox. The receipt includes, as an attachment, an xml file containing the certification data and, in the case of a full receipt, the complete original message with attachments.

The recipient, for their part, receives:

- the **Transport Envelope**, which is an email message with the subject "POSTA CERTIFICATA:" (certified email), followed by the subject of the original message, and containing in the text an indication that it is a PEC message. The message contains, as an attachment, the original email complete with any attachments.

Special cases are handled through different notices, which have in common a subject with a particular prefix, followed by the original subject; these notices include a text explaining their type. Some of them are: non-delivery notice, non-acceptance notice for virus, non-delivery notice for maximum time exceeded, etc.

### 4.8.2 ACCESS VIA WEBMAIL

The PEC mailbox holder can access it through a common Internet browser.
The address (HTTPS, browsing through a secure channel) of the Namirial webmail system is https://webmail.sicurezzapostale.it and is communicated to the holder in the welcome message sent after the mailbox has been activated.
Using an internet browser:

- the user connects to the specific address mentioned above;
- the webmail application responds at that web address, and access to it requires entering the access credentials;

- at first access the user must change the password;
- once access to the system has been validated, the user is inside the webmail application, where they can send, receive and search for messages, manage and use any additional services requested and change the application settings.

Through the webmail the user can choose, for each original message to be sent, the type of delivery receipt. As specified in § 3.2, the receipt can be full (i.e. containing the original message and any attachments), short (containing the original message with a hash code of the attachments) or summary (containing only the certification data).

## 4.9 LOSS OF THE SYSTEM ACCESS CREDENTIALS

If the system access credentials are lost, the holder of a PEC mailbox can reset the password by following the instructions at the following link: https://adesione.sicurezzapostale.it/RESETPSW/.
Alternatively, the holder can request a new password from the Provider by sending a form, which can be downloaded at the link http://www.sicurezzapostale.it/docs/Richiesta_credenziali_accesso.pdf, in which the following information must be given:

- PEC mailbox
- Name, Surname and any Company Name
- Address (Street, City, Postcode, Country)
- Tax Code and any VAT Number
- valid email (for any communications)

The request can be sent by certified email, fax or registered letter with return receipt, as indicated in the request form.
With the form, the holder must send a photocopy of a valid identity document.
The help desk staff of the Provider Namirial S.p.A. handle the processing of the requests received.

## 4.10 REQUEST AND RETRIEVAL OF MESSAGE LOGS(H)

As provided for by the regulations, holders of certified email mailboxes can request from their provider extracts of the contents of the LOG files relating to their PEC mailbox. The request can be made using the form available at the link: http://www.sicurezzapostale.it/docs/Modulo_Richiesta_LOG.pdf filled in with the following information:

- Holder's name and surname
- Sender's PEC mailbox
- Recipient's PEC mailbox
- Reference date of the message to search for
- Subject of the message to search for (optional)
- Identifier of the message to search for (optional)

The request can be sent by certified email, fax or registered letter with return receipt, as indicated in the request form.
Alternatively, the request for LOG files can be made by sending a request directly from one's own PEC mailbox to the Provider's PEC address, giving the minimum data needed to retrieve them (see previous bullet point).
With the form, the holder must send a photocopy of a valid identity document.
The certified email address used by the provider to receive LOG requests from users is also communicated to them in the welcome message sent after the mailbox has been activated.
Once the requested information has been retrieved, the help desk staff of the Provider Namirial S.p.A. communicate it to the customer by certified email or by any alternative means.

## 4.11 REQUEST FOR CLOSURE OF A PEC MAILBOX

The holder can ask the Provider to close their certified mailbox using the form available at the following link:
http://www.sicurezzapostale.it/docs/Richiesta_Cancellazione_casella_PEC.pdf.
The form must contain the following information:

- PEC to be closed
- Name, Surname and any Company Name
- Address (Street, City, Postcode, Country)
- Tax code and any VAT number
- valid PEO email (for any communications)

The request can be sent by certified email, fax or registered letter with return receipt, as indicated in the request form.
Alternatively, the closure of the PEC mailbox can be requested by sending a request directly from one's own PEC mailbox to the Provider's PEC address, giving the minimum data needed (see previous bullet point).
With the form, the holder must send a photocopy of a valid identity document.
The closure request can only be made by the mailbox holder. Following it, the Provider carries out a series of checks and sends the holder a communication, by PEC, stating the closure date of the mailbox.

The Provider also has the right to close a PEC mailbox in the event of contractual breaches by the Holder, described in the General Conditions of the Service.
As the contract expiry date approaches, the Provider sends the Holder expiry notices and an invitation to renew it. If the holder does not renew within the time limits, the Provider reserves the right to suspend the account for 30 days, after which, in the absence of renewal, the mailbox is closed.

When a mailbox is closed:

- the Holder can no longer use it to send or receive new messages;
- the Provider keeps its content for 180 days after closure; it also reserves its name, which therefore cannot be assigned to a different applicant; consequently, during this 180-day period the holder may request the restoration of the mailbox, its functions and its content;
- once the 180-day period has elapsed, without any action by the holder, the entire content of the closed mailbox is deleted. The mailbox name also remains reserved and can no longer be used for new activations. The holder can always request the activation of a new mailbox with the same name but without the content of the previous one.

## 4.12 TERMINATION OF THE CERTIFIED EMAIL SERVICE(L)

If Namirial S.p.A. ceases its activity as Certified Email Provider, it notifies the Agency for Digital Italy at least sixty (60) days before the termination date, indicating, if known, the Substitute Provider that will take over the active PEC mailboxes.
At the same time, with the same notice, the Provider announces to holders the termination of its activity as Provider, through a direct communication by PEC and an official communication published on its website.
If no Substitute Provider is to take over the PEC mailboxes, the termination notice specifies that all mailboxes will become inaccessible from the time the activity ceases.

