Aruba PEC S.p.A.

Certification Practice Statement

Version: 1.7
Date: 11/11/2021
Draft: Alessandro Capobianco
Checked by: Nicole Mazzoni, Federico Ciofi
Approved by: Andrea Sassetti
Document classification: pubblico

Version	Date	Changes
1.0	24 May 2016	First version of the document.
1.1	11 October 2016	p. 1.4 Updated table of definitions p. 2.3 Updated version index p. 4.4.3.1 Minor corrections (typos) p. 4.4.3.2 Minor corrections (typos) p. 4.5 Application qualification methods added and reference to Annex A removed p. 4.6 Meaning of acronyms added p. 4.7 Log retention period corrected p. 4.8 TSA termination plan updated p. 5.1.8 Descriptions of the figures in this paragraph updated p. 5.1.9 References to applicable regulations updated Annex A completely Removed
1.2	26 May 2017	Template updated Registered office updated
1.3	12 July 2017	New template with MGA ID code adopted p. 1.1 Regulatory references updated p. 2.3 Version reference updated p. 2.5 References corrected New paragraph p. 2.5.1 added p. 3.1.1 Obligations of relying parties included p. 4.2 Specifications for external suppliers added p. 4.2.1 Removed p. 4.4.3.2 Key management methods updated c.5 Numbering corrected p. 5.1 Users' obligations updated and typo corrected
1.4	23 May 2019	Whole document: logo and template updated p. 1.3 Regulatory references updated p. 2.1 Legal Representative updated p. 3.1 Point 4 relating to the collection and processing of personal data removed p. 3.2 Reference to information released pursuant to art. 13 of the GDPR added p. 4.3 Chapter removed p. 5.10 Reference to jurisdiction of the Court of Arezzo
1.5	14 October 2019	p. 1.3 and 4.4 – references to CNIPA Resolution No. 45/2009 (repealed) replaced p. 2.2 – references added regarding the application of recommendations issued by the Agency in AgID. Res. No. 121/2019 p. 3.3.2 and 3.3.5 – limitations of supplier's liability reworded
1.6	21.1.2021	p. 1.3 - Applicable regulatory references revised p. 2.3 – Minor changes p. 4.5 – Description of service availability revised; p. 4.6 – Specification added
1.7	21.10.2021	p. 4.6 – Log retention period updated

SUMMARY

LIST OF FIGURES

1. INTRODUCTION

1.1 Purpose of the document and main recommendations for readers

This section explains the purpose of the operating manual and provides recommendations for the correct use of the timestamp service.

Please read the entire text of the Manual as the recommendations in this section are incomplete and many other important points are covered in the other chapters. To make it easier and quicker to read the Operating Manual, we recommend consulting the list of acronyms and abbreviations at the end of this section. This operating manual is intended to illustrate and define the operating procedures adopted by Aruba PEC S.p.A. for certification activities pursuant to Presidential Decree No. 445 of 28 December 2000, “Consolidated text of the laws and regulations on administrative documentation”, published in the Ordinary Supplement to Official Journal No. 42 of 20 February 2001, Legislative Decree No. 82 of 7 March 2005, published in Official Journal No. 112 - Ordinary Supplement No. 93 “Digital Administration Code” and subsequent amendments and additions, and the Presidential Decree of the Council of Ministers (DPCM) of 22 February 2013, “Technical rules on the generation, application and verification of advanced electronic, qualified and digital signatures”, published in Official Journal No. 117 of 21 May 2013, as well as Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market, repealing Directive 1999/93/EC.

In particular, this document illustrates the methods for requesting, validating, issuing and using the timestamps provided as part of the qualified electronic timestamp service, as well as the responsibilities and obligations of the certifier, of the requesting parties and of all those who access the service for verification of the timestamp signatures.

In accordance with the information obligation (DPCM 22 February 2013, art. 40 and subsequent amendments and additions) required by law, as a digital certification provider Aruba PEC S.p.A. is publishing this operating manual so that every individual user can assess the reliability of the service being offered. It is assumed in this Operating Manual that the reader has adequate knowledge of the subject of trust services and the PKI system.

So that the qualified electronic timestamp service can be used properly, in addition to recommending that the user reads this document carefully, Aruba PEC S.p.A. recommends that anybody who needs to rely on a qualified electronic timestamp and/or the information contained in the certificate associated with it, should first check to ensure:

1. That the certificate is valid and has not been revoked or suspended, by using the specific lists of revoked or suspended certificates, available to users electronically (see the definitions of CRL and CSL).
2. That the qualified electronic timestamp was created when that certificate was being used by the private key corresponding to the public key specified in the certificate.
3. That the message associated with the qualified electronic timestamp has not been modified.

