Certified Email (PEC) Service Operating Manual Document code: ICERT-PEC-MO

Version 2.20

CONTENTS

1. INTRODUCTION TO THE DOCUMENT 4
1.1 Changes introduced since the previous issue 4
1.2 Purpose and scope of the document 11
1.3 Regulatory and technical references 11
1.4 Definitions 12
1.5 Acronyms and abbreviations 14
2. GENERAL INFORMATION 16
2.1 Identification of the document 16
2.2 Provider identification data 16
2.2.1 Registration Offices 17
2.2.2 Responsibility for the Operating Manual, contact for end users and communications 17
2.2.3 Provider's website 17
2.3 Administration of the Operating Manual 17
2.3.1 Update procedures 17
2.3.2 Rules for publication and notification 18
2.3.3 Person responsible for approval 18
2.3.4 Compliance 18
2.4 Relations with AgID 18
2.5 Reference standards 18
2.5.1 Technological 18
2.5.2 Procedural 18
2.5.3 Security 18
3. INTRODUCTION TO THE PEC SERVICE 19
4. LEGALMAIL - INFOCERT'S PEC SERVICE 21
4.1 Standard features 21
4.1.1 Message processing 23
4.1.2 Retention of the information in the certified message log 25
4.1.3 Procedure for requesting information contained in the message log 26
4.2 Features in “closed” PEC mode 27
4.3 Features in “One shot” PEC mode 27
4.4 Additional features 27
4.4.1 System logs 28
4.4.2 Management of certified domains 28
4.4.3 Customisations 29
4.5 Self-management of mailboxes 30
4.6 Security of the InfoCert PEC system 30
4.6.1 Monitoring service 31
4.6.2 Data backup 31
4.6.3 Antivirus and anti-spam 31
4.6.4 Monitoring and management of suspicious access 32
4.6.5 Blocking of attachments with suspicious extensions 33
4.6.6 Access control dashboard 35
4.7 Offer arrangements 35
4.8 Activation of and access to the service 36
4.8.1 Service activation 37
4.8.2 Activation request for a mailbox purchased via the Legalmail website (www.legalmail.it) 37
4.8.3 Activation request for a mailbox purchased through an intermediary 38
4.8.4 Activation request through InfoCert sales staff 39
4.8.5 Alternative ways of activating the service 39
4.9 Changes to mailbox data made directly by the holder 39
4.10 Revocation of mailboxes 39
4.11 Password reset 40

InfoCert S.p.A. – all rights reserved

4.11.1 Password reset using additional security information 40
4.11.2 Password reset using a signed form 40
4.12 Access to the service 40
4.12.1 Access via Webmail 41
4.12.2 Access via client 42
4.12.3 General recommendations for users 42
4.12.4 Termination of the service 43
5. SERVICE REQUIREMENTS 44
5.1 Mailbox and message size 44
5.2 Conditions for the supply of the PEC service 44
5.3 Obligations and Responsibilities 44
5.3.1 Obligations of the Provider 44
5.4 Obligations of the Holders 45
5.4.1 Limitations and compensation 45
6. DATA PROTECTION 46
6.1 Applicable legislation 46
6.2 Security measures for the protection of personal data 46
7. ACCURACY OF THE TIME REFERENCE 47
7.1.1 Security of the time validation system 47
8. SERVICE LEVELS 48
8.1 Monitoring of the Provider's service level 48
8.2 Systems maintenance. 49
8.3 Security and quality checks 49
8.4 Data backup procedures 49
8.5 Emergency services 49
9. PROVIDER INTEROPERABILITY 51
10. SECURITY MEASURES 52
10.1 Description of the security measures 52
10.1.1 Physical security 52
10.1.2 Security of procedures 52
10.1.3 Logical security 52
10.2 Rules of conduct 53
10.3 Disaster Management Procedures 53
10.4 Functions to be restored and maximum restoration times 53

InfoCert S.p.A. – all rights reserved

1. Introduction to the document

1.1 Changes introduced since the previous issue

Version/Release no.:	2.20	**Version/Release date:**	12/11/2021
Description of changes:	1. Changed the conditions for revoking a mailbox described in §4.10 2. Change to the service activation conditions, §4.8.1		
Reason for changes:	Change to the mailbox activation and revocation conditions		

Version/Release no.:	2.19	**Version/Release date:**	08/09/2021
Description of changes:	1. Added clarification on the legal value of delivery receipts §3 2. Description of the new strong authentication feature for the webmail §4.12.1 3. Description of the types of login username §4.12 and following paragraphs 4. Removed password recovery via the security question/answer 5. Harmonised the terminology throughout the document for customers, holders, applicants and mailbox users		
Reason for changes:	New features and further details		

Version/Release no.:	2.18	**Version/Release date:**	20/04/2021
Description of changes:	1. Removed the references to the “Zucchetti” provider unit following its decommissioning		
Reasons:	Decommissioning of the “Zucchetti” provider unit		
Version/Release no.:	2.17	**Version/Release date:**	31/03/2021
Description of changes:	1. Added paragraph §4.6.6 “Access control dashboard” 2. Formatting correction		
Reasons:	Addition of a new security feature		
Version/Release no.:	2.16	**Version/Release date:**	11/11/2020
Description of changes:	1. Added paragraph §4.3 “Features in ‘One shot’ PEC mode” 2. Changed the minimum webmail access requirements in paragraph §4.12		
Reasons:	Addition of a new type of mailbox		

InfoCert S.p.A. – all rights reserved

Version/Release no.:	2.15	**Version/Release date:**	29/06/2020
Description of changes:	1. §4.5.5: added paragraph "Blocking of attachments with suspicious extensions"		
Reasons:	Blocking of file extensions for messages sent from webmail		
Version/Release no.:	2.14	**Version/Release date:**	07/05/2020
Description of changes:	1. §4.10: update of the contents and clarifications 2. §4.11: update of the operating systems and browsers supported 3. §4.5.3: update of the limits and operating procedures for countering credential theft and phishing 4. §5.1: updated the maximum number of recipients 5. Minor formatting corrections		
Reasons:	Periodic review of the contents of this Operating Manual.		
Version/Release no.:	2.13	**Version/Release date:**	29/11/2019
Description of changes:	1. §4.1.3: updated the details of the digital certificate used to sign the message logs. 2. §4.7.3: specified how the access credentials are set in the case of intermediaries 3. §4.5.4: added the paragraph 4. §7.2: specified that the use of TLS 1.2 is required 5. Minor formatting corrections		
Reasons:	Periodic review of the contents of this Operating Manual.		
Version/Release no.:	2.12	**Version/Release date:**	20/09/2018
Description of changes:	1. §7.1: updated the regulatory reference and the link to the privacy notice. 2. §2.2: updated the Milan operating office 3. §6.2.1 Updated the insurance cover limits 4. Removed the mention of the option to sign messages from the webmail 5. Minor formatting corrections		
Reasons:	Periodic review of the contents of this Operating Manual.		
Version/Release no.:	2.11	**Version/Release date:**	26/10/2016
Description of changes:	Various corrections of typing errors and of links pointing to the wrong destination.		
Reasons:	Periodic review of the contents of this Operating Manual.		
Version/Release no.:	2.10	**Version/Release date:**	22/06/2016

InfoCert S.p.A. – all rights reserved

Description of changes:	1. §2.2: updated the Padua operating office. 2. §4.5.3: removed the concept of suspected spam and its handling. 3. §4.1, §5.1: updated the maximum message sizes. 4. §5.1: removed the constraint on the product of message size and number of recipients. 5. §5.1: removed the cap on the number of recipients in To 6. §7.1: updated the link to the privacy notice.		
Reasons:	§2.2: change of address of the Padua operating office. §4.5.3: discontinuation of the handling of suspected spam. §4.1, §5.1: increase in the minimum limit required by AgID. §5.1: removal of the product constraint. §5.1: removal of the constraint on recipients in To. §7.1: new link to the privacy notice.		
Version/Release no.:	2.9	**Version/Release date**:	18/09/2015
Description of changes:	1. §1.4: corrected the definitions of Customer and Applicant; added the definition of User-id; 2. §4.1: corrected the recipient of the Legalmail features; 3. §4.1.1: changed the minimum service levels; 4. §4.9: specified that revocation requests are retained; 5. §4.10.1: corrected the owner of the additional security information and of the password; 6. §7.1: replaced the chapter with the link to the privacy notice pursuant to and for the purposes of Legislative Decree no. 196/2003, “Personal Data Protection Code”.		
Reasons:	§1.4, §4.1 and §4.10.1: review of the roles and responsibilities of Applicant, Holder and Mailbox User; §4.1.1: consistency with the evolution of the service; §4.9: alignment of procedures; §7.1: avoiding duplication of information.		
Version/Release no.:	2.8	**Version/Release date**:	26/08/2015
Description of changes:	1. §2.2: updated the Provider's identification data; 2. §2.2.2: updated the contact details of the person responsible for the Operating Manual; 3. §4: removed the encryption feature from the webmail; 4. §4: clarifications on how the additional services are used 5. §11.4: removed the location of the Disaster Recovery site.		

InfoCert S.p.A. – all rights reserved

Reasons:	§2.2: data update; §4: feature discontinued; §4: consistency with the current state of development of operating systems and browsers §11.4: keeping the location of the DR site generic.		
Version/Release no.:	2.7	**Version/Release date**:	13/05/2015
Description of changes:	1. §4.9: updated the link to the revocation form; 2. §4.10.2: updated the request procedure; 3. §4.11: added the URL and the hosts for access to the "Zucchetti" provider unit.		
Reasons:	§4.9 and §4.10.2: alignment of the information; §4.11: activation of the "Zucchetti" provider unit.		
Version/Release no.:	2.6	**Version/Release date**:	13/02/2015
Description of changes:	1. §1.4: added the definition of spam 2. §4.1: changed the minimum service levels 3. §4.1.3: changed how to request the information contained in the message log 4. §4.2: changed the description of the closed mailbox 5. §4.5.3: corrected the procedures for countering spam 6. §4.9: added the URL of the cancellation form and the details on the mailbox revocation notice 7. §4.11.2: specified the hosts and ports for secure connections		
Reasons:	AgID requirement of 08/10/2014. §4.1.3: update of the procedures.		
Version/Release no.:	2.5	**Version/Release date**:	01/09/2014
Description of changes:	1. §4.1: added a limit on the number of IMAP folders 2. §4.2: changed "exclusive mailbox" to "closed mailbox" 3. §4.3.1: access period for the statistical log extended from 2 to 3 months 4. §4.5.3: described the handling used to limit outgoing spam 5. §4.7.1: specified the SLA for activating a mailbox 6. §4.8: update of the data the user can change on their own 7. §4.9: specified the SLA for deactivating a mailbox		

InfoCert S.p.A. – all rights reserved

Reasons:	Points: • 1: typo in the previous version • 2: change of name • 3: SLA change • 4: new procedures for limiting outgoing spam • 5: information omitted in the previous version • 6: procedure update • 7: information omitted in the previous version		
Version/Release no.:	2.4	**Version/Release date**:	23/04/2014
Description of changes:	1. Various § updated: change of name and website from DigitPA to AgID 2. updated §4.1: functional limits for the standard mailbox, procedures for requesting information contained in the message log 3. removed §4.1.4: extraction of InfoCamere provider logs 4. updated §4.5: system security policies 5. updated §4.7.2: sending of the contract with online digital signature, payment by bank transfer 6. added §4.8: definition of how the holder can change the mailbox data directly 7. updated §4.9: revocation of mailboxes 8. updated §4.10: password reset		
Reasons:	Points: • 1: change of name from DigitPA to AgID • 2, 4, 5, 6, 7, 8: periodic review of the document • 3: discontinuation of the InfoCamere provider's logs		
Version/Release no.:	2.3	**Version/Release date**:	01/10/2010
Description of changes:	1. Table 2 § 2.2: change of legal representative 2. § 4.1 definition of functional limits for the standard mailbox 3. Change to § 1.2 4. §1.3: added reference [9] 5. §1.5: change of name from CNIPA to DigitPA 6. §2.2: change to table 2 7. Update of §2.5.3 8. update of chap. 4: use of the PEC system instead of the paper equivalent 9. §4.1 change to the standard features 10. § 4.3.1 and 4.3.2: changed the description of the statistical and system logs		