## 4.13 HELP DESK SERVICE

For the handling of issues relating to the certified email service, the Provider Namirial S.p.A. has set up a specific communication channel (Help Desk) with end users.

The Help Desk consists of a staff of people trained and assigned to customer support for the certified email service and can be reached at the automatic dialling number given in § 2.4 during office hours: from 9.00 to 19.00, Monday to Friday.
Requests for assistance can also be sent 24 hours a day by email to pec@namirial.com or through the Provider's institutional website, at the following link: https://support.namirial.com/it/supporto-tecnico/ stating the service for which assistance is requested and filling in the required information.
Requests made by email or through the portal, if received outside working hours or on public holidays, are taken in charge from the next working day.
The customer of the service may obtain general information on certified email (how it works, possible uses of the channel, legal validity of PEC messages, etc.) and specific details on the service provided, such as:

- how to configure the email client;
- how to access and use the webmail;
- how to obtain the access credentials again after losing them;
- how to obtain an extract of the LOG files;
- what security guarantees the service offers;
- how personal data are processed.

The customer can report any problems encountered when sending and/or receiving messages through the email client or the webmail.

### 4.13.1 TROUBLE TICKETING

Through the trouble ticketing system, Namirial S.p.A. keeps track of all reports made by its customers.
The system is based on a web-based application, through which the Help Desk staff can:

- create a new ticket following a report from the customer;
- follow the "life" of the ticket through updates and status changes, up to the final resolution of the support request;
- update the ticket, recording the work done and the communications with the customer;
- search for tickets on the basis of a range of information such as the creation date, the category, the identifier of the operator handling the report etc.

All status changes are notified to the user who made the report by means of an email message.

## 4.14 SERVICE LEVELS AND QUALITY INDICATORS(J)

The Provider Namirial S.p.A. guarantees compliance with the service levels required by the regulations.

| **Service Levels** | |
|---|---|
| Maximum number of simultaneous recipients accepted in a single original message | **At least 50** |
| Maximum size of each single message (understood as the product of the number of recipients and the size of the message) | **At least 100MB from email clients** |
| Availability of the service in the reference period (four months) | **Equal to or greater than 99.8%** |
| Unavailability of the service for a single outage in the reference period (four months) | **Less than or equal to 50%** |
| Maximum time for issuing the acceptance receipt in the service availability period (calculated excluding transmission times) | **30 minutes** |

*Table 5: service levels*

The following table lists the quality indicators of the certified email service of the Provider Namirial S.p.A.

| **Quality indicators** | |
|---|---|
| Availability of the service (sending, receiving and consulting PEC messages) | **24x7x365** |
| Availability of the activation request service | **24x7x365** |
| Time to activate a new PEC account (from receipt of all the necessary documentation) | **6 working days** |
| Availability of the service for requests by the holder for message LOGs relating to the communications made | **24x7x365** |
| Access to LOG files by Namirial S.p.A. staff | **Monday to Friday from 9.00 to 19.00** |
| Maximum time for sending information on LOG files following a request by the holder | **5 working days** |
| Availability of the monitoring system, with alert messages sent by email and/or SMS when malfunctions and critical situations occur | **24x7x365** |
| Support through the call centre | **Monday to Friday from 9.00 to 19.00** |
| Receipt of reports from customers | **24x7x365** |

*Table 6: service quality indicators*

# 5 DESCRIPTION OF THE SOLUTION

## 5.1 MAIN FEATURES

The Namirial S.p.A. solution has the following features:

- full compliance with current certified email legislation, in terms of functionality as well as interoperability and security;

- security of the hardware, software and network infrastructure;
- security in the adoption of service provision procedures and processes;
- security through the use of qualified, trained and responsible staff;
- security and care in the management of sensitive data;
- scalability, modularity and extensibility of every component of the system;
- compatibility with all email clients (Outlook, Outlook Express, Thunderbird, etc.) that meet the minimum requirements set by the technical rules referred to in [V];
- compliance with the international standard RFC3161 for time stamping LOG files and for interfacing with an accredited Time Stamping Authority;
- integration with the most common network types on the market;
- use of high-security hardware signature devices (tamper-proofness/tamper-evident) for managing and maintaining both the keys and the signature certificates;
- use of hardware devices for signing and verifying messages.

## 5.2 SCALABILITY AND RELIABILITY

The architecture of the Provider Namirial S.p.A. is highly scalable; it can therefore be extended at any time to meet growing demand, so as to maintain the response times and quality levels provided by the Provider.
As regards the reliability of the architecture, it is important to note that all the servers, network devices and signature devices are installed in a redundant and load-balanced configuration. In this way there is no “single point of failure” and any malfunction of a device does not cause a service outage. In addition, shared storage is used to store common information, so as to guarantee availability, reliability and continuity of the service.

## 5.3 DATA SECURITY

The private keys and certificates used in message signing operations are entirely managed and kept inside high-security devices (**hardware security module** or **HSM**). The same devices are also used to sign emails and to verify them. The HSMs used in the solution of the Provider Namirial S.p.A. have **FIPS 140-2 level 3** certification and offer the following features:

- **tamper evidence**: detection of tampering attempts or unauthorised access;
- **tamper proofness**: erasure of the memory and of the keys in the event of access or tampering.

