Certification Practice Statement

TIMESTAMPING

Timestamping Service · Regulation (EU) 910/2014

Version 1.10

Aviva Voice Systems & Services, SL
Calle Golfo de Salónica, 27, Oficina 5ºB | 28033 Madrid, España
Teléfono: (+34) 91 233 90 82 | info@avivavoice.com
https://www.avivavoice.com

General Information

Documentary Control

Security Classification:	**Public**
Version:	**1.10**
Edition Date:	**30/09/2026**
Fichero:	**AVIVA_DPC_TSA_EN_v1.r10**

Formal State

Prepared by:	Reviewed by	Approved by:
Nombre: Jesús Maestre Fecha: 30/09/2026	Nombre: José Fernández Fecha: 30/09/2026	Nombre: José Gómez Fecha: 30/09/2026

Versions Control

Version	Changes	Description of Change	Author of Change	Date of Change
1.1	Original	Document Creation	Alejandro Grande	03/09/2021
1.2	Sin Cambios	Revisión anual	Luis Fernández	26/10/2023
1.3	Sin Cambios	Revisión anual	Luis Fernández	10/10/2024
1.4	Servicios de Certificación	Actualización norma ISO	José Fernández	26/02/2025
1.5	1.3.1 1.3.3.1. 1.3.5.1	Se adiciona a la DPC TSA la jerarquía de la que depende el servicio. Se incluyen las obligaciones de los suscriptores de acuerdo con los términos y condiciones de TSA. Se añaden las obligaciones relativas al proveedor de Servicios de Infraestructura.	Raquel Fernández	01/10/2025

Version	Changes	Description of Change	Author of Change	Date of Change
	6.1.8	Inclusión de los detalles respecto a los algoritmos hash utilizados en el servicio.		
1.6	Servicios de Certificación	Actualización norma ISO	José Fernández	26/02/2025
1.7	1.3.1 1.3.3.1. 1.3.5.1 6.1.8	Se adiciona a la DPC TSA la jerarquía de la que depende el servicio. Se incluyen las obligaciones de los suscriptores de acuerdo con los términos y condiciones de TSA. Se añaden las obligaciones relativas al proveedor de Servicios de Infraestructura. Inclusión de los detalles respecto a los algoritmos hash utilizados en el servicio.	Raquel Fernández	22/09/2025
1.8	1.3.1 1.3.2 6.1 6.1.4	Adaptación de contenido y reformulado de la DPC para reflejar el formato de RFC 3647 Se añade la jerarquía específica vinculada al servicio de sellado de tiempo de BTP. Se llevan a cabo las modificaciones relativas a la longitud de claves de 3072 bits vinculada al certificado de sellado de tiempo de BTP.	Raquel Fernández	15/10/2025
1.9	6.1.4 6.1.6	Se modifican los apartados para que incluyan la nueva longitud de clave 3072 bits.	Raquel Fernández	11/11/2025
1.10	Sin cambios	Revisión anual	José Fernández	30/09/2026

INDEX

General Information 2

Documentary Control 2
Formal State 2
Versions Control 2

INDEX 4

1. Introduction 9

1.1 Presentation 9
1.2 Document Name and Identification 9
1.3 Participants in The Certification Services 9
1.3.1. Certification Service Provider 9
1.3.2. Time Stamping Authority 10
1.3.2.1. Uanataca CA Root 2016 10
1.3.2.2. UANATACA CA 1 2021 10
1.3.2.3. AVIVA VOICE QUALIFIED TSU01 10
1.3.2.4. AVIVA VOICE QUALIFIED TSU02 10
1.3.3. Subscriber of the certification service 11
1.3.3.1 Subscriber of the certification service 11
1.3.4. Relying Parties 11
1.3.5. Service Provider of the Technological infrastructure 11
1.3.5.1 Certification Service Subscribers 12
1.4 Use Of Timestamping Service 13
1.4.1. Permitted Uses 13
1.4.2. Prohibited Uses 13
1.5 Policy Management 13
1.5.1. Organization that administers the document 13
1.5.2. Contact Information of the Organization 13
1.5.3. Document management procedures 13

2. Publication and Preservation 14

2.1 Time Stamp Preservation 14
2.2 Publication of Information of the Certification Services Provider 14
2.3 Frequency of Publication 14
2.4 Access Control 14