InfoCert S.p.A. – all rights reserved

	11. change to § 4.3.3 and added § 4.3.4 12. § 4.9: change to the password reset procedures 13. changes to §4.10 on how the service is accessed 14. change to § 4.10.1 15. change to the technical requirements in chap. 5 16. change to § 5.2 17. changes to § 7.1 18. deletion of § 9.4 on log retention 19. § 4.2: change to the description of the exclusive PEC mode		
Reasons:	Points: • 1: Change in the board of directors • 2,3,4,7,8,10,13,14,16,17,18: periodic review of the document • 4,10: change in the legislation on telephone and electronic traffic data • 5: change of name from CNIPA to DigitPA • 6,17: change of registered office • 9,11,12,13,15,19: update of the service features		
Version/Release no.:	2.2	**Version/Release date**:	20/10/2009
Description of changes:	1. §1.4, §4.1.3, §4.7.2, §4.9 Added the definition of identity document and specified the use of documents equivalent to it 2. §2.3.2 Changed the reference to the operating manual 3. Chap. 3 Update of the diagram and of the description 4. §4.5.1 Review of the information contained in the description of the monitoring service 5. §4.5.2 Update of the paragraph 6. §4.1 and §5.1 Updated the maximum message size to 50 MByte		
Reasons:	Points: • 1: specified that documents equivalent to the identity card may be used as identification documents, as provided by law • 2, 3: review and check of the Operating Manual • 4, 5: transfer of the PEC systems to a new area dedicated to InfoCert systems, with an update of the monitoring and storage/backup systems • 6: adjustment to customers' needs		
Version/Release no.:	2.1	**Version/Release date**:	16/10/2008
Description of changes:	Change to the call centre reference in paragraph		

InfoCert S.p.A. – all rights reserved

Reasons:	reference to the website www.legalmail.it used		
Version/Release no.:	2.0	**Version/Release date**:	24/06/2008
Description of changes:	1. Change to par. 2.3.1. Added a reference to the general terms and conditions of the contract concerning the validity of the versions of the Operating Manual. 2. Change to par. 4.1.3. Added the option for the holder to send requests for access to the message log information by fax as well as by PEC (if the holder no longer has the mailbox). 3. Insertion in paragraph 4.3.1 of the length of retention of the statistical log and of the system logs. 4. Change to 4.3.3 to make the operating aspects and the responsibilities in the management of custom domains clearer. 5. Change to par. 4.7 of the support email addresses. 6. Deleted the paragraphs “The systems used” and “The tools used” 7. Added par. 4.8 and 4.9. Providing users with information on the expiry/revocation of the mailbox and on password reset. 8. Change to paragraph 5.1 (maximum size of the message). The system allows a message with an attachment of up to 30 Mbyte to be sent/received (therefore an actual message size of 45 Mbyte, taking format conversions into account)		
Reasons:	Points 1, 2, 3, 4, 6,7. Review and check of the Operating Manual. Point 5. Change of the support email mailboxes. Point 8. Alignment with the CNIPA guidelines on the minimum message sizes.		
Version/Release no.:	1.1	**Version/Release date**:	18/02/2008
Description of changes:	Added paragraph 4.1.4 Changed the references to the call centre in par. 2.2.2		

InfoCert S.p.A. – all rights reserved

Reasons:	Addition of the procedure for accessing the message log information of the former provider InfoCamere S.c.p.A. Change of the call centre number.		
Version/Release no.:	1.0	**Version/Release date**:	18/07/2007
Description of changes:	None		
Reasons:	First issue		

1.2 Purpose and scope of the document

The purpose of this document is to describe the rules and operating procedures adopted by InfoCert in running the PEC service. Its content is based on the technical rules annexed to the Ministerial Decree of 2 November 2005 laying down the "Technical rules for the formation, transmission and validation, including time validation, of certified email" and on the CNIPA Circular on the procedures for submitting applications for entry in the public list of PEC Providers.

This manual is a detailed supplement to the privacy notice given to the holders of the service pursuant to Article 13 of Legislative Decree 196/03 and Article 13 of Regulation (EU) 679/2016.

The copyright in this document belongs to InfoCert S.p.A. All rights reserved.

1.3 Regulatory and technical references

Regulatory references

[1] Presidential Decree no. 137 of 7 April 2003 (Official Gazette no. 138 of 17 June 2003) and Article 13 of Regulation (EU) 679/2016

[2] Legislative Decree no. 82 of 7 March 2005 (in Official Gazette no. 112 of 16 May 2005 - Ordinary Supplement no. 93) - Digital Administration Code, as amended (hereinafter referred to as CAD)

[3] Presidential Decree no. 445 of 28 December 2000 (Official Gazette no. 42 of 20/2/2001), as amended by DPR 137/2003 (hereinafter referred to as TU)

[4] Prime Ministerial Decree of 13 January 2004 (Official Gazette no. 98 of 27/04/2004)

[5] Ministerial Decree of 2 November 2005 laying down the "Technical rules for the formation, transmission and validation, including time validation, of certified email" (Official Gazette no. 266 of 15/11/2005)

[6] Legislative Decree no. 196 of 30 June 2003 (Official Gazette no. 174 of 29 July 2003) laying down the "Personal Data Protection Code"

[7] CNIPA Circular no. CNIPA/CR/49 of 24 November 2005, "Procedures for submitting applications for entry in the public list of certified email (PEC) providers referred to in Article 14 of Presidential Decree no. 68 of 11 February 2005"

[8] Presidential Decree no. 68 of 11 February 2005, Regulation laying down provisions for the use of certified email, pursuant to Article 27 of Law no. 3 of 16 January 2003.

[9] Regulatory implementation on telephone and electronic traffic data - 24 July 2008 - Official Gazette no. 189 of 13 August 2008" issued by the Italian Data Protection Authority.

Technical references

[10] RFC 1847 (Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted)

[11] RFC 1891 (SMTP Service Extension for Delivery Status Notifications)

[12] RFC 1912 (Common DNS Operational and Configuration Errors)

[13] RFC 2252 (Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions)

[14] RFC 2315 (PKCS #7: Cryptographic Message Syntax Version 1.5)

[15] RFC 2633 (S/MIME Version 3 Message Specification)

[16] RFC 2660 (The Secure HyperText Transfer Protocol)

[17] RFC 2821 (Simple Mail Transfer Protocol)

[18] RFC 2822 (Internet Message Format)

[19] RFC 2849 (The LDAP Data Interchange Format (LDIF) - Technical Specification)

[20] RFC 3174 (US Secure Hash Algorithm 1 – SHA1)

[21] RFC 3207 (SMTP Service Extension for Secure SMTP over Transport Layer Security)

[22] RFC 3280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List - CRL Profile)

[23] Information Technology – Open Systems Interconnection – The Directory: Authentication Framework; ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8

1.4 Definitions

The definitions used in drafting this document are listed below. For the terms defined in the legislation referred to above, reference is made to the definitions laid down therein. Where appropriate, the corresponding English term, generally used in publications, standards and technical documents, is given in curly brackets.

Time-stamping authority {*Time-stamping authority*}
the software/hardware system, managed by an accredited Certifier, that provides the time-stamping service.

Non-delivery notice – [5]

Non-acceptance notice – [5]

Anomaly envelope – [5]

Transport envelope – [5]

PEC mailbox – [5]

Customer
coincides with the definition of **Holder**

Contract

InfoCert S.p.A. – all rights reserved

the contract for the activation of the Legalmail PEC service, consisting of the Activation Request, the General Terms and Conditions and the documents referred to therein, which together govern the relationship between the parties;

Certification data – [5]

Recipient – [8]

PEC domain – [5]

Electronic signature – [TU]

Qualified electronic signature – [TU]

Digital signature {*digital signature*} – [TU]

CAD – Digital Administration Code
Legislative Decree no. 82 of 7 March 2005 (in Official Gazette no. 112 of 16 May 2005 - Suppl. no. 93)

Certified email provider (PEC Provider) – [5]

Index of PEC Providers – [5]

Message log – [8]

Time stamp – [4]

PEC message – [8]

Original message – [5]

Email – [8]

Certified email – [8]

Access point – [5]

Delivery point – [5]

Incoming point – [5]

Technical rules
Annex to the Ministerial Decree of 2 November 2005 [5], laying down the technical standards for the processing of PEC messages.

Short delivery receipt – [5]

Full delivery receipt – [5]

Acceptance receipt – [5]

Delivery receipt – [5]

Take-charge receipt – [5]

Summary delivery receipt – [5]

Applicant
The natural person who requests the activation of the Legalmail PEC Service on behalf of the customer/holder identified on the basis of the information given in the Activation Request

Activation Request

InfoCert S.p.A. – all rights reserved

the Customer's proposal requesting the activation of the Legalmail PEC Service;

Time reference – [8]

Legalmail Service
the service under which InfoCert assigns to the Customer one or more Legalmail PEC mailboxes that comply with the features specified in the Technical Annex to the Ministerial Decree [5].

Spam
communications for sending advertising or direct sales material or for carrying out market research or commercial communication (see Articles 7, paragraph 4, letter b), 130, paragraph 1 and 140 of the Personal Data Protection Code - Legislative Decree no. 196 of 30 June 2003)

Holder

The party, including a business, holding InfoCert PEC mailbox(es) under Ministerial Decree 2.11.2005

User-id

identifier of the Mailbox User that can be used, together with the password, as an authentication credential; a distinction is made between:

- "user-id master": identifier issued at the time of activation, which has full control of the mailbox;
- "user-id slave": secondary identifier that can send from and access the mailbox but cannot change its configuration.

User

coincides with the **Mailbox User**

Computer virus – [8]

Coordinated Universal Time {*Coordinated Universal Time*}
Time scale with a precision of one second as defined in ITU-R Recommendation TF.460-5

Registration Office
Body appointed by the Provider to carry out the activities required for the Provider to issue PEC mailboxes.

Mailbox User
coincides with the definition of **User**: the person to whom the Customer assigns the use of the Legalmail PEC mailbox;

Identity document
Valid identity card or equivalent document (see Article 35, paragraph 2 of the TU).

1.5 Acronyms and abbreviations

AgID - Agency for Digital Italy: established by Decree-Law no. 83, converted into Law no. 134/2012. It inherits the responsibilities of the Department for Digitalisation and Innovation of the Presidency of the Council of Ministers, of the Agency for the Dissemination of Technologies for Innovation, of DigitPA and of the Higher Institute of Communications and Information Technologies as regards network security.

InfoCert S.p.A. – all rights reserved

CNIPA – National Centre for Information Technology in Public Administration – from 29 December 2009, pursuant to Article 2, paragraph 1 of Legislative Decree 177/2009, the National Centre for Information Technology in Public Administration (CNIPA) takes the name: "DigitPA"

DPCM - Prime Ministerial Decree
This refers to the DPCM of 13 January 2004 laying down the "Technical rules for the formation, transmission, storage, duplication, reproduction and validation, including time validation, of documents".