## 5.4 SYSTEM FEATURES

The certified email solution adopted by Namirial S.p.A. is based on the **OpenPEC** product, an Open Source project created to build a Certified Email system compliant with the guidelines issued by the National Centre for Information Technology in Public Administration (DigitPA).
OpenPEC is designed as an extension of the most common Open Source mail servers on the market (such as Postfix) and has the following features:

- full compatibility with current legislation;
- high performance;
- reliability, scalability and modularity;
- compatibility with the main Hardware Security Module (HSM) vendors;
- ability to manage systems with a large number of domains and/or mailboxes;
- automatic and transparent updating of the local certified domains of the Provider;
- time stamping and archiving of logs.

## 5.5 TIME REFERENCES

The Ministerial Decree referred to in [V] establishes that a time reference must be applied to every message, receipt or notice. The time reference may deviate by no more than 1 second from the UTC (Coordinated Universal Time) reference scale. All the events making up the transaction at the access point, the incoming point and the delivery point use a single time value. In other words, the indication of the time at which the message is processed is unique within the LOGs, receipts, notices and messages generated by the system.

The primary time reference source of the PEC platform consists of the same devices used by Namirial to provide its accredited Time Stamp Authority service. Namirial is an eIDAS Qualified Trust Service Provider also for issuing qualified time validations and certificates. In particular, it has obtained certificate no. IT269191 issued by Bureau Veritas Italia SpA for issuing qualified time validations (time stamps).

**The PEC system therefore interfaces with the servers of the Time Certification and Validation service provided by Namirial S.p.A. To guarantee a correct and accurate time value, the NTP servers of the National Institute of Metrological Research (INRIM) are also contacted.** The system clock is kept synchronised with the reference clock, which also compensates for drift and fluctuations that may arise from system load, environmental variations and other factors.
The date format is ***dd/mm/yyyy*** where:

- **dd** are the 2 digits of the day
- **mm** are the 2 digits of the month
- **yyyy** are the 4 digits of the year.

The time format is **hh:mm:ss** where:

- **hh** are the 2 digits of the hours (00-23)
- **mm** are the 2 digits of the minutes
- **ss** are the 2 digits of the seconds.

The time data is followed, in round brackets, by the **zone**, i.e. the difference, in hours and minutes, between legal time and the UTC reference. The value of this difference is preceded by a + or – sign indicating a positive or negative difference with respect to UTC.
For example, the time reference ***07/12/2006 17:35:16 (+0100)*** indicates 7 December 2006, 17 hours, 35 minutes, 16 seconds, 1 hour ahead of UTC.

## 5.6 ARCHIVING OF LOGS AND OF MESSAGES CONTAINING VIRUSES, AND THEIR LEGALLY COMPLIANT RETENTION

The Ministerial Decree referred to in [V] establishes that every certified email system must provide for a single time interval of no more than twenty-four hours within which the legal LOGs of the messages are saved without interruption; the LOGs are kept for a period of at least 30 months.
A time stamp must be applied to the LOG files, which establishes, in a certain and legally recognised way, the exact moment at which the file is archived. The time stamp is a time reference validated by a trusted third party, the so-called **Time Stamping Authority** (**TSA**).
The Ministerial Decree also establishes the methods for detecting, reporting and retaining certified email messages containing viruses; in particular:

- when sending, it is at the Access Point, i.e. in the phase immediately following the sending of the message, that the sending provider must check for viruses in the original email messages. The system must then inform the sender that their message contains a virus, and this communication takes place through the issue of an “AVVISO DI NON ACCETTAZIONE PER VIRUS” (non-acceptance notice for virus).
- when receiving, the recipient provider must check for viruses at the Incoming Point. The system must issue and send to the sender’s provider a virus detection notice with the subject “PROBLEMA DI SICUREZZA” (security problem); consequently, the sender’s provider issues a message called “AVVISO DI MANCATA CONSEGNA PER VIRUS” (non-delivery notice for virus) and places it in the sender’s mailbox.

Messages containing viruses must be kept for a period of at least 30 thirty months, as established by the regulations referred to in [V] and [X].

On 5 July 2016, AgID also issued the "INSTRUCTIONS FOR THE RETENTION OF MESSAGE LOGS AND OF CERTIFIED EMAIL MESSAGES WITH VIRUSES", which require the provider to place the legal LOG files and the messages containing viruses in Legally Compliant Retention, in accordance with the provisions of Legislative Decree 82/2005 and the technical requirements of the Prime Ministerial Decree (DPCM) of 3 December 2013.
The retention process is intended to guarantee:

- the certain identification of the party that created the document (typically the party responsible for the document) and of the administration that produced the document;
- the integrity of the document;
- the intelligibility and easy retrieval of the documents and of the identifying information, including the original registration and classification data;
- compliance with the security measures described in §8.6, in accordance with the provisions of the GDPR

The solution adopted by Namirial S.p.A. complies with the regulations in question and does what is necessary to guarantee maximum continuity of service.

# 6 PROCEDURES AND TECHNOLOGICAL AND SECURITY STANDARDS USED

## 6.1 REFERENCE TECHNOLOGICAL STANDARDS

The list of reference technological standards is given below.