3. Identification and Authentication 16

3.1 Initial Registration 16
3.1.1. Type of Names 16
3.1.2. Meaning of the Names 16
3.1.3. Use of anonymous and pseudonymous 16
3.1.4. Interpretation of name formats 16
3.1.5. Uniqueness of names 16
3.2 Initial Identity Validation 16

3.3 Identification and Authentication of Renewal Requests 16
3.4 Identification and Authentication of Revocation, Suspension or Reactivation Request 16

4. Operational Requirements 18

4.1 Requests for Time Stamp 18
4.1.1. Legitimation to apply for the issuance 18
4.1.2. Registration Procedure and Responsibilities 18
4.2 Processing the Request 18
4.3 Time Stamp Issue 18
4.4 Certificate Delivery and Acceptance 19
4.5 Key Pair and Certificate Usage 19
4.6 Certificate Modification 19
4.7 Revocation, Suspension or Reactivation of certificates 19
4.7.1. Causes of Certificate Revocation 19
4.7.2. Reasons for suspension of certificates 20
4.7.3. Reason for reactivation of certificates 20
4.7.4. Who can request the revocation, suspension or reactivation 20
4.7.5. Procedures for revocation, suspension or reactivation request 20
4.7.6. Temporary period of revocation, suspension or reactivation application processing 20
4.7.7. Obligation to consult certificate revocation or suspension information 21
4.7.8. Frequency of issuance of certificate revocation lists (CRLs) 21
4.7.9. Maximum period of publication of CRLs 21
4.7.10. Availability of the service checking in line with the state of the certificates 21
4.7.11. Obligation to check the consultation certificate status service 22
4.7.12. Special Requirements in case of compromise of the private key 22
4.8 Completion of the Subscription 22
4.9 Deposit and Recovery of Keys 22
4.9.1. Policies and practices of deposit and key recovery 22
4.9.2. Policy and practices of encapsulation and recovery of key session 22

5. Physical Security Controls, Management and Operations 23

5.1 Physical Security Controls 23
5.2 Location and Construction of Facilities 23
5.2.1. Physical Access 24
5.2.2. Electrical Power and Air Conditioning 24
5.2.3. Exposure to water 24
5.2.4. Fire prevention and protection 24
5.2.5. Backup Storage 25
5.2.6. Waste Management 25
5.2.7. Offline Backup 25
5.3 Procedure Controls 25
5.3.1. Trust Roles 25
5.3.2. Identification and authentication for each role 26
5.3.3. Roles requiring separation of task 26
5.4 Personnel Controls 26
5.4.1. History, qualification, experience and authorization requirements 26
5.4.2. Procedures of history investigation 27

5.4.3. Training requirements 27
5.4.4. Retraining frequency and requirements 28
5.4.5. Job rotation frequency and sequence 28
5.4.6. Sanctions and authorized action 28
5.4.7. Professional contracting requirements 28
5.4.8. Documentation supplied to personnel 28
5.5 Security Audit Procedures 28
5.5.1. Types of recorded events 28
5.5.2. Frequency of processing Audit Logs 30
5.5.3. Period of retention of audit logs 30
5.5.4. Audit logs protection 30
5.5.5. Audit log backup procedures 30
5.5.6. Location of the audit logs storage system 31
5.5.7. Notification of the audit event to the subject that caused the event. 31
5.5.8. Vulnerability analysis 31
5.6 Information Files 31
5.6.1. Retention period for the files 31
5.6.2. Protection of the file 31
5.6.3. File Backup procedures 31
5.6.4. Requirements of timestamping 32
5.6.5. Location of the file system 32
5.6.6. Procedures to obtain and verify file information 32
5.7 Key Renewal 32
5.8 Compromised Key and Disaster Recovery 32
5.8.1. Management procedures of incidents and compromise 32
5.8.2. Resources, applications or data corruption 32
5.8.3. Compromised private key of the entity 32
5.8.4. Business continuity capabilities after a disaster 32
5.9 Service Termination 33

6. Technical Security Controls 34

6.1 Generation and Installation of Their Pair Keys 34
6.1.1. Generation of the key pair 34
6.1.2. Sending of the public key to the certificate issuer 34
6.1.3. Public key distribution of the certification services provider 34
6.1.4. Key Sizes 35
6.1.5. Generation of public key parameters 35
6.1.6. Quality check of the public key parameters 35
6.1.7. Key generation in IT applications or in equipment goods 35
6.1.8. Hash Algorithms Used in the Service 35
6.2 Private Key Protection 36
6.2.1. Cryptographic modules standards 36
6.2.2. Private key multi-person (n of m) control 36
6.2.3. Private key backup 36
6.2.4. Private key transfer into a cryptographic module 36
6.2.5. Method of activating the private key 36