IETF - Internet Engineering Task Force
The IETF is an open international community of network designers, operators, vendors and researchers involved in the evolution of the Internet architecture and the smooth operation of the Internet.

ISO - International Organization for Standardization
Founded in 1946, ISO is an international organisation made up of national standards bodies.

ITU - International Telecommunication Union
Intergovernmental body through which public and private organisations develop telecommunications. The ITU was founded in 1865 and became the regulatory body for telecommunications standards.

LDAP – Lightweight Directory Access Protocol
Protocol used to access the register of Providers.

MX - Mail eXchange record
Entry in a "domain name database that identifies the mail server responsible for handling email for that domain.

DNS - Domain Name System
It is the domain lookup service. It is a program that can translate the mnemonic names used by users to identify a site into the corresponding IP addresses

IP address
Numerical address that identifies the computers connected to the network.

PEC – Certified Email

TSA – Time Stamping Authority

TU – Consolidated Act
This refers to Presidential Decree no. 445/2000, as amended, *"Consolidated Act on legislative and regulatory provisions on administrative documentation"*.

InfoCert S.p.A. – all rights reserved

2. General information

The increasingly frequent use of email in place of traditional means (post, fax, courier) creates the need for reliable, secure systems capable of providing the guarantees required by the rules on administrative documentation. Over recent years, a body of laws and regulations has defined the technical and organisational features needed to give email messages the same legal value as traditional forms of communication.

This Operating Manual provides users with the information they need to assess InfoCert's offer as Provider of a PEC system, and describes how to access the service.

2.1 Identification of the document

This document is called “Operating Manual” and is identified by the document code:
ICERT-PEC-MO
The version and release level can be identified at the foot of each page.

2.2 Provider identification data

InfoCert S.p.A. is the **PEC Provider** (pursuant to the Ministerial Decree of 2 November 2005 [5]) that manages one or more PEC domains, operating in compliance with the Technical Rules and as prescribed by the Consolidated Act, the CAD and DPR 68/2005 [8]. In this document the term Provider is used to refer to InfoCert.

The full details of the organisation acting as Provider are as follows:

Table 2

Company name	**InfoCert S.p.A. - Company subject to management and coordination by Tinexta S.p.A.**
Registered office	**Piazza Sallustio n. 9 - 00187 Roma**
Legal representative	**Daniele Vaccarino** As Chairman of the Board of Directors
Administrative Office	**Via Marco e Marcelliano 45, 00147 Roma**
Companies Register Registration No.	**Tax code and registration number: 07945211006** in the Companies Register of ROMA Registration date: 09/04/2004
VAT no.	**07945211006**
Website	http://www.infocert.it http://www.legalmail.it/
Operating offices	• Via Marco e Marcelliano 45, 00147 Roma • Piazza Luigi da Porto 3, 35131 Padova • Via Carlo Bo 11, 20143 Milano

InfoCert S.p.A. – all rights reserved

2.2.1 Registration Offices

PEC mailboxes are marketed by InfoCert both through its direct sales network and through partners.

2.2.2 Responsibility for the Operating Manual, contact for end users and communications

InfoCert is responsible for drawing up, publishing and updating this document.

Questions, comments and requests for clarification concerning this Operating Manual should be addressed to the following person and address:

InfoCert S.p.A.
PEC Service Manager
Piazza Luigi da Porto 3
35131 Padova

Call Centre: the contact details of the Legalmail Call Centre are available at the page
http://help.infocert.it/
Web: http://www.legalmail.it
email: infocert@legalmail.it

2.2.3 Provider's website

Information on the PEC services offered by InfoCert can be consulted online on the website **http://www.legalmail.it**

2.3 Administration of the Operating Manual

2.3.1 Update procedures

The Provider reserves the right to make changes to this document for technical requirements or for changes to procedures resulting from laws or regulations or from optimisation of the work cycle. Each new version of the Operating Manual cancels and replaces the previous versions, as provided for in the general terms and conditions of contract.

Changes that have no significant impact on users increase the release number of the document, while changes with a significant impact on users (such as major changes to the operating procedures) increase the version number of the document. In any case, the manual will be promptly published and made available in the manner provided for.

At intervals of no more than one year, the Provider checks that this Operating Manual complies with its own process for delivering the PEC service.

Any change to the operating manual will be submitted to AgID before the provider publishes it on the website.

InfoCert S.p.A. – all rights reserved

2.3.2 Rules for publication and notification

This document is published in electronic format on the Provider's website at:
http://www.legalmail.it/manualeoperativo.pdf

2.3.3 Person responsible for approval

This Operating Manual is verified by the Service Manager.

2.3.4 Compliance

The contents of this Operating Manual fully comply with the PEC legislation, with particular reference to the technical rules described in the Presidential Decree [8] and the Ministerial Decree [5] and to the specifications of the CNIPA Circular [7].

2.4 Relations with AgID

This Operating Manual, drawn up by the Provider in accordance with the legal requirements, has been delivered in copy to AgID.

2.5 Reference standards

2.5.1 Technological

For the technological standards, reference has been made to the list of specifications issued by the IETF (RFC) cited in the references.

2.5.2 Procedural

All the Provider's operating processes described in this Operating Manual, like every other activity of the Provider, are carried out in accordance with the company Quality Plan, in compliance with the ISO9001 standard.

2.5.3 Security

To ensure the security of the PEC service, InfoCert uses techniques and procedures based on international (*de jure* or *de facto*) standards and on the specific rules in force in Italy.

The procedures have been drawn up and fine-tuned on the basis of the following standards:

- Information Technology Security Evaluation Criteria (ITSEC) v. 1.2
- Common Criteria for Information Technology Security Evaluation v 2.2
- ISO/IEC 17799 - Information technology -- Security techniques -- Code of practice for information security management
- UNI CEI ISO/IEC 27001:06 – Information Technology – Security Techniques – Information security management systems – Requirements.
- ISO IEC 27002:05 – Information Technology – Security Techniques – Code of practice for Information Security Management

The cryptographic devices used are FIPS 140-2 level 3 certified.

InfoCert S.p.A. – all rights reserved

3. Introduction to the PEC service

The following diagram gives a schematic illustration of the PEC service. This short description is not intended to be an exhaustive technical description of the service, but to introduce the Mailbox User simply and intuitively to the specific features of the PEC service.
All the aspects of the service are examined in detail later in this document, as required by the legislation laid down in the Ministerial Decree [5].

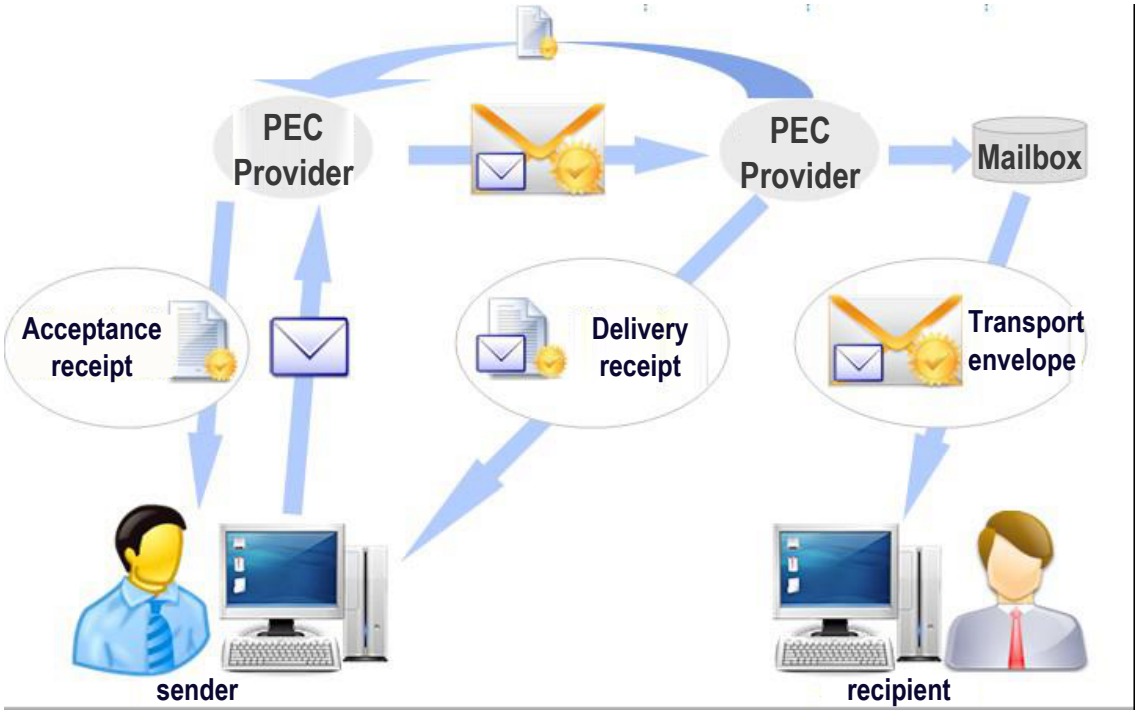


Figure 1

After passing the authentication phase in which the system validates their credentials, the 'sender' Mailbox User can send a message.

The message (the white envelope in figure 1) reaches the system of the sender's provider, where it is analysed to check that it complies with the PEC rules and, if it does, it is enclosed in another message, in turn signed by the mail provider, and forwarded to its destination.

In this case the sender receives the *acceptance receipt* signed by their provider and thus has proof that their message has been correctly accepted by the system.

If the provider cannot accept the message, the sender will receive a notice ('*non-acceptance notice*') giving the reason why the system did not accept it.

The figure shows the case in which sender and recipient belong to domains managed by different providers, so the message must pass from domain A to domain B.

The recipient's provider (domain B) notifies the sender's provider (domain A), with the *take-charge receipt*, that it has successfully taken charge of the message.

The transit of the message is thus tracked, so that the sender can always be informed of the route taken by their message.

InfoCert S.p.A. – all rights reserved

The mail provider of domain B places the message in the recipient's mailbox and notifies the sender that the operation was successful by means of the *delivery receipt*, which also contains the original message as an attachment, unless the sender requests otherwise.

The message is now available to the recipient, who can read it at their discretion.

In total the sender will receive at least 2 receipts for each message sent: an '*acceptance receipt*' and a *delivery receipt*.

If the sender sends a message to several recipients in a single transmission, they will receive a *delivery receipt* for each PEC recipient, so the total number of receipts will normally be equal to the number of recipients +1 (*acceptance receipt*).

If particular events occur (virus detection, incorrect recipients, ...), other notifications may be received.

The issue of the delivery receipt does not depend on whether or not the recipient opens the message, and the receipt is issued in any case when the message is placed in the mailbox; this is one of the distinctive features of the PEC system.

For the sender, the delivery receipt has legal value and can be relied upon against third parties, in whatever mail folder or other digital medium it is kept, provided that its integrity can be verified by checking its signature.

If the delivery receipt is not received within 24 hours, the message is deemed not to have been delivered. In that event, we advise the sender to send the message again.

Notifications from ordinary mail systems are in fact linked to the opening of the message and to the recipient's willingness to send the notification of receipt to the sender: however, a notification of this type does not have the legal value, enforceable against third parties, of the receipts issued and signed by accredited providers.