For more information, please refer to the Aruba PEC S.p.A. website http://www.pec.it or contact customer services at: assistenza@ca.arubapec.it.

1.2 References to standards

Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".

ISO/IEC 19790:2012: "Information technology -- Security techniques -- Security requirements for cryptographic modules".

ISO/IEC 15408 (parts 1 to 3): "Information technology -- Security techniques -- Evaluation criteria for IT security".

ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

ETSI EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Timestamps

ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Timestamping protocol and timestamp token profiles".

FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".

PKCS. Public Key Cryptography Standards. Standards designed to ensure the interoperability of cryptographic techniques. The components of this standard are numbered. More information about the PKCS standards implemented are available at http://www.rsa.com.

LDAP. Lightweight Directory Access Protocol. Protocol used to access directory services online (in particular X.500 directory services) that may contain information about users and their digital certificates.

X.500. A set of ITU-T standards for electronic directory services.

X.509. ITU-T T standards for digital certificates. X.509 v3 refers to certificates that contain or are able to contain extensions.

Secure Sockets Layer (SSL). The protocol originally developed by Netscape, which then became the universal standard for authenticating websites and encrypting communication between clients (browsers) and web servers.

IPSec. Set of open standards for ensuring secure private communication within IP networks at network level, which provide network-level encryption.

SHA-1. Secure Hash Algorithm (SHA), algorithm specified in the Secure Hash Standard (SHS, FIPS 180), developed by NIST. SHA-1 is a version of the SHA algorithm published in 1994.
The reference standard consists of the ISO/IEC 10118-3:2004 standard.

SHA-256. Secure Hash Algorithm (SHA), algorithm specified in the Secure Hash Standard (SHS, FIPS 180), developed by NIST.
The reference standard consists of the ISO/IEC 10118-3:2004 standard.

1.3 Regulatory framework

[1] Presidential Decree (DPR) No. 445 of 28 December 2000, “Consolidated text of the laws and regulations on administrative documentation”, published in the Ordinary Supplement to Official Journal No. 42 of 20 February 2001.

[2] Prime Ministerial Decree (DPCM) of 22 February 2013, "Technical rules on the generation, registration and verification of advanced, qualified and digital electronic signatures, pursuant to articles 20, paragraph 3, 24, paragraph 4, 28, paragraph 3, 32, paragraph 3, letter b) , 35, paragraph 2, 36, paragraph 2, and 71.", published in Official Journal No. 117 of 21 May 2013.

[3] Regulation (EU) No. 910/2014 of the European Parliament and of the Council, dated 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market, repealing Directive 1999/93/EC.

[4] Legislative Decree (DLGS 196) No. 196 of 30 June 2003, “Personal Data Protection Code”, published in Ordinary Supplement No. 123 of Official Gazette No. 174 of 29 July 2003, and subsequent amendments.

[5] Legislative Decree (CAD) No. 82 of 7 March 2005, "Digital Administration Code" (CAD), published in Official Journal No. 112 of 16 May 2005.

[6] Resolution No. 121 of 17 May 2019, “Guidelines containing the Technical Rules and Recommendations relating to the generation of qualified electronic certificates, qualified electronic signatures and seals and qualified electronic timestamps” (Resolution No. 121/2019).

[7] Law of 11 August 1991, "Introduction of the National Calibration System”, Published in Official Gazette No. 104 of 6 May 2002.

[8] Legislative Decree No. 159 of 4 April 2006 “Supplementary and corrective provisions to Legislative Decree No. 82 of 7 March 2005 containing the digital administration code”, Published in Official Journal No. 99 of 29 April 2006.

[9] Regulation (EU) 2016/679 (“GDPR”) of the European Parliament and of the Council dated 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, repealing Directive 95/46/EC.

1.4 Definitions and acronyms

CA	Certification authority
CAD	Digital Administration Code
CRL	Certificate revocation list
CSL	Certificate suspension list
CSR	Certificate signing request
AGID	Digital Italy Agency
DPCM	Prime Ministerial Decree of 30 March 2009[2]
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol with SSL
ISO	International Standard Organization
ITSEC	Information Technology Security Evaluation Criteria
LDAP	Lightweight Directory Access Protocol
NTP	Protocol for accessing services providing a guaranteed date and time
OCSP	Protocol for checking the status of digital certificates online
OID	Object Identifier
POP	Point of Presence
PKCS	Public Key Cryptography Standards
PKI	Public key infrastructure
RDN	Relative Distinguished Name
RPA	Relying Party Agreement
RSA	Encryption system
SET	Secure Electronic Transaction
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
TLS	Transport Layer Security
TSA	Time Stamping Authority (time stamping system)
SP	Security Procedures – Aruba PEC S.p.a.'s security procedures
VTEQ	Qualified Electronic Timestamp
WWW	World Wide Web
X.509	ITU-T specifications for certification and associated authentication framework
TSP	Trust Service Provider