6.2.6. Method of deactivating the private key 36
6.2.7. Cryptographic modules classification 37
6.3 Computer Security Controls 37
6.4 Life Cycle Technical Controls 37
6.4.1. System development controls 38
6.4.2. Security management controls 38
6.4.2.1. Classification and management of information and goods 38
6.4.2.2. Management Operations 38
6.4.2.3. Treatment of support and safety 38
6.4.2.4. Planning Systems 38
6.4.2.5. Reports of incidents and response 39
6.4.2.6. Operational proceedings and Liabilities 39
6.4.2.7. Access system management 39
6.4.2.8. Life cycle management of cryptographic hardware 39
6.5 Network Security controls 40
6.6 Engineering controls of Cryptographic Modules 40
6.7 Time Sources 40
6.8 Electronic Qualified Time Stamp Time Accuracy 40
6.9 Change of State of a Qualified Signature Creation Device 41

7. TSU Certificate Profile 42

7.1 Certificate Profile 42
7.1.1. Version Number 42
7.1.2. Certificate extensions 42
7.1.3. Object Identifier (OID) of the algorithms 42
7.1.4. Names Format 42
7.1.5. Names Restriction 42
7.1.6. Object Identifiers (OID) of certificates types 42
7.2 Certificate Revocation List Profile 43
7.2.1. Version Number 43
7.2.2. OCSP profile 43

8. Compliance Audit 44

8.1 Frequency of Compliance Audit 44
8.2 Identification and Qualification of the Auditor 44
8.3 Auditor Relationship to Audited Entity 44
8.4 Topics Covered by Audit 44
8.5 Actions taken as a result of Lack of Conformity 44
8.6 Treatment of Audit Reports 45

9. Business and Legal Requirements 46

9.1 Fees 46
9.1.1. Timestamping service fees 46
9.1.2. Timestamping status information Access fees 46
9.1.3. Fees for other services 46
9.1.4. Refund Policy 46
9.2 Financial Capacity 46

9.2.1. Insurance coverage 46
9.2.2 Other assets 46
9.2.3. Insurance Coverage for subscribers and relying third parties in certificates 46
9.3 Confidentiality 46
9.3.1. Confidential Information 47
9.3.2. Legal disclosure of information 47
9.4 Personal Data Protection 47
9.5 Intellectual Property Rights 49
9.6 Obligations and Civil Liability 49
9.6.1. AVIVA Obligations 49
9.6.2. Guarantees offered to subscribers and relying third parties in certificates 50
9.6.3. Rejection of other guarantees 50
9.6.4. Limitation of liability 50
9.6.5. Fortuitous event and force majeure 51
9.6.6. Applicable Law 51
9.6.7. Severability, survival, entire agreement and notification clauses 51
9.6.8. Competent Jurisdiction Clause 51
9.6.9. Resolution of conflicts 51
Annex I – Acronyms 52

1. Introduction

1.1 Presentation

This document declares the certification practices for the service of issuing qualified electronic time stamps of Aviva Voice Systems and Services SL, hereinafter AVIVA, by making use of the public key infrastructure (PKI) of Uanataca, S.A.

1.2 Document Name and Identification

This document is the "AVIVA Time Stamping Certification Practices Statement".

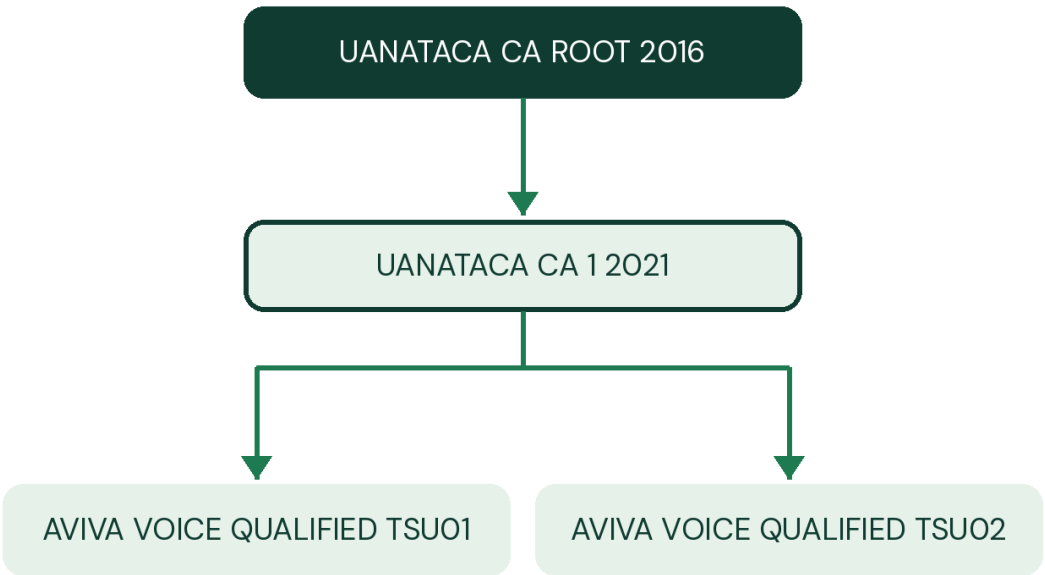
1.3 Participants in The Certification Services