- RFC 1847 (Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted)
- RFC 1891 (SMTP Service Extension for Delivery Status Notifications)
- RFC 1912 (Common DNS Operational and Configuration Errors)
- RFC 2252 (Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions)
- RFC 2315 (PKCS 7: Cryptographic Message Syntax Version 1.5)
- RFC 2633 (S/MIME Version 3 Message Specification)
- RFC 2660 (The Secure HyperText Transfer Protocol)
- RFC 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)

## 6.2 SECURITY STANDARDS

For the provision of the certified email service, the Provider Namirial S.p.A. adopts the guidelines and principles of the **ISO 27001:2013** security standard.
The standard, which replaces the reference standard BS 7799 (Information Security Management System ISMS), requires a series of processes, measures and procedures to be carried out to provide all the guarantees of security and data protection needed in critical and sensitive systems such as certified email.
In a context where IT risks caused by breaches of security systems are constantly increasing, the ISO 27001:2013 standard aims to protect data and information from threats of all kinds, in order to ensure their:

- **integrity** (accuracy and completeness)
- **confidentiality** (accessible only to authorised individuals)
- **availability** (certainty that the information is always available to the staff in charge)

To this end, the guidelines provide, for both the company and its customers, the requirements needed to obtain an adequate system for managing the security of information and sensitive data.
The standard also provides procedures for:

- risk analysis (identification of weak points, study of possible threats and of the probability that they will occur, analysis of any impacts on the system)
- risk management (system monitoring, detection of problems and their resolution, elimination of weak points, reduction of risks for the entire system).

### 6.2.1 SIGNATURE DEVICES (HSM)

The HSM devices used to sign and verify PEC messages are certified according to the **FIPS 2** standard, published by the **National Institute of Standards and Technology** (**NIST**). The standard specifies the security requirements that must be met by cryptographic modules used within systems in which sensitive data are processed. This series includes the specifications of cryptographic modules and their interfaces, rules, services and authentication process. The requirements also cover physical security constraints and the Key Management process.
The FIPS 2 Standard consists of four qualitative security levels, the first 3 of which are met.

| Level | Security Type | Description |
|---|---|---|
| **Level 1** | Cryptographic modules | Security applied to cryptographic modules; in particular it concerns the encryption algorithms. |

| | | |
|---|---|---|
| **Level 2** | Physical security | Tamper evidence – Application of coatings and labels able to detect tampering attempts or unauthorised access. |
| **Level 3** | Physical security | Tamper proofness - Mechanisms able to erase the memory in the event of unauthorised access or tampering attempts.<br>Secure authentication systems with control of the roles and of the specific authorisations for each operator |
| **Level 4** | Physical security | Protects security against external environmental events such as temperature or voltage fluctuations. It is generally used for devices located in unprotected or uncontrolled environments. |

*Table 7: HSM security levels*

The signature devices used in the PEC system of the Provider Namirial S.p.A. are **FIPS-2 Level 3** certified (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf).

## 6.3 SECURITY MEASURES

The certified email system of the Provider Namirial S.p.A. offers all the security guarantees compatible with the type of service provided. The security measures listed below are described in more depth and detail in the **Security Plan**, a confidential document drawn up in accordance with the provisions of the circular referred to in [VI], kept at the Provider's premises and delivered to AgID.

### 6.3.1 HUMAN RESOURCES ASSIGNED TO SYSTEM MANAGEMENT

In compliance with the regulations, in addition to the Service Manager there are 5 other managers of the PEC service:

- Manager for the registration of holders
- Manager of technical services
- Manager of checks and inspections (auditing)
- Security Manager
- Manager of message LOGs and of the time reference system

The above managers each coordinate a working group made up of staff with the necessary experience and specifically trained through internal training courses. Each person in charge is made aware of their responsibilities and informed about the sensitivity of the service provided and the need to devote the greatest possible care and attention to carrying out the tasks assigned. In the initial phases, each new person in charge is personally followed by a company tutor.

### 6.3.2 INFRASTRUCTURE SECURITY

From a purely IT point of view, the security of the system is ensured by the Provider Namirial S.p.A through the adoption of a series of measures, such as:

- firewalls with very restrictive access policies (only the strictly necessary ports are enabled)
- antivirus system updated at least 4 times a day
- software products constantly updated, both following the release of new versions and of patches (before an update is put into production, tests are carried out in a dedicated testing environment)
- use of secure protocols for communication between the user and their provider (SMTP/S, POP3/S, IMAP/S) and between one provider and another (STARTTSL)
- signing of messages with FIPS-2 Level 3 certified HSM devices
- physical separation of the front end, back end and storage levels (so as to increase the degree of data protection)
- use of network storage external to the system, to increase the level of protection of user information
- system redundant in all its parts, so as to avoid a "single point of failure"
- backup system, to reduce the risk of data loss

### 6.3.3 RISK ANALYSIS AND MANAGEMENT

The certified email system of Namirial S.p.A. undergoes periodic checks, aimed at analysing its critical points, identifying its vulnerabilities and identifying the possible risks to which it is exposed. Thanks to careful analysis, the Provider

Namirial S.p.A. is able to prevent most malfunctions and to prepare to manage and solve problems that cannot be foreseen in advance. During the analysis, the possible faults are divided into:

- minor faults
- major faults

The former are defects caused by problems in the hardware and software systems and can generally be solved through ordinary or extraordinary maintenance, such as replacing devices or upgrading software components. The latter are failures caused by catastrophic events, malicious acts or human error due to incompetence or negligence, and may cause serious damage and service interruption.

### 6.3.4 ACTIONS TO COUNTER THE SPREAD OF MALICIOUS CONTENT

Namirial S.p.A. works constantly to improve the quality and security of the service by introducing up-to-date technologies and qualified staff. To guarantee maximum speed and effectiveness of intervention, what is described below must be understood as indicative and not exhaustive.
We would also point out that all the actions and efforts made by Namirial S.p.A. to counter the phenomenon in question remain a support to the user, who must always pay the utmost attention to using the PEC service securely.