2 IDENTIFICATION DETAILS - OPERATING MANUAL PUBLICATION

2.1 Identification details of the Qualified Trust Service Provider

Company Name: **Aruba PEC S.p.A.**
Registered office: **Via San Clemente, 53 – 24036 Ponte San Pietro (BG)**
Legal Representative: **Giorgio Cecconi**
REA number: **145843**
Company Registry registration number: **01879020517**
VAT number: **01879020517**
Telephone number (switchboard): **+39 0575 0500**
FAX number: **+39 0575 862022**
PEC [certified email] address: **direzione.ca@arubapec.it**
ISO OID (private enterprise number): **1.3.6.1.4.1.29741**
Main web server: http://www.pec.it
Trust services web server: https://ca.arubapec.it

2.2 Policy **ID**

The ID for the electronic timestamp policy described in this document is **0.4.0.2023.1.1**, corresponding to the "**Best practices Timestamp Policy**" (BTSP) defined in the **ETSI TS 319 421** standard. By including this object identifier (OID) in the timestamp tokens, Aruba PEC's TSA certifies its compliance with the BTSP policy.

Unless otherwise requested by the parties in question, electronic certificates intended for qualified electronic timestamps are issued in accordance with application of the recommendations issued by the Agency which are designed to guarantee greater interoperability and the use of online services in Italy (AgID Resolution No. 121/2019, with subsequent amendments and additions). Full application of the recommendations contained in the resolution is confirmed through the addition of a PolicyIdentifier element to the Certificate Policies field (OID 2.5.29.32), with the **agIDcert** value (OID 1.3.76.16.6). The provisions of this Timestamping Authority Practice Statement assume full compliance with these recommendations.

2.3 Operating manual version

This Operating Manual belongs to Aruba PEC S.p.A., all rights reserved.
The Operating Manual will be updated by its manager when there are significant technical or regulatory changes that require a change to the service. If the update is substantial, a new version of the document will be published. If the update is minor, a new release will be published. The version/release number is shown on the front cover of the document and in the footer of every page.

2.4 Publication of the manual

This document is published on the main pages of the web server for the trust services specified in paragraph 2.1.

2.5 Manager of the operating manual

Aruba PEC is responsible for defining, publishing and updating this document. The person responsible for this operating manual at Aruba PEC is:

Andrea Sassetti
Director of Certification Services
Aruba PEC S.p.A.

Tel.	+39 0575 1939715
Fax.	+39 0575 862022
Email:	CPS-requests@ca.arubapec.it

2.5.1 Drafting and revision of the operating manual

The process of drafting and approving the operating manual complies with the procedures laid down for the company's Quality Management System.

In particular, the manual is reviewed and, if necessary, updated at least once a year and the changes are approved by the CA Services Department, once they have been verified by the relevant departments in the company.

3 GENERAL PROVISIONS

3.1 Obligations of the requesting party, of the trust service provider and of users

1. The party applying for the Qualified Electronic Timestamp service must take all appropriate organisational and technical measures to avoid causing harm to others.
2. The qualified trust service provider must take all appropriate organisational and technical measures to avoid causing harm to others.
3. The qualified trust service provider that issues [or] provides the Qualified Electronic Timestamp service must also:
   a. Ensure that the qualified electronic timestamp links the date and time to electronic data in such a way as to reasonably exclude the possibility of undetectable changes to the data;
   b. this is based on an accurate time-measuring source connected to coordinated universal time;
   c. it is applied via an advanced electronic signature or sealed with an advanced electronic seal from the qualified trust service provider or an equivalent method;
   d. comprehensively and clearly inform those requesting the service about the procedure for issuing qualified electronic timestamps and the technical requirements for accessing them;
   e. use durable communication media to provide all useful information for individuals requesting the qualified electronic timestamp trust service, including in particular the exact terms and conditions for using qualified electronic timestamps and the procedures for making complaints and resolving disputes; this information, which may be provided electronically, must be written using clear language and must be provided before the agreement is entered into by the person requesting the service and the qualified trust service provider.