1.3.1. Certification Service Provider

The electronic certification service provider (TSP / PSC) is the natural or legal person that provides one or more trust service. AVIVA is a trust service provider, acting in accordance with Regulation (EU) 910/2014 OF THE EUROPEAN PARLAMENT AND BOARD of 23rd July of 2014 related to the electronic identification and to the relying services for electronic transactions within the domestic market and repealing Directive 1999/93/CE, as well as the technical rules of the ETSI applicable to the issuance of qualified Time-Stamps, mainly the 319 421, in order to facilitate the legal requirements and international recognition of its services.

AVIVA is subject to annual Audit under the security standard ISO/IEC 27001:2022

For the provision of certification services, AVIVA VOICE has established a hierarchy of certification entities.



1.3.2. Time Stamping Authority

The Time Stamping Authority (TSA) is the trusted third party that provides the time stamping service. AVIVA is the trust service provider that provides the qualified time stamping service.

1.3.2.1. Uanataca CA Root 2016

This is the Root Certification Authority of the hierarchy that issues certificates to other certification entities, and whose public-key certificate is self-signed.

Identification data:

CN:	UANATACA ROOT 2016
Huella digital:	6d c0 84 50 a9 5c d3 26 62 c0 91 0f 8c 2d ce 23 0d 74 66 ad
Válido desde:	Viernes, 11 de marzo de 2016
Válido hasta:	Lunes, 11 de marzo de 2041
Longitud de clave RSA:	4.096 bits

1.3.2.2. UANATACA CA 1 2021

This is the Certification Authority within the hierarchy that issues certificates to end entities and electronic timestamp sealing certificates, and whose public-key certificate has been digitally signed by UANATACA ROOT 2016.

CN:	UANATACA CA1 2021
Huella digital:	a1 db ea 6c 10 7a a3 e8 1e 16 c9 af 8e 55 7f ed 3d 90 cf 98
Válido desde:	jueves, 3 de junio de 2021
Válido hasta:	sábado, 3 de junio de 2034
Longitud de clave RSA:	4.096 bits

1.3.2.3. AVIVA VOICE QUALIFIED TSU01

CN:	AVIVA VOICE QUALIFIED TSU 01
Huella digital:	1c f7 1f ac 43 dc f1 ee d1 89 17 7f f3 1d c4 d7 46 22 43 90
Válido desde:	miércoles, 3 de noviembre de 2021
Válido hasta:	unes, 5 de noviembre de 2029
Longitud de clave RSA:	2.048 bits

1.3.2.4. AVIVA VOICE QUALIFIED TSU02

CN:	AVIVA VOICE QUALIFIED TSU 02
Huella digital:	5d b4 de 83 c0 80 69 f0 c2 88 16 42 8a 6f c4 15 57 df 54 c1
Válido desde:	miércoles, 15 de octubre de 2025
Válido hasta:	lunes, 17 de octubre de 2033
Longitud de clave RSA:	3.072 bits

1.3.3. Subscriber of the certification service

The subscriber are the end users that receives the timestamps issued by AVIVA. The subscribers of the certification services are:

- Companies, entities, corporations and organizations that acquire them from AVIVA for its use in its business or organizational corporate level and which have been identified in the certificates.

- Natural persons that acquire the certificates for themselves and they have been identified in the certificates.

The subscriber of the trust service is the client of the Trust Service Provider.

1.3.3.1 Subscriber of the certification service

The subscriber undertakes to:

- Submit requests for qualified electronic time stamps in accordance with the procedure and, if necessary, using the technical components provided by AVIVA VOICE, in compliance with the provisions set forth in the Certification Practice Statement (CPS) and the COMPANY's documentation.