#### 6.3.4.1 ANTI-MALWARE TECHNOLOGIES

Namirial S.p.A. uses several constantly updated anti-malware technologies in parallel.
The solutions in use do not merely search for virus signatures on different repositories but use innovative systems such as sandboxes and patented algorithms to detect 0-days.
The anti-malware analysis covers not only attachments but also the body of messages, with particular attention to URLs.
False positives are also monitored to adapt the behaviour of the systems to the traffic's specific features and changes over time.
Messages detected as malicious are handled according to the regulations and reported to the sender or to their provider.

#### 6.3.4.2 ATTACHMENT ANALYSIS

Attachments are the message component that receives the most attention from security systems.
Specific checks on attachments are carried out in addition to the action of the anti-malware tools, to block their sending or simply to warn the user of suspicious cases requiring the utmost attention.
In particular:

- the webmail applies some restrictions on the types of file that can be attached to a new PEC message: a user who tries to attach one or more files considered potentially dangerous will receive a notice with the name of the file that has been blocked.
  There are also checks on attachments that are viewed or downloaded from the webmail, and if the system detects potentially dangerous conditions a specific message will be shown to the user;
- access point: the same restrictions apply, causing new certified messages from email clients to be blocked and non-acceptance receipts containing a suitable warning message to be issued;
- incoming point: in the event of suspicious situations such as macros or encrypted attachments, a specific special header is added to the incoming transport envelope, which integrators can use for any reporting.

#### 6.3.4.3 PASSWORD POLICY

Namirial S.p.A. applies a set of rules to help the user choose a secure and reliable password.
The password is chosen by the mailbox holder and must meet predefined complexity requirements, which Namirial S.p.A. reserves the right to update at any time:

- it must be at least 8 characters long;
- it must contain alphanumeric characters, special characters _.-?#+;:!@, upper and lower case letters;
- recent passwords cannot be reused;
- it is checked that there are no commonly used words or repeated sequences of characters;
- it is checked that the password is not included in lists of passwords involved in data breaches;
- an information tool is provided that allows the user to easily assess the strength of the password entered.

The password can be changed by the mailbox holder from the *Settings* section of the webmail.
If it is lost, a new one can be set by accessing the dedicated link available on the login page of the webmail.

#### 6.3.4.4 SYSTEMS FOR MONITORING SUSPICIOUS ACTIVITY

Traffic analysis systems, not only automatic ones, are used to highlight attack patterns by correlating, among other things, the number of messages sent in the reference period, the source addresses, the type of mailbox and transparent antispam analysis of outgoing transport envelopes.
If Namirial S.p.A. detects anomalous behaviour in outgoing traffic, the PEC mailbox credentials will be reset immediately and the holder will be notified using the contact details held, with the suggestion to run a thorough antivirus scan of their workstation before updating their access credentials.

#### 6.3.4.5 MUTUAL ASSISTANCE PROCEDURES BETWEEN PROVIDERS

Namirial S.p.A. reserves the right to set up mutual assistance procedures between providers in order to strengthen the fight against the spread of malicious content conveyed through the PEC channel.
This may involve sharing URLs, message types, behavioural patterns and analyses, IOCs (Indication Of Compromise) and other information anonymously, always guaranteeing the utmost confidentiality in compliance with the provisions of the privacy regulation.

### 6.3.5 SPAM PREVENTION

In compliance with current legislation, Namirial S.p.A. provides the antispam service on the ordinary email traffic entering the PEC mailbox. Receipt of such traffic is optional and must be enabled through the *Settings* section of the webmail. This service merely alerts users through appropriate notices and moves messages considered unwanted and/or dangerous to a dedicated folder.
It is important to remember that the antispam service does not guarantee exact filtering but is a support tool for the user, who must always carefully assess the reliability of the messages received.

### 6.3.6 MONITORING OF SECURITY LEVELS

Security levels are checked through continuous monitoring of all the main components of the certified email system. Internal inspection visits are also carried out at least every six months, aimed at examining the system as a whole in order to verify its level of security and identify any critical points. To achieve certainty that the system is secure and compliant, the following are monitored:

- network devices (firewall, router, etc.)
- equipment (server, HSM, etc.)
- software components
- the organisational and procedural flows in place
- the work of the staff involved

Each visit ends with a detailed report that captures the state of the system, lists the checks carried out and highlights all the measures to be taken to improve the entire system. In addition to technical measures such as replacing, updating or upgrading hardware and software components, organisational changes may be made, such as changing an internal procedure or replacing staff deemed unsuitable for the service.

## 6.4 OPERATING PROCEDURES USED IN PROVIDING THE SERVICE(E)

Through careful staff organisation, scheduled backup management, accurate and constant system monitoring and the application of precise and established problem-solving procedures and methods, Namirial S.p.A. is confident that it can guarantee its customers high and consistent service levels over time.

### 6.4.1 STAFF ORGANISATION

As already mentioned in **§** 6.3.2 and in compliance with the Decree referred to in [V], Namirial S.p.A. has set up an internal structure made up of the following sector managers:

- 1 Service manager;
- 1 manager for the Registration of holders;
- 1 manager of Technical services;
- 1 manager of Checks and inspections (auditing);
- 1 Security manager;

- 1 manager of message LOGs and of the time reference system.

All the staff involved in providing the service have the knowledge and experience needed to carry out the tasks assigned.

### 6.4.2 MONITORING SYSTEM

All the certified email services of Namirial S.p.A. are constantly checked through a dedicated monitoring system. The system generates alert signals whenever the critical thresholds set during administration are exceeded. The alert signals, collected 24x7x365, are sent by email to the staff in charge, who are able to intervene promptly to resolve the critical issue. Through the monitoring system, the Provider Namirial S.p.A. checks the following parameters for all the machines in the system: disk space, CPU load, memory usage, process activity, queue status, etc.
In addition to internal checks, for security checks and system monitoring Namirial uses an external partner, in service 24/7/365, which, following the detection of malfunctions and/or anomalies, makes reports in the manner and within the times indicated in the manual.
The monitoring infrastructure is equipped with a SIEM system that processes all the information coming from the devices and Servers, performing a real-time analysis that makes it possible to intercept any attacks and send the related report to the above external SOC, with which H24 escalation procedures have been agreed according to the severity of the events detected.