InfoCert S.p.A. – all rights reserved

4. Legalmail - InfoCert's PEC service

The PEC service, which guarantees a high degree of reliability and security, is provided by InfoCert under the name Legalmail. It allows the Customer to have PEC mailboxes, which make it possible to communicate with other mailboxes of the same type over the worldwide Internet.
The service also makes it possible to send, receive and consult ordinary email messages.
The use of PEC mailboxes guarantees the customer secure access to their own mailbox, either through a mail client (Thunderbird, Outlook Express, ...) or directly from the Internet using the most common browsers (the service is called Webmail).
The service includes the delivery to the customer's mailbox of the various types of receipts described in the previous chapter.

Unlike the usual email mailboxes, certified email mailboxes allow email to be sent with legal value in accordance with the provisions of the legislation on Certified Email.

Legalmail fully complies with the technical rules referred to in the Ministerial Decree [5] and published by AgID on the website http://www.agid.gov.it/ ; the features of these mailboxes therefore make them interoperable with the PEC mailboxes distributed by other accredited PEC providers.

Where permitted by law, certified email can be used instead of paper mail. Messages received in the certified mailbox are deemed to have **reached** the mailbox holder.

Please note that the possibility of using the PEC system instead of its paper equivalents is subject to the specific legislation and that, between private parties, a prior declaration by the recipient of their willingness to use PEC is currently required.

4.1 Standard features

The most important features of the service, in compliance with the official legislation, are:

- sending to the sender of an acceptance receipt for each outgoing message that complies with the regulatory requirements.
- insertion of the messages leaving the sender's mailbox into a so-called “transport” envelope signed by the Provider. The transport envelope is delivered unchanged to the destination mailbox.
- issue of a delivery receipt for each recipient to whom the message has been delivered, if the message is sent to a PEC mailbox with legal value (as provided for by AgID)

- insertion of incoming messages that do not come from PEC mailboxes into an “anomaly” envelope
- the electronic signature of the PEC service Provider on the receipts and on the transport envelope, which always contain information relating to the message (time, from,

InfoCert S.p.A. – all rights reserved

to, etc.) both in human-readable text format and in XML format
- alignment of the time of the receipts and of the transport message with Coordinated Universal Time (UTC), to within one second
- sending of the entire original message as an attachment to the delivery receipt sent to the sender (as proof of what was sent and delivered) for each recipient in "TO", unless the sender requests otherwise
- retention of a log of the main events; the system keeps track of the operations carried out, recording in a log the significant data of the operation: the unique identification code of the message (Message-ID), the date and time of the event, the sender of the original message, the subject of the message, etc.;
  the system keeps no information that would allow the content of the message to be traced after the Mailbox User has downloaded and deleted the message from the server, unless there are specific legal provisions or an explicit request from the customer (through subscription to additional services).
- prohibition on the use of hidden recipients (BCC or CCN)
- requirement of at least one recipient in "TO".
- take-charge receipt between different mail providers of the circuit (not visible to users, but essential for tracking the complete route taken by the message)

The above features will be subject to all the changes required if the legislation and the provisions issued by AgID evolve.

InfoCert accepts no responsibility for the correct handling of messages by other PEC providers.

InfoCert enables the Holder to use the features listed through the Legalmail service, which therefore includes:
- issue of the PEC mailbox and of the related user-id for access
- assignment of a password, and reassignment and change on request
- access to the mailbox from a mail client
- sending of messages with a mail client
- access to the mailbox and sending of messages with webmail
- option to sign and encrypt messages through mail clients (using signature devices and certificates issued both by InfoCert and by other Certification Bodies)
- option to save messages from webmail
- use of the Legalmail website (www.legalmail.it) with support information
- call centre for information support
- an up-to-date antivirus that checks incoming and outgoing documents and messages.

The Legalmail service guarantees:
- a certified email mailbox size of no less than 1 GB;
- a maximum message size of 100 MB;
- the option to define internal subfolders, each of which can contain up to 5,000 messages;

- up to 50,000 messages in total in the mailbox;
- up to a total of 500 folders/subfolders in the mailbox.

InfoCert S.p.A. – all rights reserved

The Provider reserves the right to block access to the service if the above limits are exceeded or if situations arise that could compromise the security of the mailbox or of the service, as indicated in § 4.5.

Any specific requirements will be met through a contractual agreement which, starting from the listed features guaranteed to all users, may offer additional services and/or volumes.

The InfoCert PEC service complies with the technical and organisational rules set out in the reference legislation, namely:

- Presidential Decree no. 68 of 11 February 2005, "Regulation laying down provisions for the use of certified email";
- Ministerial Decree of 2/11/2005 laying down the "Technical rules for the formation, transmission and validation, including time validation, of certified email"
- Technical Annex to the Ministerial Decree indicated in the previous point, "Technical rules for the service for transmitting electronic documents by certified email"

InfoCert also undertakes to adapt the service promptly to any changes in the legislation.

4.1.1 Message processing

The system ensures compliance with all the rules laid down for PEC by the reference documents [8] and [5], in particular the rules on the processing and exchange of messages between PEC mailboxes listed below:

1. **the acceptance receipt and the transport envelope, for sending**

Through the acceptance receipt, the PEC system notifies the successful sending of a message, achieved when it passes all the formal and content checks (for example, the message is checked for computer viruses), and makes it compliant with the system by 'enveloping' it in the transport envelope.

2. **non-acceptance notices for formal exceptions and for computer viruses**;

The PEC system notifies the non-acceptance of the message and the reason why it was rejected (formal error, virus in the message sent).
One reason for the non-acceptance of a message due to a formal error is, for example, a breach of the PEC rule that does not allow an email address other than that of the sender's own mailbox, i.e. the one corresponding to the credentials used to access the service, to be used in the "From" field. There must also be consistency between the from used at SMTP protocol level and the from given inside the mail message.

3. **take-charge receipts;**

the PEC systems of the circuit notify each other that they have taken charge of a message passing between different domains, in order to track the route of the message completely; these receipts do not reach the sender, but only the service providers.

InfoCert S.p.A. – all rights reserved

4. **The full delivery receipt**

The sender's mailbox receives from the PEC system a notification message that the message sent has been received in the recipient's PEC mailbox. In the usual case, the system sends a full receipt with the certification data and the original message attached for the direct recipients in 'to'.

5. **The short delivery receipt:**

At the request of the mailbox user, instead of the full receipt, the system sends a short receipt with the certification data and an extract of the original message attached.
In this case it is essential that the mailbox user keeps the original message if they consider it necessary to prove not only the sending and the delivery of the message to the recipient's mailbox, but also the content of the message itself.
The extract of the message cannot in fact be read on its own, but can be associated by IT tools (hash functions) only with the message that generated it, thus making it enforceable against third parties.
If the original message is not available or has been altered even slightly, it can no longer be relied upon against third parties.

6. **The summary delivery receipt:**

For PEC recipients in copy 'Cc', notification is given by means of a summary receipt with only the certification data attached.
The summary receipt can also be requested for recipients in TO; in this case, however, the certification of the content of the message is lost and only the certification of the subject / date and time / sender / recipient remains.
The reason for not attaching the full original message to every type of receipt is to save space in the sender's mailbox, avoiding filling it with potentially very large messages that, in the case of multiple sendings, are redundant.

7. **The anomaly envelope for messages coming from non-certified mailboxes:**

When a non-PEC message is delivered to a PEC mailbox, it is placed in an anomaly envelope to highlight the event, so that the recipient can easily distinguish certified messages from the others. The anomaly is normally due to the fact that the email message comes from a sender outside the PEC circuit

8. **The computer virus detection notice:**

The PEC service also aims to guarantee, more effectively than ordinary mail systems, security against the receipt and spread of computer viruses.
The Provider checks incoming PEC messages coming from other providers to verify that they are virus-free. Messages that contain computer viruses are not forwarded to the recipient, and the Provider generates a virus detection notice to be returned to the sender's provider, using as the address the one specified for receipts in the Index of PEC Providers, and indicating the error found. This message is not forwarded to the recipient, but is used by the sender's provider to notify its sender that the message could not be delivered.

InfoCert S.p.A. – all rights reserved

9. Non-delivery notices, in the cases provided for:
The sender is always notified of the outcome of sending a message. If the message cannot be delivered, the sender will receive from the recipient's provider a **non-delivery notice** giving the reason why the system could not place the message in the destination mailbox. Some error cases, such as an incorrect address or the notice that the destination mailbox does not have enough space to hold the message, give the sender useful indications on the action to take in order to send the message correctly.
If the recipient's provider does not notify that it has "taken charge" of the message within 12 hours of its sending, the sender receives from its own provider a "non-delivery notice for exceeding the maximum time limits", i.e. a notification warning of a possible delivery failure. If the recipient's provider does not notify "delivery" within the 24 hours following the sending, the sender receives from its own provider a "non-delivery notice".

10. The generation of all the xml files required by the legislation:
These files contain data describing the message (date and time of sending, sender, recipient, subject, message identifier etc.) and are used by PEC systems for automatic processing.

11. The insertion of the time reference in all the required messages/logs:
A time reference is inserted in all the required messages / logs. The time reference used has an error of less than one second with respect to Coordinated Universal Time (UTC).

12. Retention for 30 months of the logs of the main events concerning messages in transit:
The legislation requires the following information to be recorded in the certified log:

- the unique identification code assigned to the original message
- the date and time of the event
- the sender of the original message
- the recipients of the original message
- the subject of the original message
- the type of event (acceptance, reception, delivery, receipts, error, etc.)
- the identification code of the related messages generated (receipts, errors, etc.)
- the sender's provider

The availability of this information at all PEC providers guarantees the holder the possibility of obtaining, within 30 months of sending, the elements, enforceable against third parties, relating to the sending, the route of the message and the outcome of the sending.

4.1.2 Retention of the information in the certified message log

The *certified log* is a file in which the operations carried out by the PEC system are recorded.
The PEC technical rules define the format and the information to be kept in the certified log (message log referred to in the Ministerial Decree [5], Article 10 and par. 6.2 of its technical annex).

InfoCert guarantees the content of the log file with:

- electronic signature and (daily) time stamping of the certified log file by the PEC

InfoCert S.p.A. – all rights reserved

system;

- daily sending of the time-stamped and signed log files to the InfoCert storage system for the preservation of electronic documents, in compliance with the technical rules contained in CNIPA Resolution no. 11/2004. The legally compliant storage system provides for:
  - substitute storage, by electronic transmission, of a suitably digitised analogue document or of an electronic document;
  - the electronic production of a document already held in substitute storage;
  - responsibility for the procedure, which also involves affixing the time stamp and the procedure control signature, using digital signature and digital time-stamping technologies;
  - the storage on optical media at InfoCert of a copy of all the documents sent for storage;

It is possible to request to view the information contained in the certified log.

Subject to the restrictions arising from the need to guarantee the protection of users' personal data, reports extracted from the certified log containing information on the transit of messages within the PEC system may be provided.

To access the information contained in the certified log, the mailbox user must follow the procedure described in the next section.

4.1.3 Procedure for requesting information contained in the message log

The mailbox Holder must send to the address servizio_legalmail@legalmail.it, from their own PEC mailbox, a request for information contained in the message log, specifying the information they need.

The request must be worded as follows:

I hereby request from the support team of InfoCert's "Legalmail" PEC service the information on the sending/receipt of the messages identified by the following details:

- *time period* (mandatory, not earlier than 30 months);
- *sender* (optional; if specified, this means all the messages sent by that sender to the applicant's mailbox);
- *recipient* (optional; if specified, this means all the messages sent from the applicant's mailbox to that recipient)
- *only the messages sent by the applicant / only the messages received by the applicant / both the messages sent and the messages received by the applicant*.