3.1.1 Obligations of those accessing the verification of electronic timestamps

Those intending to use documents with corresponding qualified electronic timestamps must:

1. ensure that the information contained in the qualified electronic timestamps matches the details of the qualified trust service provider;
2. ensure that the corresponding message has not been modified/altered;
3. ensure that the qualified electronic timestamp has been signed correctly by the trust service provider and that the private key used for this signature has not been compromised before the timestamp was added.

3.2 Obligations regarding the processing of personal data

The qualified trust service provider collects the data subjects' personal data exclusively in accordance with the provisions of the policy issued in accordance with article 13 of Regulation (EU) 2016/679. Data may not be collected or processed for any other purposes without the explicit consent of the person to whom it refers.

3.3 Limitations of Liability and any limits on compensation

This section describes the limitations applying to the liability assumed by the Certifier when carrying out its activities.

3.3.1 Knowledge of the operating manual

Those requesting the VTEQ service and those intending to access VTEQ verification are assumed to have first read and understood this Operating Manual, with particular reference to the methods described herein for the timestamp and verification processes. The Certifier is explicitly released from any liability resulting from ignorance of or incorrect use of the procedures described in this manual.

3.3.2 Force majeure

Except in the event of wilful misconduct or negligence, the qualified trust service provider will not be held liable in the event of circumstances beyond its control or for reasons not attributable to it. This means that, except in the event of wilful misconduct or negligence, the qualified trust service provider will not be liable for damages of any kind, suffered by anyone and caused by an act of God or force majeure, if the service cannot be provided, if an order or prohibition is issued by any authority, including but not limited to, networks or technical equipment that are not working correctly, where this is beyond the Certifier's control, for interruption of the electricity supply, flooding, strikes, fire, acts of war, epidemics, coups d'état, earthquakes and other disasters.

3.3.3 Disclaimer and Limitations of the qualified trust service provider's liability

Once it has finished providing the qualified electronic timestamp service, the qualified trust service provider has no further obligation to verify the validity of the data and information contained in the request, nor does it have any obligation, which also applies before the qualified electronic timestamp service is provided, to verify the validity, accuracy and integrity of the electronic documents to which the user wishes to add the timestamp; the qualified trust service provider does not assume any further obligation, guarantee or liability with respect to the provisions of this Operating Manual or current legal provisions, and will not be liable for damages of any kind, suffered by any person, if such damages result from a breach of the provisions and content of this Operating Manual or of current legal provisions.

3.3.4 Indemnity

The party requesting the VTEQ service and the user who verifies it indemnify and hold the qualified trust service provider and its assignees harmless against any direct or indirect liability, expense, harm or damage resulting from claims or legal actions brought by third parties for which the qualified trust service provider is deemed liable to third parties, due to an action attributable to the requesting party and/or the user of the VTEQ service, expressly including, but not limited to, liability and damages resulting from any invalid, inaccurate or out-of-date information or data given to the qualified trust service provider and/or incorrect use of the procedures described in this Operating Manual.

3.3.5 Exclusion of compensation for indirect damages

Except in the event of wilful misconduct or negligence, the qualified trust service provider will not be liable for any indirect damage or for any loss of profit and/or loss of data or any other indirect and consequential damages resulting from or in connection with the use, delivery, licensing, performance or non-performance of certificates, qualified electronic digital timestamps or any other digital transaction or service offered or considered in this Operating Manual.

3.3.6 Limitations of Liability

The qualified electronic timestamp service offered by Aruba PEC S.p.A. is not designed, intended or authorised for use or sale as a control device in hazardous circumstances, or for use in situations that require an error-free environment, such as the management of nuclear power stations, aviation communication or navigation systems, air traffic control or communication systems or weapons control systems in which any failure would directly result in death, personal injury or serious damage to the environment.

3.3.7 Hazardous activities

The qualified electronic timestamp service offered by Aruba PEC S.p.A. is not designed, intended or authorised for use or sale as a control device in hazardous circumstances, or for use in situations that require an error-free environment, such as the management of nuclear power stations, aviation communication or navigation systems, air traffic control or communication systems or weapons control systems in which any failure would directly result in death, personal injury or serious damage to the environment.

3.4 Service fees

For the service fees please refer to the information request form on website http://www.pec.it.

4 HOW THE SERVICE OPERATES

This section describes how the qualified trust service provider operates and in particular the roles of the members of staff responsible for the qualified electronic timestamp service, how timestamps are requested and the communication process with the parties requesting them.

4.1 Roles of the employees responsible for providing the Qualified Electronic Timestamp Service

The organisational structure is defined in accordance with the ETSI EN 319 401 standards and in accordance with current Italian law.