### 6.4.3 PROBLEM MANAGEMENT AND RESOLUTION

Problems are managed according to the following procedure:

1) The **Help Desk** (**HD**) service takes charge of the report, which may come:
   - from outside, from a customer
   - from inside, from a member of the PEC service staff
   - from the monitoring system, following the detection of an anomalous event

   In all three cases, a help desk operator takes charge of the report and forwards it to the **Support Team** (**TdS**).
2) The TdS takes charge of the report, analyses it, verifies the actual extent of the problem and seeks a solution.
3) The TdS identifies the possible solutions to the problem and compares them, in order to select the best one in terms of least impact on the service and speed of resolution.
4) The TdS may consider the advisability of using third-party support, meaning either specialised internal staff or external consultants.
5) The TdS implements the solution and solves the problem. If support from staff outside the company has been planned, the TdS assists them throughout all the activities carried out and constantly supervises, tracking all the operations carried out in real time.
6) Once the work has been completed, the TdS informs the Help Desk.
7) The Help Desk service carries out a further check that the problem has been resolved and informs the person who made the report.

## 6.5 ACTIONS TAKEN BY THE PROVIDER IN THE EVENT OF MALFUNCTIONS

Under the CNIPA circular referred to in [VII], the Provider is required to promptly notify AgID of the malfunctions detected in its system. In the report, the Provider must also provide an initial assessment of the incident and describe any measures taken in this regard. Service disruptions are classified according to the following table:

| Type | Code | Description |
|---|---|---|
| Uncontained anomalous behaviour | 1A: detected by the provider | Behaviour not compliant with the technical rules referred to in art. 17 of Presidential Decree no. 68 of 11 February 2005, relating to the basic functions (processing of the original message, receipts and notices), whose potential impact is not contained. |
| | 1B: detected by third parties | |
| Contained anomalous behaviour | 2A: detected by the provider | Behaviour not compliant with the technical rules referred to in art. 17 of Presidential Decree no. 68 |

| | | |
|---|---|---|
| | 2B: detected by third parties | of 11 February 2005, relating to the basic functions (processing of the original message, receipts and notices), whose potential impact is contained. |
| Blocking malfunction | 3A: detected by the provider | Type of malfunction as a result of which the functions of the PEC system, as defined in the technical rules referred to in art. 17 of Presidential Decree no. 68 of 11 February 2005, cannot be used in whole or in part by users. |
| | 3B: detected by third parties | |

*Table 8: actions taken in the event of malfunctions*

User reports are classified according to the following identification codes:

| Code | Description |
|---|---|
| **RC** | Report of a complaint relating to the contractual relationship |
| **AL** | Report of a complaint relating to the LOG access procedure |
| **SA** | Report of an anomaly/service disruption not attributable to the provider (client, internet connection, management of decentralised user accounts) |

*Table 9: classification of malfunction events*

In cases 1A and 1B the provider suspends its own service, informing its users and the other providers. In cases 2A and 2B the Supervisory Body may decide to suspend the provider's service until the problem has been solved. In both cases the provider implements the suspension; this results in an "AVVISO DI NON ACCETTAZIONE" (non-acceptance notice) for formal exceptions (for outgoing messages) and in the Take-charge Receipt not being issued for messages coming from the other Providers.
In the event of suspension and once the service disruption has been eliminated, the Provider Namirial S.p.A. may resume its activity. In this case it must send the Supervisory Body a detailed report on what happened and on the measures taken.

# 7 OBLIGATIONS AND RESPONSIBILITIES

## 7.1 OBLIGATIONS AND RESPONSIBILITIES OF THE PROVIDER

In compliance with current legislation and the provisions of the Decree referred to in [V], the Provider Namirial S.p.A. undertakes to:

- comply with and guarantee the service levels provided for;
- guarantee interoperability with the other accredited Providers;
- keep the LOGs relating to the transmissions that have taken place and make them available, in the manner provided for in this manual, for the uses provided for by law;
- send its customers information on how to request, search for and present message LOGs;
- inform the holder about how to access the service and the necessary technical requirements;
- record, in a dedicated LOG file, the individual transmission phases of each message;
- keep the LOG files for at least 30 months;
- apply the time stamp to the LOGs of message transmissions;
- issue all the receipts, envelopes and notices provided for by the regulations (transport envelope, take-charge receipt, acceptance receipt, delivery receipt, non-acceptance notice, non-delivery notice, non-delivery notice for maximum time exceeded, virus detection notice, etc.);
- apply a time reference to every message;
- preserve the integrity of the original message in the related transport envelope during every transmission;
- comply with the rules of European Regulation 679/2016 (GDPR) on the protection of personal data;
- not keep the private passwords of the corresponding certified email accounts;
- detect messages containing computer viruses and issue the related notices;
- keep messages containing computer viruses for the period provided for by the regulations;
- adopt measures to prevent the introduction of harmful executable code;
- adopt emergency procedures and services to ensure that transmission is completed even in the event of incidents (except for disastrous and sudden events such as earthquakes, attacks, etc.);
- guarantee the confidentiality, integrity and unalterability, also over time, of the LOG files;
- guarantee the secrecy of the correspondence transmitted through its certified email system;
- use secure protocols to guarantee the secrecy, authenticity and integrity of the information transmitted through the PEC system;
- keep the information on the agreements made with customers, in compliance with current legislation;
- activate/deactivate a PEC mailbox after verifying the authenticity of the request and the plausibility of the data it contains;