Legalmail support sends the information requested by the Mailbox User to the same mailbox used to send the requests. The information extracted from the logs will be sent in CSV (comma separated values) format, signed in P7M format with an automatic signature certificate issued in the name of the Legalmail Service Manager. The information released may be used by the Mailbox User for the purposes permitted by law.
The log information service is chargeable unless otherwise agreed with the Customer.

InfoCert S.p.A. – all rights reserved

4.2 Features in “closed” PEC mode

For particular types of mailbox it will be possible to activate the mailbox in “closed PEC” mode. In this mode the mailbox only accepts incoming PEC messages (sent from other PEC mailboxes). Traditional email messages will therefore be rejected by the system.

Activation of this mode will be reserved:

- for some contractual types of mailbox, as their standard and only mode;
- for other types of mailbox, at the request of the Mailbox Users (configuration via webmail).

4.3 Features in “One shot” PEC mode

For particular types of mailbox it is possible to activate the mailbox in “One shot” mode.

In this context, the mailbox is assigned to the Mailbox User by the Provider, under an agreement with InfoCert's partner (if any). That partner identifies the relevant Mailbox User, guarantees their key and contact data, and provides InfoCert with appropriate evidence that the process is correct.

“One shot” PEC has the following specific features:

- The mailbox can only be activated through a specific activation process of the Partner, verified however by InfoCert, on a predefined domain
- The mailbox only accepts one incoming PEC message, sent from a predefined PEC mailbox
- Sending is disabled
- The PEC address is not known to the Mailbox User
- The mailbox cannot be revoked
- Access to the mailbox is only allowed through a webapp, following authentication, defined in accordance with the relevant contract
- Access to the mailbox is limited in time, for a period that varies according to the relevant contract
- To request the certified log, unlike what is provided for in paragraph *4.3.1 “Procedure for requesting information contained in the message log”*, the request for this type of mailbox must contain: an indication that it concerns a OneShot PEC, its date of receipt and the tax code of the data subject.

4.4 Additional features

Further features have also been added to the service to make the use of PEC easier and more understandable for the Mailbox User.

The main ones are:

- additional text, beyond the minimum required by the technical rules, is inserted in the transport and anomaly envelopes and in the receipts, with the aim of helping users to interpret the

InfoCert S.p.A. – all rights reserved

meaning of what they are receiving

- the additional text of the acceptance receipts includes the original identifier of the message sent by the sender. Under the PEC rules, this identifier must be overwritten by a new identifier, applied by the PEC server to guarantee the uniqueness of the identifier of the original messages accepted across the whole certified mail infrastructure and to allow the correct tracking of the messages and of the related receipts

- If the email client communicating with the access point has already inserted a Message ID in the original message to be sent, this must be replaced with the identifier described above. To allow the sender to associate the message sent with the corresponding receipts, the original Message ID, if any, will be available in the receipts and in the transport envelope and reported in the Certification data [**5**].

- in webmail (if activation of the service is requested), special features have been added to make it easier to read PEC messages (which arrive "enveloped"), to prevent the sending of messages that would then be rejected under the PEC rules (without "TO", with "CCN"/"BCC") and to check the validity of the signatures of the PEC providers.

4.4.1 System logs

The services and products that form part of the architecture of the PEC system and are involved in providing the service record information on the traffic of messages in transit, to allow checks on the status of the service or on any malfunctions.

The information in the system log registers is kept by the provider for a maximum period of six months in compliance with the "Regulatory implementation on telephone and electronic traffic data - 24 July 2008 - Official Gazette no. 189 of 13 August 2008" issued by the Italian Data Protection Authority.

4.4.2 Management of certified domains

InfoCert offers the option to define/customise other domains or subdomains for PEC mailboxes. It is also possible to use subdomains within domains already used for non-certified mailboxes (the new certified subdomain will be managed by the InfoCert systems).

The Customer can request the use of mail domains other than the standard legalmail.it ones.

Different domains can be used in different ways:

- customisation of a subdomain within those available to InfoCert
- customisation of the Customer's own subdomain

The subdomain within InfoCert will be configured as a second-level domain of the type

InfoCert S.p.A. – all rights reserved

<COMPANY_NAME>.legalmail.it; the addresses will therefore be of the type <MAILBOX>@<COMPANY_NAME>.legalmail.it (for example, mario.rossi@acme.legalmail.it). <COMPANY_NAME> is a name that will be proposed by the Customer but decided at the discretion of InfoCert, which reserves the right to reject the proposals made, as provided for in paragraph 4.7.1. below of this Operating Manual.

On the other hand, customising the Customer's own subdomain will consist in configuring a domain of the type <SUBDOMAIN>.<DOMAIN>.it (where <DOMAIN>.it is an existing domain managed by the Customer); the addresses will therefore be of the type <MAILBOX>@<SUBDOMAIN>.<DOMAIN>.it (for example, mario.rossi@cert.acme.it). <SUBDOMAIN> is a name defined by the customer and used as a subdomain of the main domain.
In this case the Customer will be responsible for ensuring that the DNS servers of the manager of the COMPANY_NAME.it domain are suitably configured, so that the email of the subdomain is routed to the Legalmail servers.

The Customer is responsible for maintaining the correct DNS configuration of the domains.
InfoCert will remove from the index of certified domains any domains that, after verification, are found not to be configured correctly.
Whenever the MX records are changed, have an anomaly or are restored, the Customer must notify the provider of the event (using the mailbox servizio_legalmail@legalmail.it).
If no such notice is given, the proper performance of the service cannot be guaranteed.

Please note that, under the PEC rules, the domains/subdomains used cannot also be used for non-certified mailboxes.

InfoCert will add the domains used to the index of PEC providers. This index must in fact contain, among other things, the list of all the PEC domains managed by each operator.

4.4.3 Customisations

Legalmail provides some further features, offered separately, that allow the way Legalmail mailboxes are accessed to be customised.

The elements that can be changed concern:

- webmail interface access url. The Customer or intermediary can request the activation of a customised web access, such as “https://webmail.nomeimpresa.it” or “https://pec.sitoordine.it”, through which their users can access the webmail interface.

- Address of the SMTP, IMAP and POP3 services, to customise configuration via client. The customer or intermediary can request the activation of customised SMTP/IMAP/POP3 services, such as “smtp.pec.nomeimpresa.it” or “imap.pec.sitoordine.it”, to customise the configuration of client access to their mailboxes.

- graphic customisation of the webmail interface. Graphic customisation of Webmail consists in the possibility of changing some graphic elements for users of a domain other

InfoCert S.p.A. – all rights reserved

than the standard ones (see par. 4.3.3), or for access via customised url (see point 1). The elements that can be changed are: the images (banners) at the top of the pages; the colours of many of the page elements

The customer is responsible for maintaining the correct DNS configuration of the customised urls requested (points 1 and 2), where the domain used is not under the direct responsibility of InfoCert.

Access via customised services in any case guarantees the use of secure protocols (HTTPS for Webmail access, SMTPS or SMTP STARTTLS for sending from a client, IMAPS or POP3S for accessing and consulting the mailbox).

InfoCert reserves the right to refuse the activation of services or the inclusion of materials that could cause problems in the use of the service (for example colour combinations without contrast that make some wording difficult to read, or images whose size is not compatible with the structure of the webmail pages), as well as the activation of services or the inclusion of materials that could cause offence or constitute breaches of the law, it being understood that, except in cases of wilful misconduct or gross negligence, InfoCert accepts no responsibility for checking the elements supplied by the Customer or the Customer's right to use them.

These optional Legalmail services do not include the development of new graphic elements or new solutions, but are limited to applying what is received from the customer.

4.5 Self-management of mailboxes

Mailbox self-management is the web service provided by InfoCert that allows some selected Customers and Resellers to manage and update their own Legalmail mailboxes independently

InfoCert reserves the right not to provide this optional service. Some non-exhaustive examples of reasons why self-management may be refused or revoked are:

- the Customer requests the setting up of a very small number of mailboxes;
- the Customer or Reseller does not provide the necessary guarantees of reliability and security.

4.6 Security of the InfoCert PEC system

InfoCert continuously updates and supplements its security systems.

Certified email systems aim to guarantee:

- the security of the system through duplicated systems and firewalls
- secure access based on sending a protected password and/or access via digital certificates on signature devices
- the security of the message, with protected communication (with the customer and with the other providers), support for signature and encryption from signature devices, and antivirus checks on all mail in transit
- the sending of PEC messages in compliance with the legislation, which requires specific acceptance and delivery receipts to be sent.

InfoCert S.p.A. – all rights reserved

To build the PEC system, mailing tools and application components for checking the message and sending the specific receipts have been integrated.

The Provider reserves the right to take action on mailboxes and on access to the service where situations arise that could compromise the security of the mailboxes or of the service itself.

4.6.1 Monitoring service

To check the availability of the product, web probes and Event Management tools have been activated which, if components are unavailable, alert system administrators and operators.

Two automatic probes built for this purpose are used:

- a probe that simulates the use of the PEC mailbox from a mail client: it sends a message and waits for the appropriate replies, checking that they are consistent with what was sent;
- a probe that simulates the behaviour of a Mailbox User accessing Webmail: the probe in fact accesses the web application, authenticates, performs a series of operations on the mailbox and then logs out.

Each of these tools, if it detects a malfunction, sends an alert message, which is handled so as to ensure the best response to the Mailbox User.

The alerts from the probes are analysed by the company Problem Management process (a procedure included in the company procedures certified Vision 2000); the process involves the production of specific outputs.

4.6.2 Data backup

As for the Certification Authorities, backups of the file systems used by the various platforms in the data centre are also performed regularly for the mail systems.

InfoCert uses the most modern infrastructures for backing up disk contents. The products used to manage backups control and manage the execution of the backups and their archiving.
The backup policies provide for a weekly backup of the mailboxes; a daily incremental backup is also provided for.

The retention time of a backup is one month, except in specifically identified cases.

4.6.3 Antivirus and anti-spam

All the mail systems are equipped with antivirus software, for both incoming and outgoing mail.
The antivirus software is installed on the front-end systems, and the configuration is such that all messages in which viruses are detected are in any case passed to the PEC engine to analyse whether a “non-acceptance/detection/non-delivery due to computer virus” message should be delivered or the message rejected/deleted in compliance with the legislation in force.

InfoCert S.p.A. – all rights reserved

The system automatically checks for updates to the antivirus product and, if any are available, makes them operational immediately.

The service offers an antispam system that operates on all messages. The antispam software is installed on the front-end systems and the configuration is such that all messages detected as spam are in any case passed to the PEC engine. Checks and actions are then activated depending on whether the message is incoming or outgoing.

For incoming ordinary mail messages, the Mailbox User can choose whether to move the messages marked as spam to the "Junk Mail" subfolder or to delete them. The Mailbox User is not allowed to disable spam checking completely or to act on incoming PEC messages on the basis of this criterion.

For outgoing messages, their detection is tracked in a special log on a database. This log is scanned periodically: if a mailbox is found to have sent more than 10 spam messages in an hour, that mailbox will be blocked by changing its password. A link for resetting the password will be sent to the customer by email or by SMS to one of their contact references.

The aim of this procedure is to counter spam sent using credentials stolen through phishing or malware.

Mailboxes can also be blocked by changing the password if suspicious activity is detected, such as the sending at regular intervals of empty messages or of messages with suspicious content (for example URLs used for phishing).

Following repeated blocking of the mailbox for *spam* or suspicious activity, as described above, InfoCert may consider revoking it, as per paragraph 4.10 below.