The roles of trust and the corresponding responsibilities are formally assigned by Management through letters of appointment. The requirements for retaining an appointment are re-evaluated at least annually and when there are changes to the company's organisational structure. Those entrusted with such roles can make use of employees and staff members to carry out their activities, in accordance with the general provisions adopted by the company.

The roles and tasks of employees are allocated in such a way that a single person is not able to circumvent the security measures in place to protect the TSA systems; in addition, those entrusted with these tasks are free from any conflicts of interest that could harm the impartiality of the activities assigned to them.

Aruba PEC has defined the following roles of trust/individuals in positions of responsibility within the context of the TSA service:

- Security Officer: responsible for implementing and managing security procedures. This individual serves as the "Security Supervisor" required under current Italian law.
- System Administrator: responsible for installing, configuring and maintaining the TSA systems. The System Administrators perform the role of the "Technical Systems Operation Supervisor" required under current Italian law.
- System Operator: responsible for the day-to-day operation of the TSA systems.
- System Auditor: responsible for checking the archives and audit logs of the TSA systems.

In accordance with current Italian law, the following individuals are also appointed to positions of responsibility at Aruba PEC, in addition to those mentioned above:

- The manager of the certification and timestamp service;
- The manager of technical and logistical services;
- The manager of audits and inspections (auditing).

The roles listed above may rely on other employees and operators to carry out tasks for which they have expertise.

4.2 Dealings with external organisations

The qualified trust service provider may delegate certain activities to third parties, including those belonging to the Aruba PEC corporate group, in order to ensure that the service is provided as effectively as possible.

In such cases, the qualified trust service provider will use specific agreements to ensure that these external organisations are bound by:

a) the requirement to respect the provisions of this Operating Manual;
b) the requirement to respect the applicable technical and legal regulations governing provision of the service;
c) the requirement to respect the in-house policies that relate to processing of the customers' and users' personal data;
d) the requirement to respect the software and hardware security policies adopted by the qualified trust service provider within its own organisation;
e) the requirement to respect the quality policies adopted by the qualified trust service provider.

External agents to whom activities may be delegated within the context of the trust services governed by this Operating Manual are chosen and selected taking into account their experience, competence

and professionalism, to ensure that the provisions of this document and the regulations referred to herein are respected.
At the time of writing this Operating Manual, the Aruba PEC TSP-Q does not use any supplier outside the Aruba Group for provision of the qualified timestamp service.

4.3 Operating procedures for adding and defining qualified electronic timestamps

4.3.1 Qualified Electronic Timestamps

A qualified electronic timestamp is a piece of information containing the date and time associated with one or more electronic documents. The time reference is generated using a system that guarantees a deviation of no more than one second from UTC.
The time reference used by Aruba PEC is obtained from a high-precision device that guarantees a difference of no more than one second from the UTC (IEN) time scale, referred to in Ministry of Industry, Commerce and Trade Decree No. 591 of 30 November 1993.
The qualified electronic timestamp is provided by Aruba PEC on the basis of the provisions of art. 42 of Regulation (EU) No. 910/2014 of the European Parliament and of the Council, dated 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/CE and its implementation rules.

4.3.2 Requesting the qualified electronic timestamp service

The qualified electronic timestamp service offered by Aruba PEC S.p.A. is available via the HTTPS protocol.
The formats and coding of accepted requests and qualified electronic timestamps returned by the service comply with the data structures described in RFC 3161 and ETSI EN 319 422.
A request is accepted by the web server servizi.arubapec.it, via the address https://servizi.arubapec.it/tsa/ngrequest.php (which must be configured on the client chosen for interfacing with the service) with the credentials provided by Aruba PEC S.p.A. when the TSA account was activated (which must be entered in the software chosen for interfacing with the service).
Aruba PEC's TSA service only accepts requests for timestamps that contain tracking information on the electronic evidence to be timestamped according to the hash algorithm **SHA-256** (dedicated hash-function 4 defined in the ISO/IEC 10118-3:2004 standard and subsequent amendments).
Once the user has been authenticated and the accuracy of the request received has been verified, the availability of the timestamp is assessed. If it is available, the system returns the TimeStampResp (RFC3161) containing the TimeStampToken (RFC3161) for the HASH included in the TimeStampReq (RFC3161) provided when the request was sent
If the TSA system receives a qualified timestamp request that does not comply with the above requirements, an error message will be generated.

Summary of the procedure followed by the user:

1. Launch the signature and verification application
2. Select the function for adding the VTEQ
3. Select the file;
4. The software requires an Internet connection as it will attempt to access CRL and/or OCSP;
5. The software shows a video of the result of adding the qualified electronic timestamp. The content of the file can be read using programs suitable for that file's format (for example: PDF files can be read with Acrobat Reader).