- uniquely associate the holder and the certified email mailbox;
- issue and/or renew a requested PEC account, according to the procedures described in this Operating Manual;
- revoke and/or suspend a PEC account, promptly notifying the holder and giving the reasons, in the manner provided for in this Operating Manual;
- adopt a procedure for replacing the electronic certificates relating to its signature keys in such a way as not to cause service interruptions;
- promptly request the revocation of the certificates relating to the keys used for signing messages and for the secure connection to the AgID website, in the event of their proven compromise;
- adopt security measures to prevent the unlawful and uncontrolled duplication of the private signature keys or of the devices containing them;
- promptly notify its users of any termination and/or interruption of the Certified Email service;

- adopt security measures to allow only authorised persons logical and physical access to the system;
- use a time reference system that constantly guarantees the synchronisation of the machines involved, with a deviation of no more than one minute with respect to the Coordinated Universal Time (UTC) scale;
- use signature devices that comply with current legislation.

## 7.2 OBLIGATIONS AND RESPONSIBILITIES OF THE HOLDERS

**The Holder is solely and exclusively responsible for the content of their messages.** By subscribing to the service offered by the Provider Namirial S.p.A., the Holder undertakes to:

- use the service only for the uses permitted by law;
- give consent to the use of their personal data, pursuant to European Regulation 679/2016 (GDPR);

- provide the Provider with all the information needed to identify themselves and to activate the service, guaranteeing, under their own responsibility, the authenticity and accuracy of the data provided;
- promptly send the Provider any changes and/or updates to be made to the data provided, should such data have changed;
- use the PEC mailbox securely, protecting and keeping their passwords with the utmost care in order to guarantee their integrity and confidentiality;
- keep a copy of the messages sent and/or received, together with the related receipts;
- adopt measures to prevent the introduction of harmful executable code (virus/malware/etc.) into messages;
- equip themselves with an up-to-date, valid operating system, constantly updated with respect to the requirements of national privacy legislation, as well as with suitable intrusion prevention, antispam and antivirus systems;
- inform any persons authorised to use their mailbox of the security rules designed to prevent unauthorised use of the mailbox.

If the Holder fails to comply with the above obligations, the Provider Namirial S.p.A. reserves the right to suspend the PEC service or to disable the PEC mailbox, with immediate effect and without being bound to give notice, until the termination of the related contractual relationship with the Holder, in the most serious cases.
Private individuals wishing to use the certified email service in their dealings with the Public Administration must expressly declare their address; businesses, in their dealings with each other, may declare their explicit willingness to accept certified email by indicating their PEC mailbox in their registration with the Companies Register. Both declarations are binding only on the declarant and are revocable.

## 7.3 LIMITATIONS AND COMPENSATION

In no event shall the Provider Namirial S.p.A. be liable for events not attributable to it, and in particular for damage caused by the LRAs, Holders, Applicants, Users or any third party, directly or indirectly, as a result of their failure to comply with the rules and obligations set out in this Operating Manual; furthermore, in no event shall the Provider be liable for the failure of those parties to adopt measures of special diligence suitable to avoid causing damage to third parties and which are required of users of certification services, or for the carrying out of unlawful activities.
In no event shall the Provider Namirial S.p.A. be liable for breaches or harmful events caused by fortuitous events or force majeure.
Without prejudice to the mandatory limits of the law, the Provider Namirial S.p.A. shall not be liable for damage caused by malfunctions, delays or interruptions, provided that they fall within the service levels described in this manual.
Without prejudice to the mandatory limits of the law, the Provider Namirial S.p.A. can in no way be held liable, by way of example but not limited to, for damage arising from force majeure, fortuitous events, catastrophic events (fires, earthquakes, explosions) or in any case events not attributable to Namirial S.p.A., should they cause delays, malfunctions or interruptions of the service.
The Provider Namirial S.p.A. assumes no obligation regarding the retention of the messages sent and transmitted through its PEC mailboxes. This responsibility is assumed exclusively by the customer/holder.
The Provider Namirial S.p.A. has no responsibility for the content of the messages sent and received through its PEC mailboxes.
The Provider Namirial S.p.A. reserves the right to amend this operating manual if technical changes are made to the system, or in the event of changes to the commercial offer or regulatory adjustments.
For matters not provided for in this chapter, the limitations on compensation established by the Provider Namirial S.p.A. can be found in the contractual conditions for the supply of the service, made public and available at the website http://www.sicurezzapostale.it/richiesta-adesione.asp.

## 7.4 INSURANCE POLICY

Namirial S.p.A. has taken out an insurance policy covering the risks and the damage caused to third parties in the course of its activity as Certified Email Provider. The policy covers the risks arising from the activity and any damage caused to third parties, pursuant to Presidential Decree no. 68 of 11 February 2005, with a maximum limit of €7,500,000 (seven million five hundred thousand euros) per single unlawful act, per insurance year and for all financial losses arising from all claims for damages brought against all insured parties and for all insurance cover combined.

# 8 PERSONAL DATA PROTECTION(K)

The procedures and operating methods adopted by Namirial S.p.A., as controller of personal data, in carrying out its activity are described below. Personal information concerning the mailbox holders and, more generally, the customers of the service provided is processed, stored and protected in accordance with the provisions of [II] on the protection of personal data.