4.6.4 Monitoring and management of suspicious access

InfoCert continuously monitors access to PEC mailboxes through all the permitted protocols (webmail, IMAP4s and POP3s) in order to identify possible unauthorised access by malicious parties or malware/bots.
Some of the criteria used for this activity are:

- Reputation of the connecting IP
- Geolocation of the connecting IP
- Check of failed attempts in correlation with the credentials used
- Sequences of suspicious operations

If there is reasonable suspicion that a mailbox has been accessed without authorisation:

- the mailbox is blocked by changing the password
- a notice with a link for resetting the credentials is sent to the secondary email
- InfoCert customer care and any intermediary are notified

The block prevents both sending and access, but does not affect the receipt of new messages or the

InfoCert S.p.A. – all rights reserved

content of the mailbox at the time of the block.

4.6.5 Blocking of attachments with suspicious extensions

When only the webmail service at the address https://webmail.infocert.it is used, attachments with extensions considered potentially dangerous, either because they are directly used in malware distribution campaigns or because they are linked to the execution of code that can change parameters or the system environment with real repercussions on its integrity, are blocked with the wording "The uploaded file has an extension that is not allowed".

When emails are sent via SMTPs, this check is not performed.

The list of suspicious extensions that are therefore blocked is given below:

.ASP	ACTIVE SERVER PAGE	**.PIF**	WINDOWS PROGRAM INFORMATION FILE (MICROSOFT)
.BAT	BATCH PROCESSING	**.PRF**	WINDOWS SYSTEM FILE
.CHM	COMPILED HTML HELP	**.PRG**	PROGRAM FILE
.CMD	DOS CP/M COMMAND FILE, COMMAND FILE FOR WINDOWS NT	**.PST**	MS EXCHANGE ADDRESS BOOK FILE, OUTLOOK PERSONAL FOLDER FILE (MICROSOFT)
.COM	COMMAND	**.REG**	REGISTRATION INFORMATION/KEY FOR W95/98, REGISTRY DATA FILE
.CPL	WINDOWS CONTROL PANEL EXTENSION (MICROSOFT)	**.SCF**	WINDOWS EXPLORER COMMAND
.CSH	CSH SCRIPT	**.SCR**	WINDOWS SCREEN SAVER
.EXE	EXECUTABLE FILE	**.SCT**	WINDOWS SCRIPT COMPONENT, FOXPRO SCREEN (MICROSOFT)
.HLP	WINDOWS HELP FILE	**.SHB**	WINDOWS SHORTCUT INTO A DOCUMENT
.HPJ	PROJECT FILE USED TO CREATE WINDOWS HELP FILE	**.SHS**	SHELL SCRAP OBJECT FILE

InfoCert S.p.A. – all rights reserved

.HTA	HYPERTEXT APPLICATION	**.PS1**	WINDOWS POWERSHELL
.INF	INFORMATION OR SETUP FILE	**.PS1XML**	WINDOWS POWERSHELL
.INS	IIS INTERNET COMMUNICATIONS SETTINGS (MICROSOFT)	**.PS2**	WINDOWS POWERSHELL
.JS	JAVASCRIPT SOURCE CODE	**.PS2XML**	WINDOWS POWERSHELL
.JSE	JSCRIPT ENCODED SCRIPT FILE	**.PSC1**	WINDOWS POWERSHELL
.LNK	WINDOWS SHORTCUT FILE	**.PSC2**	WINDOWS POWERSHELL
.MSC	MICROSOFT MANAGEMENT CONSOLE SNAP-IN CONTROL FILE (MICROSOFT)	**.TMP**	TEMPORARY FILE/FOLDER
.MSH	MICROSOFT SHELL	**.URL**	INTERNET LOCATION
.MSH1	MICROSOFT SHELL	**.VB**	VBSCRIPT FILE OR ANY VISUALBASIC SOURCE
.MSH2	MICROSOFT SHELL	**.VBE**	VBSCRIPT ENCODED SCRIPT FILE
.MSHXML	MICROSOFT SHELL	**.VBP**	VISUAL BASIC PROJECT FILE
.MSH1XML	MICROSOFT SHELL	**.VBS**	VBSCRIPT SCRIPT FILE, VISUAL BASIC FOR APPLICATIONS SCRIPT
.MSH2XML	MICROSOFT SHELL	**.VSMACROS**	VISUAL STUDIO .NET BINARY-BASED MACRO PROJECT (MICROSOFT)
.MSI	WINDOWS INSTALLER FILE (MICROSOFT)	**.WS**	WINDOWS SCRIPT FILE
.MSP	WINDOWS INSTALLER UPDATE	**.WSC**	WINDOWS SCRIPT COMPONENT
.OPS	OFFICE PROFILE SETTINGS FILE	**.WSF**	WINDOWS SCRIPT FILE
.JAR	COMPRESSED ARCHIVE FILE PACKAGE FOR JAVA CLASSES AND DATA	**.WSH**	WINDOWS SCRIPT HOST SETTINGS FILE

InfoCert S.p.A. – all rights reserved

.OCX	ACTIVEX CONTROL FILE	**.CLA**	JAVA CLASS FILE
.PL	PERL SCRIPT LANGUAGE SOURCE CODE	**.CLASS**	JAVA CLASS FILE

4.6.6 Access control dashboard

When accessing the Legalmail webmail (https://webmail.infocert.it), the access statistics of the mailbox for the current user are shown in "Account", section "Access and Security".

In particular, the following are shown, broken down by access channel:
1. Date and time of access
2. IP address or InfoCert service from which access is made
3. The browser or the access device

The possible access channels are:
a) Webmail
b) Clients or applications
c) Legalmail mobile app

4.7 Offer arrangements

The PEC service is offered in the form of mailboxes on a domain entered in the relevant index held by AgID

The offer includes:
- mailboxes belonging to domains already owned by InfoCert (for example: legalmail.it)
- mailboxes belonging to subdomains chosen by the customer, within domains already owned by InfoCert (for example: *nomecliente*.legalmail.it)
- mailboxes belonging to domains available to the customer.

Customers are therefore also allowed to use subdomains of domains they own.
In this case the customer is asked to have the manager of their domain insert an appropriate **MX** record in its **DNS** servers so that the email of the domain is routed to the InfoCert PEC system.
Responsibility for the correct **DNS** configuration lies solely with the customer.

Unless otherwise agreed with the customer, all mailboxes can be accessed:

- via the web interface offered with the product (webmail)
- via the most widely used secure email protocols; this allows the mailbox to be used both with the normal tools commonly found on workstations (for example Outlook Express) and by the customer's applications

The webmail service provides, among others, the following features:

- list of incoming messages, list sorting

InfoCert S.p.A. – all rights reserved

- viewing and downloading of the message and its attachments
- searching for messages in folders
- folder management
- address and certificate book
- management of the main service options
- filters

At the customer's request, InfoCert can issue mailboxes with special features, such as mailboxes that reject all incoming non-certified mail messages.

The reference price of the offer is the one shown on the website www.legalmail.it for the single mailbox and the features described on the website.
InfoCert may apply discounts of varying size to this price on the basis of various factors. All the mailboxes have all the functions and features provided for PEC.

Other main features include (unless the customer requests otherwise):

- an antispam system
- the option to access webmail using user-id and password
- the support of a call centre available both by telephone and by email (see par. 2.2.2 for details)
-

The offer also includes the option to customise some features of the mailboxes. These customisations are subject to separate financial conditions.
Examples include:

- the customisation of some graphic elements in the webmail interface, for all the mailboxes of a domain
- additional mailbox space compared with the standard

In addition, InfoCert can provide other complementary services that the customer may request, such as the integration of the mailbox into other services offered by InfoCert.

4.8 Activation of and access to the service

InfoCert offers customers various ways of making the following requests relating to the PEC service:

- requests for new mailboxes
- mailbox renewals
- activation of additional services
- revocation of mailboxes

Legalmail is marketed by InfoCert both through its direct sales network and through partners: the procedures may differ depending on the number of mailboxes requested and the type of customer.

InfoCert S.p.A. – all rights reserved

For detailed information, you can write to: legalmail@infocert.it.

Mailboxes can also be purchased through the website www.legalmail.it

4.8.1 Service activation

The InfoCert PEC service is activated by acquiring a mailbox belonging to the InfoCert certified domain.

InfoCert reserves the right to refuse the names proposed by the customer in the following cases, given purely by way of example: identical names, very long names, names very similar to each other, names very similar to well-known trademarks, names reserved for public Bodies and Institutions, etc.

InfoCert also reserves the right to refuse to activate the service for parties whose mailbox has previously been revoked for repeated breaches of the service policies, as provided for in paragraphs 4.6.3 and 4.10.

Activation requests can be made as follows:
- direct request via the website www.legalmail.it
- request through an InfoCert authorised intermediary
- request through InfoCert sales staff.

The new mailbox is activated within two working days of completion of the request.

4.8.2 Activation request for a mailbox purchased via the Legalmail website (www.legalmail.it)

No customisations (use of particular domains etc..) are provided for mailboxes purchased from the website, so they will be set up in the legalmail.it domain.

The Legalmail website pages contain the documentation that the customer must read:
- General conditions for the supply of the Legalmail service
- Legalmail Operating Manual
- Privacy notice on the processing of personal data

The online flow for requesting the PEC mailbox is as follows:
Formulation of the request.
Completion of the online Request form (over a secure HTTPS channel) with the information needed to activate the PEC mailbox.
If the request is completed successfully, the procedure presents online the mailbox credentials (with an expired password) and the completed Mailbox Activation Request form for the mailbox (the mailbox is reserved but NOT activated until the flow is complete).

Sending of the contract.
Once the contract has been completed, the customer, as Holder of the mailbox, directly or through a delegate (the Applicant), must sign the activation request and send it to the collection centre set up at InfoCert; if the contract is not signed with a digital signature, it must be accompanied by a legible photocopy of a valid identity document or equivalent

InfoCert S.p.A. – all rights reserved

document.
The procedures for sending the contract are as follows:

- **by Fax with handwritten signature:** the customer must send to the number indicated in the activation process on the website the activation request completed and signed by the Applicant, accompanied by a photocopy (front and back) of a valid identity document of the Applicant (see par. 1.4);
- **by email with handwritten signature:** the customer must send to the email address indicated in the activation process on the website the activation request, completed, signed by the Applicant and scanned, accompanied by a photocopy (front and back) of a valid identity document of the Applicant (see par. 1.4);
- **with online digital signature**: the system requires the Applicant to affix two digital signatures in the specific sections of the contract completed online.

PEC mailbox activation
If the documentation sent, both administrative and contractual, passes the necessary checks, the activation of the PEC mailbox is prepared. The customer is notified of the activation by an email to the mailbox indicated in the activation request.

4.8.3 Activation request for a mailbox purchased through an intermediary

The activities required to activate PEC mailboxes purchased through an intermediary or through the relevant InfoCert sales representative are described below.
For mailboxes purchased through an intermediary, customisations are possible (use of particular domains, webmail graphics etc.).
The customer receives from the intermediary the InfoCert documentation and forms relating to the following points:

- General conditions for the supply of the Legalmail service
- Legalmail Operating Manual
- Activation Request
- Privacy notice on the processing of personal data

All contracts are prepared by InfoCert and contain the service conditions. The holder, or their delegate, must sign the activation request; the intermediary is responsible for checking that the request is correct and complete.

The intermediary activates the mailboxes requested using tools provided by InfoCert.

When the Intermediary finalises the entry procedure, the InfoCert self-management platform sends an email to a back-up mailbox indicated by the end user, containing a link that allows the password of the newly created PEC mailbox to be set, again through online procedures provided by InfoCert.