Once it has received a request in the format described above, the Aruba PEC Time Stamping Authority will send a message containing a TimeStampToken (RFC3161) coded in DER, as required by RFC 3161.

4.3.3 Logical and physical security of the qualified electronic timestamp system

Thanks to technical precautions designed to prevent access by unauthorised individuals and damage caused by accidental events, processors offering the VTEQ location service are physically protected to prevent the possibility of any physical compromise.

4.3.3.1 Physical security

The qualified electronic timestamp system that Aruba PEC offers to its account holders is based on front-end web servers that manage transactions with customers, the authentication, accounting and archiving of qualified electronic timestamps, and on back-end servers that deal with creating qualified electronic timestamps and managing the devices that acquire and synchronise the time references.
The qualified electronic timestamp servers are hosted in technical rooms to which access is controlled by means of security passes and/or biometric systems.
Only authorised personnel are able to access these rooms. These environments are also protected from flooding and fires by special devices (sensors, sprayers, air conditioning, etc.) and the computers are powered by a dedicated electricity supply, backed up with an uninterruptible power supply.

4.3.3.2 Software security

The front-end and back-end servers for the qualified electronic timestamp system interact with each other via secure communication protocols and can only be activated by authorised operators.
In particular, the back-end servers sign the qualified electronic timestamps using a cryptographic hardware device (or "signature device") of the highest quality and security. The signature algorithm used is RSA with a key length of 2048 bits which is used exclusively for the qualified electronic timestamp service. The RSA key pair is generated within the signature device. The private key of the pair is used in the signature device. The signature device can only be activated by a specially authorised operator who has the necessary keyword. The key pair and corresponding certificates will be replaced at least every three months.

4.4 Procedure for using the qualified electronic timestamp verification system

Thanks to an internal software verification procedure, Aruba PEC has qualified the applications that it provides to its customers and which allow them to verify the qualified electronic timestamps added to electronic documents in the form of PKCS#7/CAdES, PAdES and XAdES “cryptographic envelopes”. These applications make it possible to check:

1. The integrity of the document to which the qualified electronic timestamp is added;
2. The authenticity and reliability of the qualified electronic timestamp;
3. The date and time when the qualified electronic timestamp was associated with the electronic document.

Summary of the action taken by the user:

1. Launch the signature and verification application
2. Select the VTEQ verification function.
3. Select the file
4. The software requires an Internet connection, as it will attempt to access CRL and/or OCSP
5. The software shows a video of the result of the verification. The content of the file can be read using programs suitable for that file's format (for example: PDF files can be read with Acrobat Reader).

The qualified electronic timestamp verification products provided by Aruba PEC comply with the provisions of art. 42, paragraphs 2 and 6 of the DPCM and the requirements of paragraph 5 of Resolution no. 121/2019 [7].

The user must remember that certain file formats allow the addition of executable code (macros or commands) to the electronic document without changing its binary structure, in order to activate functions that may change actions, data or facts represented in that document (Art. 4, paragraph 3 of the DPCM [2]).
Although they are subject to qualified electronic timestamps, those files do not have the same effects as those described in article 21, paragraph 2 of the CAD [6].
The user alone has responsibility for using the standard functions for each product, to ensure that this condition is satisfied.

4.5 Service availability

The service is made available 24 hours a day, every day of the week, including holidays, via the secure HTTPS protocol in accordance with the formats and specifications defined in RFC 3161. The technology infrastructure, illustrated in the figure below, shows how there is no Single Point Of Failure (SPOF) and the system ensures that a very high level of service is achieved.