## 8.1 ORGANISATIONAL STRUCTURE OF NAMIRIAL S.P.A.

**Namirial S.p.A.** is the **Controller of personal data**, as provided for by [II] on the protection of personal data. The data protection officer, DPO, is Serena Donegani.
Namirial S.p.A. identifies and appoints the persons in charge of processing, who operate under the direct authority of the Controller or of the Processor, following the instructions they give.

## 8.2 PROTECTION AND RIGHTS OF DATA SUBJECTS

The Provider Namirial S.p.A. guarantees the protection of data subjects, in compliance with European Regulation 679/2016 (GDPR) on the processing of personal data. In particular, the provider gives data subjects all the necessary information regarding the right of access to personal data and the uses of such data permitted by law.
Data subjects may access their data, and exercise all the rights under arts. 15-22 of the GDPR, by written request, using the form that can be downloaded from the Namirial website ww.namirial.com .to be sent to the data protection officer, also by email to s.donegani.dpo@namirial.com who will process the request without undue delay. Data subjects must give written consent to the processing of their data by the Provider Namirial S.p.A.

## 8.3 PROCESSING METHODS

All personal information acquired during the provision of the PEC service is processed by the provider, which adopts the security measures described in this manual in order to prevent its loss, unlawful use or access by staff not expressly authorised. Data in electronic format are stored on dedicated data servers and on optical media inside protected cabinets. Data in paper format are stored by an external company called Archivi Service. These data are consulted on request, made exclusively by staff authorised by Namirial S.p.A. and after a specific request form has been sent to Archivi Service. Namirial S.p.A. reserves the option of keeping paper data at its head office, in paper archives to which only expressly authorised persons in charge have access.

## 8.4 PURPOSES OF PROCESSING

Personal data are acquired for the following purposes: (these purposes must be the same as those accepted in the privacy notice)

- provision of the certified email service;
- management of the contractual relationship;
- any checks on the quality of the service and on the security of the system;
- commercial activities, carried out by sending information on the launch of similar products and/or services or of products and/or services directly connected with the PEC service. The data subject may object to the processing of personal data for this type of communication.

The data collected are in no way used for profiling activities by Namirial S.p.A. and are not sold or provided to third parties for commercial or marketing purposes or for statistics and market research.

## 8.5 OTHER FORMS OF DATA USE

Personal data may be used for purposes other than the supply of PEC services and may be disclosed to public bodies, such as law enforcement agencies, public authorities and judicial authorities, if those bodies request them for reasons of public order and in compliance with the provisions of law on the security and defence of the State and the prevention, detection and/or prosecution of crimes.

## 8.6 DATA SECURITY

In compliance with current legislation, Namirial S.p.A. adopts all the security measures needed to minimise:

- the risks of destruction or loss, including accidental loss, of data;

- the risks of damage to the hardware resources on which the data are stored;
- the risks of damage to the premises in which the data are kept;
- unauthorised access to the data;
- processing activities not permitted by law or by company regulations

Through the security measures adopted by the provider, also attested by the certifications obtained in the 27001 scope with extension to the 27017 and 27018 standards (Cloud scope) (cf. § 6.3), the following features, among others, are guaranteed:

- the integrity and safeguarding of data against tampering or modification by unauthorised parties
- the availability of data and their consequent usability;
- the confidentiality of data, i.e. the guarantee that only authorised persons have access to the information.

# REFERENCES

| NUMBER | DESCRIPTION |
|---|---|
| [I] | Presidential Decree no. 445 of 28 December 2000 |
| [II] | REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) |
| [III] | Presidential Decree no. 68 of 11 February 2005. |
| [IV] | Legislative Decree no. 82 of 7 March 2005 “Digital Administration Code” (CAD). |
| [V] | Ministerial Decree of 2 November 2005 and subsequent supplementary notes, “Technical Rules for the service of transmitting electronic documents by Certified Email”. |
| [VI] | Circular CNIPA/CR/49 of 24/11/2005, “Procedures for submitting the application for accreditation in the public list of PEC Providers”. |
| [VII] | CNIPA Circular no. 51 of 7 December 2006: “Performance of supervision and control of the activities carried out by those entered in the list of certified email (PEC) providers referred to in art. 14 of Presidential Decree no. 68 of 11 February 2005. |
| [VIII] | CAD 30/12/2010 no. 235 - Amendments and additions to Legislative Decree no. 82 of 7 March 2005, laying down the Digital Administration Code, pursuant to article 33 of the law of 18 June |
| [IX] | Instructions for the retention of message logs and of certified email messages with viruses.<br>Version 1.0 of 05/07/2016 |
| [X] | DECREE OF THE PRESIDENT OF THE COUNCIL OF MINISTERS of 3 December 2013. Technical rules on retention systems pursuant to articles 20, paragraphs 3 and 5-bis, 23-ter, paragraph 4, 43, paragraphs 1 and 3, 44, 44-bis and 71, paragraph 1, of the Digital Administration Code referred to in Legislative Decree no. 82 of 2005. |
| [XI] | AgID - Instructions for the retention of message logs and of certified email messages with viruses – ver 1.0 of 05 July 2016 |

# INDEX OF TABLES

Table 1: definitions and Acronyms 8
Table 2: correspondence table between CNIPA/CR/56 and the Operating Manual 11
Table 3: Provider identification details 12
Table 4: certifications of the Provider 13
Table 5: service levels 27
Table 6: service quality indicators 28
Table 7: HSM security levels 32

# INDEX OF FIGURES

Figure 1: How the PEC system works 15
Figure 2: PEC mailbox activation flow 19

*This document is an English translation of the original Italian document and is provided for ease of reference. The translation may contain errors, omissions or inaccuracies. In the event of any discrepancy or inconsistency between this translation and the Italian original, the Italian original shall prevail to the extent permitted by applicable law.*