In some specific cases, typically when the customer is a professional association, the setting of the password is preceded by acceptance of the terms of use of the PEC mailbox, which include, among other things, the reference to the General Terms and Conditions and the privacy notice.

InfoCert S.p.A. – all rights reserved

4.8.4 Activation request through InfoCert sales staff

The sales representative collects the information on the request and on the mailboxes to be activated; identifies the Applicant, defines the agreement and has the related PEC mailbox Activation Request signed, checking that the data entered are correct and complete.

The mailboxes requested are then activated directly by the sales representative or through other designated InfoCert staff.

4.8.5 Alternative ways of activating the service

InfoCert reserves the right to provide new procedures and flows for users to request new activations. The procedures currently used and those that may be used in the future will guarantee compliance with the rules on users' privacy and on the security and confidentiality of transactions.

4.9 Changes to mailbox data made directly by the holder

The mailbox holder is given the option to change online, completely independently, some data entered when the mailbox was registered.
Once authenticated with the mailbox credentials, the holder accesses the “My mailbox” section of the webmail and can change the following data:

- email for technical, commercial or service communications;
- telephone
- mobile phone

In addition, to meet the needs of those who have made a mistake in defining the mailbox name, within (and only within) the first 10 days from the activation of the mailbox, the name can be changed from Legalmail self-management. The old name nevertheless remains registered in the Legalmail systems and is no longer available for other registrations.

4.10 Revocation of mailboxes

A PEC mailbox may be revoked:

- on the natural expiry of the contract if the customer does not renew it;
- at the direct request of the holder, using the form available at the URL: https://www.legalmail.it/upload/Legalmail-D-1-Modulo_disdetta.pdf; revocation requests are retained for a minimum of ten years;
- by decision of InfoCert, following repeated blocking of the mailbox caused by the Holder or the Mailbox User through spam or suspicious activities, as described in more detail in paragraph 4.6.3.

The customer is notified of the revocation of the mailbox and informed of the procedure for the complete deletion of the contents of the mailbox (see the following points).

From the revocation of the mailbox:

- the mailbox can no longer be used to send or receive new messages
- for the 30 days following the revocation, the messages in the mailbox received

InfoCert S.p.A. – all rights reserved

before the revocation can still be consulted; **from the 31st day following the revocation, the mailbox can no longer be accessed**

- for 185 days following the revocation, InfoCert keeps the contents of the mailbox; during this period the mailbox can be renewed, restoring its functions and contents

- thereafter all the contents of the mailbox will be deleted. The name of the mailbox will remain reserved and can no longer be used for new activations. The holder may subsequently reactivate the mailbox, without the contents being restored.

4.11 Password reset

If the Mailbox User no longer has the password for accessing the mailbox, a new one can be set in one of the two ways described in the following paragraphs.

Note: if the Mailbox User has the password for accessing the mailbox, the password change function is available through the options of the Webmail interface.

The Mailbox User is responsible for changing the passwords used periodically. InfoCert in any case reserves the right, for security reasons and after giving prior notice, to force them to expire.

4.11.1 Password reset using additional security information

When accessing the service via Webmail, and in its options, a service is available that allows the user to:

- define some additional security information (alternative email, mobile phone number) associated with the user-id
- define a new password for the user-id with one of the following alternatives:
  - receive a token on the mobile number previously entered
  - receive, via the alternative email, a link for entering the new password

When entering the security information, one or more of the requested items can be entered; when requesting the reset, the user can choose between the various options on the basis of the information previously provided.

4.11.2 Password reset using a signed form

If a password needs to be reset and the security information described in the previous paragraph or other contact information has not been defined or is not known, the holder must follow the procedure indicated on the page https://contatta.infocert.it/recupera-password/.

If the holder of a mailbox obtained through an authorised reseller has lost or forgotten the access password, they can recover it by contacting the reseller's customer service.

4.12 Access to the service

The Customer will use the service through a connection to the Internet, which they must obtain through a separate subscription with a suitable operator.

InfoCert S.p.A. – all rights reserved

The data transfer speed of the Customer's connection has a decisive influence on the performance of the service as perceived by the Mailbox User. Please note therefore that a high-speed connection ensures a better service and must be agreed with the telecommunications operator.

The Mailbox User can access the Legalmail service with the user-id and password assigned by InfoCert with a specific authorisation profile for the mail service.

There are three types of access credentials:

1. **Standard credentials**: allow full access to and management of a PEC mailbox by the mailbox user.
2. **Multi-user credentials** (only available for some types of customer): allow access to a PEC mailbox by several distinct mailbox users, each of whom is assigned a pair of access credentials.
3. **Multi-mailbox credentials** (only available for some types of customer): allow access only to the PEC mailboxes authorised in advance.

To access the Legalmail mailbox, the Mailbox User can use their own email client. In addition to the standard method, access is also available with an Internet browser by connecting to the webmail service at https://webmail.infocert.it (or any customisations).
Access to the Legalmail PEC mailbox, both with a client and via Webmail, and the exchange of messages take place through secure protocols (TLS >= 1.2).

The customer remains responsible for constantly checking that their equipment is up to date with the security criteria to be adopted, both in terms of antivirus (to avoid being a source of contamination) and in terms of operating systems (using only those that provide constant updates to prevent contamination).

4.12.1 Access via Webmail

The access URL of the Legalmail webmail is: https://webmail.infocert.it.

Webmail is accessed with user-id/PEC address and password using an Internet browser updated to the latest security standards.

Optionally, the second authentication factor (strong authentication) can be activated through specific configuration on webmail and installation of the MyInfocert app by the mailbox user.

In the case of access with a multi-mailbox user-id, the user is asked which of the authorised mailboxes to work on, after which all further operations take place on the selected PEC mailbox.

The service allows the user to consult incoming mail, send email messages, organise incoming mail and configure various mailbox options.

InfoCert S.p.A. – all rights reserved

For detailed information on enabling strong authentication and on all the other functions of the webmail service, consult the relevant online manuals, available at: https://help.infocert.it/.

4.12.2 Access via client

To access InfoCert PEC through a mail client, one of the following clients must be used:

- Microsoft Outlook 2003 or later;
- Microsoft Outlook Express 6 or later.
- Microsoft Windows Live Mail 12 or later.
- Mozilla Thunderbird 24 or later;
- Apple Mail on Mac OS X 10 or later.

The client must also be configured with the appropriate parameters to define, for example, the type of mail server to connect to and the parameters used by the server to authenticate the Mailbox User's mailbox.

A secure connection (TLS >= 1.2) is required for all access methods.

For access, the client must be configured with the user-id provided at activation and the related password. In the case of access with a multi-mailbox user-id, the client must be configured in a particular way, available in the documentation provided to the enabled customer.

These are the standard protocols, hosts and ports that can be used for the sending and mailbox access service:

Service	**Protocol**	**Host**	**Port**
Sending	SMTP/S	sendm.cert.legalmail.it	465
	SMTP StartTLS	sendm.cert.legalmail.it	25
Mailbox access	POP3/S	mbox.cert.legalmail.it	995
	IMAP/S	mbox.cert.legalmail.it	993

For some enabled Customers, customised host names can be used instead.

For the configuration details of the various clients and of multi-mailbox access, please refer to the online manuals, available at: https://help.infocert.it/.

4.12.3 General recommendations for users

InfoCert S.p.A. – all rights reserved

For correct use of the mailboxes, it is advisable to check the mailbox frequently; in fact, every message received in the PEC mailbox is deemed to have reached the Holder of that mailbox (DPR 68/2005 [8]).

Messages should be deleted from the mail server often enough to prevent all the space assigned to the mailbox from being occupied and subsequent messages from therefore being rejected. The Legalmail service only keeps track of the logs of the main events and, in its standard configuration, does not include the legally compliant storage of the messages exchanged by email or of the related receipts.

Workstations should be equipped with constantly updated antivirus software to guarantee greater security for what is sent and received. Although the Legalmail mailbox is equipped with an antivirus capable of protecting against the main dangers of infection, it is not possible to check all potentially harmful content automatically; in particular, please note that encrypted messages or files cannot be checked.

Verifying the identity of the sender and of the recipients by the most suitable means is advisable practice. Purely by way of example, the signature affixed to an attachment to the message can be used to identify the sender. Under no circumstances can the name of the mailbox be a valid indication for identifying the holder with certainty

4.12.4 Termination of the service

If it ceases its activity as a PEC provider, the Provider will notify AgID of this intention at least 60 days in advance, indicating, if already known, the Provider that will take over the mailboxes.

With the same advance notice, the Provider informs all the holders of the PEC mailboxes it manages of the cessation of its activities (by PEC and/or a specific announcement on the website www.legalmail.it).

If the provider that will take over the mailboxes is not indicated, the notice will clearly state that none of the mailboxes will be accessible any longer from the time the Provider ceases its activities. InfoCert in any case provides for the mailboxes affected by the cessation of the service to remain active in read-only mode (without the possibility of sending / receiving messages) for a period of no less than 30 days from the day set for the cessation of the service.

InfoCert S.p.A. – all rights reserved

5. Service requirements

5.1 Mailbox and message size

The minimum initial size of a mailbox is 1 GB: this size can be increased.

Please note that the maximum guaranteed size of a PEC message is 100 MB. The sending or receipt of a message with attachments of a total size of up to 70 MB is guaranteed.
Email systems transform attachments to allow their transmission, and this increases the size of the message sent.

Before sending a message of significant size, it is good practice to check that there is sufficient **space** to receive all the delivery receipts.

If the message is sent (in "TO") to many PEC recipients and the message size is significant, it must be borne in mind that each delivery receipt has the whole message sent attached, unless the sender instructs otherwise.

To acquire all the delivery receipts correctly, sufficient space must therefore be available in the sender's own mailbox. Otherwise, the receipts exceeding the size of the mailbox will not be delivered.

For this reason, limits have been set on the maximum number of recipients for a single sending,

equal to a total of **1,000 between To and Cc**

The Mailbox User is responsible for checking how full their PEC mailbox is, and for emptying it periodically.

5.2 Conditions for the supply of the PEC service

The service is governed and provided in accordance with the legislation in force and with the provisions of the Contract, which comprises:

- the activation request;
- the general conditions for the supply of the service;
- the Operating Manual;
- the privacy notice.

All the documentation can be found on the website www.legalmail.it

5.3 Obligations and Responsibilities

5.3.1 Obligations of the Provider

The Provider guarantees the supply of the PEC service in accordance with the legislation in force, according to the service levels described therein, and on the basis of the provisions of the Contract.

InfoCert assumes no obligation to retain the messages sent and received by the Customer and/or the Mailbox Users with the PEC mailbox covered by the Service.

InfoCert S.p.A. – all rights reserved

Such retention is the sole responsibility of the Customer and/or the Mailbox Users themselves.

InfoCert accepts no responsibility for the certified mail services provided by other providers

5.4 Obligations of the Holders

The Customer assumes the obligations and liabilities under current legislation and the Contract.

5.4.1 Limitations and compensation

Under no circumstances will the Provider be liable for events not attributable to it, and in particular for damage suffered by the Customer, the Mailbox User or any third party caused directly or indirectly by their failure to comply with the rules set out in this Operating Manual and in the Contract, or by the carrying out of unlawful activities.

Except in cases of wilful misconduct or gross negligence, the Provider will not be liable for service disruptions falling within the service level parameters indicated in paragraph 9 below and, in any case, within the limits provided for in the contract concluded with the Customer
Except in cases of wilful misconduct or gross negligence, the Provider will not be liable for failure to perform the obligations assumed under the service contract if such failure is due to causes not attributable to the Provider itself, such as - purely by way of example - fortuitous events, unforeseeable and uncontrollable technical malfunctions, actions by the authorities, force majeure, natural disasters and other causes attributable to third parties.