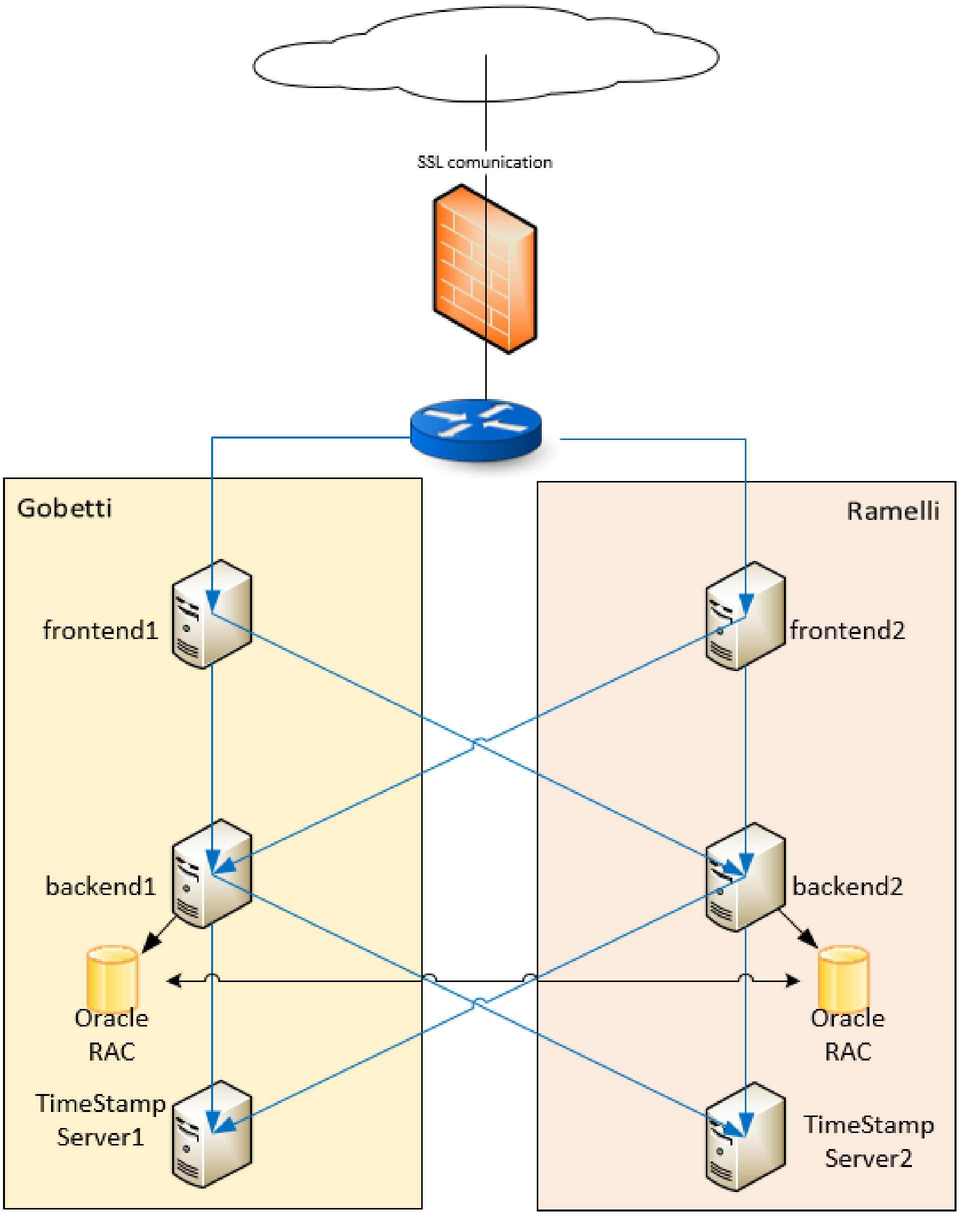

Figure 1 – infrastructure

The front-end and back-end servers are part of virtual atmospheres installed at the two Data Centres in Arezzo (IT1-IT2) and are set up online/with online balancing so that they can perform the twofold task of load balancing and business continuity in the event of a hardware or software failure.

Both the front-end servers are able to query the two back-end servers, which in turn are able to query both the servers responsible for adding the Timestamp.

The records present in the OracleRAC database at the two data centres make it possible to authenticate and keep track of timestamp requests.

The Timestamp Servers, on the other hand, are physical, so that they can host the PCI Thales Solo+ HSMs which are chosen because they are able to manage around 100 times the expected workload.

The HSMs that have been chosen also have a manufacturer's declared Mean Time Between Failure (MTBF) of 1,105,978 hours.

4.6 Retention of logs

Aruba PEC retains the logs (electronic records) of the timestamps issued for 30 years unless a specific contractual agreement establishes a different period, but always greater than or equal to the 20 years provided for by law.

4.7 TSA Termination Plan

The following is a description of the action that will be taken if, for any reason, the company decides to terminate the timestamp service, or to terminate its own TSA activities.

Before termination of the service:

- At least 60 days before the scheduled termination date, a message will be sent to all customers of the TSA service (or other services that include the TSA services) and to the national Supervisory Body and the Conformity Assessment Body.
- Again giving 60 days' notice, information will also be published in a prominent place on the TSA website, so that Relying Parties are also aware of this.
- Again giving 60 days' notice, the TSA will send a message to all subcontractors, informing them that, after the deadline, they will no longer be authorised to perform activities associated with the issuing of timestamps.
- Responsibility for storing evidence (timestamps, audit logs, etc.) will be contractually transferred to another trustworthy entity that is able to guarantee their retention for a period of at least 20 years. Responsibility for publishing the terminated public TSA key on its website, as well as for maintaining the CRL's URL, will also be transferred to that entity.
- A plan will be adopted for destroying the private timestamp keys as well as the associated cryptographic material (if any) needed for recovery.

On the termination date:

- The private timestamp keys, as well as the associated cryptographic material (if any) needed for recovery, which records the operation, will also be destroyed (by logical deletion).
- The certificates for all the TSUs belonging to the terminated TSA will be revoked.

5 GENERAL TERMS AND CONDITIONS

This chapter presents the general terms and conditions of this Operating Manual that have not been covered in other sections.

5.1 Users' Obligations

For the sole purpose of verifying qualified electronic timestamps, the user has the following obligations:

- To understand the scope of use of qualified electronic timestamps, and any associated limitations; the limitations applying to the Certifier's liability and indemnification, as described in the Certifier's Operating Manual;
- To verify the validity of the electronic document with which a qualified electronic timestamp is associated;
- To verify the data in the qualified electronic timestamp and, in particular, that matching the data provided in this Operating Manual. To ensure that the qualified electronic timestamp has been correctly signed by the trust service provider and that the private key used for this signature has not been compromised before the point at which the timestamp was added;
- To take all appropriate organisational and technical measures to avoid causing harm to others;
- To understand and comply with all precautionary measures outlined in this Operating Manual and any other agreements with the trust service provider, including limitations applying to liability and compensation.

5.2 Invalidity or non-applicability of clauses

If, for any reason and to any extent, any of the provisions of this Operating Manual, or its corresponding application, is found to be invalid or unenforceable, the rest of this Operating Manual (as well as the application of the invalid or unenforceable provision to other individuals or in other circumstances) will remain valid, and the invalid or unenforceable provision will be interpreted as closely as possible to the parties' intentions.

5.3 Interpretation

Unless otherwise specified, this Operating Manual must be interpreted in good faith, in accordance with what is deemed fair and reasonable, in line with the applicable Italian and European legislation and international commercial usage.

5.4 No waiver

The failure of any party to enforce any provision of this Operating Manual will not be regarded as a waiver of the future application of that provision or of any other provision.

5.5 Communications

If any person wishes or is required to communicate, ask or request anything in relation to this Operating Manual that communication must be sent to the following address by PEC [certified] email: direzione.ca@arubapec.it, or in writing.

Written communications must be delivered by a postal service that provides confirmation of delivery, or by a standard guaranteed service, registered mail with confirmation of delivery, addressed as follows: Aruba PEC S.p.A.: Via Sergio Ramelli, 8 – 52100 Arezzo.

5.6 Headings and Annexes of this Operating Manual

The headings, sub-headings and other titles in this Operating Manual are provided only for convenience and reference, and must not be used in the interpretation or application of any provision contained herein. The annexes, including the definitions provided in this Operating Manual, are an integral and binding part hereof for all intents and purposes.

5.7 Changes to the Operating Manual

General Changes

Aruba PEC S.p.A. reserves the right to update this Operating Manual periodically, for future application and not retroactively.

The changes will replace any provision that is in conflict with the reference version of the Operating Manual.

5.8 Breaches and other material damage

Users of the service covered by this manual declare and guarantee that their submission to the qualified TSP (Aruba PEC) and the use of information relating to their request for the qualified electronic timestamp service do not interfere with or harm the rights of any third party in any jurisdiction regarding trademarks, service marks, trade names, corporate names, or any other intellectual property right, and that they will not attempt to use the service for illegal purposes, including unlawful interference to the company's contractual or potential advantage, unfair competition, actions intended to damage the reputation of another person, misleading advertising, and actions that create confusion about individuals or legal entities.

Users of the service covered by this manual agree to hold the qualified TSP (Aruba PEC) harmless and to compensate it for any loss or damage resulting from such interference or breach.

5.9 Applicable Rules

The qualified trust services covered by this Operating Manual are governed by the legal provisions of the Italian and European Union legislative system.

The aim is to ensure uniform treatment and mutual recognition within the Community's legislative system.

5.10 Jurisdiction

For any legal disputes in which Aruba PEC S.p.A is the plaintiff or defendant in connection with use of the certification service, the operating procedures and application of the provisions of this Manual, the Courts of Arezzo will have sole jurisdiction, to the exclusion of any other competent court and to the exclusion of circumstances in which the law allows for the jurisdiction of the consumer's court.

(END OF DOCUMENT)