The Provider has taken out an insurance policy covering the risks of its activity and damage caused to third parties, with the following cover limits:

- **€10,000,000 per individual claim**
- **€10,000,000 per year.**

During the performance of this contract, InfoCert reserves the right to change the way the Legalmail Service is provided in order to adapt it and bring it into line with any legislation that may be issued to govern PEC services.

InfoCert S.p.A. – all rights reserved

6. Data protection

6.1 Applicable legislation

See the privacy notice pursuant to and for the purposes of Article 13 of Legislative Decree 196/2003 and Article 13 of Regulation (EU) 679/2016, the so-called General Data Protection Regulation ("GDPR"), and the implementing provisions of the Italian Data Protection Authority.

The full documentation is available at the URL:
https://www.infocert.it/pdf/privacy-attivazione.pdf

6.2 Security measures for the protection of personal data

All PEC messages and communication through mail clients or the WEB interface take place through secure protocols and connections, such as (SMTP + TLS), (IMAP + TLS), (POP3 + TLS) and HTTPS.

In addition, only accredited users who have passed the security checks can access their own InfoCert PEC mailboxes.

InfoCert S.p.A. – all rights reserved

7. Accuracy of the time reference

The time reference of the Provider's system is based on synchronisation with the time-stamping system maintained by InfoCert as an Accredited Certifier for Qualified Signatures.

The InfoCert system requires all procedures to refer to the date/time of the system clock, which is kept aligned with the systems of the TSA (Time Stamping Authority). The latter obtains the exact UTC (Coordinated Universal Time) from the synchronisation signal of a high-quality external receiver, which in turn obtains the time from a radio receiver tuned to the signal broadcast by the National Electrotechnical Institute (IEN) “Galileo Ferraris”. The receiver used has been calibrated and certified in advance by the IEN itself; since the transit times of the internal network (at 1 Gbs) tend to zero, the time signal thus obtained complies with the accuracy margins required by the legislation in force (DPCM 13/1/2004), equal to 1 second.

7.1.1 Security of the time validation system

The system for the time-stamping service can only be activated by authorised operators using a series of passwords and a certain number of smart cards.
Once activated, the system does not require further interactive login procedures, except to shut it down and restart it for maintenance purposes.

Any shutdown of the system can only be resolved by the authorised operators.

The TSA system has a specific component dedicated to monitoring the following conditions:

1. attempts to tamper with the security of the system
2. loss of the synchronisation signal with the external time source
3. degradation of performance in terms of response time
4. availability of the non-rewritable storage medium

If one or more of the above conditions occurs, the seriousness of the event is assessed, and the time-stamping service is stopped if the necessary security measures are not in place.

InfoCert S.p.A. – all rights reserved

8. Service levels

The service hours are:

Service	Hours
Sending messages from webmail or a mail client	*From 0:00 to 24:00* 7 days a week
Access to messages received, from webmail or a mail client	*From 0:00 to 24:00* 7 days a week

The service is therefore available 24 hours a day, every day of the week.

Service availability is no less than 99.8% on a four-monthly basis, with a maximum duration of a single outage of less than 2 h 52 min. and 48 sec.

The service level refers to InfoCert's systems, including the connection between InfoCert and the telecommunications network, but not to the network itself or to the Customer's access to it, whose service level is the responsibility of the network provider.

For details of the service limitations not attributable to InfoCert, please refer to the previous paragraph 'Limitations and compensation' in chapter 6.

8.1 Monitoring of the Provider's service level

Procedures and automatic systems are in place for monitoring the status of the system that provides the PEC service and of the Provider's entire technical infrastructure.

Automatic monitoring tools are installed that allow the Provider to check the system by assessing the events and the states in which the system finds itself.

The system is configured to take, depending on the evolution of its states, actions of the following types:

- recording of events;
- recognition of events;
- resolution of problems;
- notification to operators.

The architecture of the InfoCert PEC system has been designed to guarantee the high reliability of the system by using redundant systems, as illustrated in the paragraph 'The tools adopted' in chapter 4.

InfoCert S.p.A. – all rights reserved

8.2 Systems maintenance.

For the correct configuration of new systems and the correct restart of a system that has undergone maintenance, a checklist is provided listing the tests to be carried out to guarantee that, at the end of any maintenance activity, the system works correctly and in compliance with the PEC rules.

8.3 Security and quality checks

The Provider's operating procedures and security procedures are subject to periodic checks linked to verifications set up by the internal auditing function. These checks aim to verify the correct application of the procedures provided for and their actual effectiveness in relation to the set objectives.
In addition to process auditing activities, analyses and checks are planned on the records produced by the applications and systems during normal operation. The purpose of this activity is to check that all the events that have occurred fall within normal operation and that no events prejudicial to security occur. The recording of the events that have occurred, and their consequent attributability, also constitute a further security measure.

To allow mail to be kept in a protected environment, the Legalmail PEC system is equipped with several levels of firewalls and intrusion detection.

The events recorded in the technical and application logs undergo automatic checks and spot checks.

8.4 Data backup procedures

The data of the networked systems are backed up daily by an automated archiving system. Periodically, a copy of the media containing the backup data is stored in a security cabinet, to which access is allowed only to the designated operator belonging to the Provider's organisation.

Periodically, a copy of these media is also taken to a secure location outside the Provider's premises, so that it is available even in the event of disasters.

To guarantee that the complete system can be restored after failures, all the other data and programs needed to provide the service are backed up. The archiving procedures and times of these backups are the same as those of the data backup procedures.

8.5 Emergency services

To guarantee the completion of transmission and the issue of receipts, the following technical and organisational solutions have been put in place:

- Redundant systems: all systems are redundant so as to guarantee high reliability of the service, while the Mailbox User mailboxes, accessible from several systems, are kept on NAS (Network

InfoCert S.p.A. – all rights reserved

Attachment Storage) systems – see details in chap. 4, “The tools adopted”.

- Automatic monitoring tools: automatic tools for checking the system and its various functional components are active in the Certified Mail system. Depending on the problems detected, the system provides for actions to resolve them or for notification to operators so that they can intervene (see chap. 9, “Monitoring of the Provider's service level”).
- Disaster management: the Provider has adopted the procedures needed to guarantee the continuity of the service even in situations of high criticality or disaster – for details see chap. 11, “Disaster Management Procedures”.
- Notifications of processing problems: the system (Certified Mail engine) checks the messages in transit, detecting problems in the propagation or processing of messages. If a problem is detected, the system:
  - saves the current transaction to special error queues
  - attempts to restore the transaction automatically at predefined time intervals in order to recover the messages in the error queue
  - promptly alerts the operators to the problem with automatic notices. The authorised operators use a special console to check and manage the problem and restore the blocked transactions after the systems or the necessary software have been reactivated.

InfoCert S.p.A. – all rights reserved

9. Provider interoperability

In compliance with the provisions of DPR 68/2005 [8], InfoCert guarantees interoperability with the other providers in accordance with the PEC rules (DM 2/11/2005 [5]).

InfoCert will periodically repeat the appropriate checks with the other providers in order to maintain interoperability between the respective systems.

InfoCert S.p.A. – all rights reserved

10. Security Measures

The Provider has implemented a security system for the information system of the PEC service. The security system implemented is structured on three levels:

- a physical level, which aims to secure the premises where the Provider manages the service
- a procedural level, with purely organisational aspects
- a logical level, through hardware and software technological measures that address the problems and risks connected with the type of service and with the infrastructure used.

This security system is designed to avoid risks arising from the malfunctioning of systems, the network and applications, as well as from unauthorised interception or modification of data.

All the Provider's operating processes in providing the PEC service comply with the company Quality Plan.

10.1 Description of the security measures

10.1.1 Physical security

The measures adopted provide adequate security guarantees with regard to:

- Characteristics of the building and its construction;
- Active and passive anti-intrusion systems;
- Physical access control;
- Power supply and air conditioning;
- Fire protection;
- Flood protection;
- Storage procedures for magnetic media;
- Storage sites for magnetic media.

10.1.2 Security of procedures

- To guarantee that no individual can on their own compromise or alter the overall security of the system or carry out unauthorised activities in the management of the service, the organisation of work provides for the separation of roles, with the activities considered critical assigned to different people with separate and well-defined tasks.
- The staff responsible for designing and providing the Certified Mail service are employees of the provider and have been selected on the basis of their experience in designing, implementing and running IT services and of their reliability and confidentiality.
- Training sessions are planned periodically to develop awareness of the tasks assigned. In particular, before staff are assigned to operational activities, training sessions are held to provide all the skills (technical, organisational and procedural) needed to carry out the tasks assigned

10.1.3 Logical security

Access to the systems is allowed only to authorised staff.

Operators are entitled to access the systems with the minimum authorisations needed to perform

InfoCert S.p.A. – all rights reserved

their duties.

The systems keep track of accesses and of the operations carried out.

10.2 Rules of conduct

InfoCert's Security Policies and the related documents set out the guidelines and company policy for all the services in the company. These documents aim to create greater awareness and consideration among all staff of the confidentiality of information and of the activities carried out during office hours. Staff are explicitly asked to observe “the utmost confidentiality” regarding all the information that comes into their possession. The rules for the physical access of employees and external consultants, the rules for the use of badges and the rules for access outside office hours are set out. Part of the documents is dedicated to the security of equipment, systems and IT applications. The rules on the use of passwords (secrecy and the need to change them periodically) and of PCs (use limited to professional purposes, care of and responsibility for the machine, prohibition on using software not released by the relevant office, rules for remote connection, rules for virus management, rules for Internet access and email use, immediate removal of access rights when no longer needed) are set out. The aim of the policies expressed in them is also to minimise the possibility of illegal or unauthorised software being introduced, even unintentionally, into the internal network.
All the non-confidential documents addressed to staff are available on the company Intranet.

10.3 Disaster Management Procedures

The Provider has adopted the procedures needed to guarantee the continuity of the service even in situations of high criticality or disaster.

The disastrous events taken into consideration are those that would make one of the rooms housing the InfoCert systems unusable. For the purpose of restoring the Provider's critical functions, the unusability of the data centre room is therefore taken into consideration.

For non-catastrophic events, the continuity of the service is guaranteed because:

- all the systems are replicated and provide a high-availability service; in the event of a hardware failure, the service is in any case guaranteed by a twin system;
- load balancing and network redundancy between the systems are guaranteed by dedicated devices configured so that, if a system does not respond, the traffic in transit is diverted to its twin system.

Besides guaranteeing service continuity in the event of hardware failures, the redundancy of the systems also guarantees service continuity during software or hardware upgrades.

10.4 Functions to be restored and maximum restoration times

For the PEC Management service, InfoCert has set up an infrastructure with logistical and procedural mechanisms designed to prevent events that could compromise its ability to

InfoCert S.p.A. – all rights reserved

provide the service.

InfoCert uses a remote Disaster Recovery centre, where there is a subnetwork of offline systems, kept up to date so as to be able to provide service to the company's most critical products in the event of a disaster that put the Padua data centre out of operation; the Disaster Recovery site is connected to the Padua site by a high-speed line to handle the load of the updates, which are carried out daily.
At the Disaster Recovery site there are systems on stand-by to host the PEC service.

In the event of disasters, the functions essential to minimise the interruption of the service and guarantee compliance with the legal requirements regarding the availability of the information recorded in the message log have in any case been identified.

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.

InfoCert S.p.A. – all rights reserved

InfoCert
TINEXTA GROUP