- Follow the instructions specified in AVIVA VOICE's TSU certificate PDS.

- Verify the electronic signatures of the electronic time stamps, including the validity of the certificate used.

- Use the electronic time stamps within the limits and scope described in this CPS and PDS.

1.3.4. Relying Parties

The relying parties are the persons and organizations that receive the qualified time stamps.

To trust certificates, the relying parties must verify them, as it is established in the certification practice statement.

1.3.5. Service Provider of the Technological infrastructure

AVIVA and UANATACA, S.A. have signed a contract for the provision of technology services in which UANATACA will provide the public key infrastructure (PKI) that supports the trust service of AVIVA. UANATACA makes available to AVIVA the technical personnel necessary for the correct performance of the reliable functions of a Trusted Service Provider.

UANATACA is the provider of Infrastructure services for certification services, provides its technological services to AVIVA so that it can carry out the services inherent to a Trusted Services Provider, always guaranteeing the continuity of services in the conditions and under the requirements demanded by the regulations.

UANATACA is a Trusted Service Provider accredited in accordance with the provisions of 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 and repealing Directive 1999/93/EC.

The PKI of UANATACA is subject to annual audits for the evaluation of the conformity of qualified providers of trust services according to the applicable regulations, under the norms:

a) ISO/IEC 17065:2012

b) ETSI EN 319 403

c) ETSI EN 319 421

d) ETSI EN 319 401

e) ETSI EN 319 411-2

f) ETSI EN 319 411-1

Also, UANATACA's PKI is subject to annual Audit under the security standards:

a) ISO 9001:2015

b) ISO/IEC 27001:2022

1.3.5.1 Certification Service Subscribers

The Public Key Infrastructure (PKI) Provider undertakes to make available to AVIVA VOICE the necessary technology services for the provision of certification services. In this regard:

• The provider shall have the necessary hardware to ensure that the aforementioned services are delivered with the levels of security required by the applicable regulations for such purposes.

• The provider shall have the necessary software to ensure that the aforementioned services are delivered with the levels of security required by the applicable regulations for such purposes.

• The provider shall guarantee the custody and hosting of the systems (hardware and software) in a Data Processing Center (Data Center) with appropriate logical and physical security levels, in accordance with generally accepted international standards.

• The provider shall be responsible for providing third-level technical support, meaning it shall provide technical assistance for issues that exceed AVIVA VOICE's management capacity and that are directly related to the definitions and/or technical failures of the technological infrastructure.

• In the provision of services to AVIVA VOICE, the provider shall make available the necessary technical personnel for the operation of the public key infrastructure, who will perform trusted roles dedicated to the administration and operation of the systems, specifically:

- PKI Security Officer
- Internal Auditor or Systems Administrator

- Systems Operator or CA Administrator
- CA Operator

1.4 Use Of Timestamping Service

1.4.1. Permitted Uses

The Time Stamping service issues time stamps in order to prove that a data has existed and has not been altered from a specific moment in time. The use of the time stamping service is limited to the applications and / or systems of clients (individuals or legal entities) that have contracted these services.

The Time Stamping Services from AVIVA are identified with OID: 1.3.6.1.4.1.46916.2

1.4.2. Prohibited Uses

The Time Stamping Service will not be used for purposes other than those specified in this document. In the same way, the service should only be used in accordance with the applicable regulation.

1.5 Policy Management

1.5.1. Organization that administers the document

Aviva Voice Systems and Services SL
C/ Golfo de Salónica 27 5ª planta 28033 Madrid
+34 912339082
info@avivavoice.com

1.5.2. Contact Information of the Organization

Aviva Voice Systems and Services SL
C/ Golfo de Salónica 27 5ª planta 28033 Madrid
+34 912339082
info@avivavoice.com

1.5.3. Document management procedures

The documental and organization system of AVIVA guarantees, according to the existence and request of the corresponding procedures, the correct maintenance of this document and the specification of the service related to itself.

2. Publication and Preservation

2.1 Time Stamp Preservation

AVIVA safely store all time stamps generated for at least 15 years. Likewise, it has a published deposit, where all the information related with the time stamping service is stored.

That service is available 24 hours, 7 days per week and, in case of the system failure was under AVIVA's control, it will make its best efforts to ensure that the service is back available according with established deadlines and procedures with respect the business continuity plan.

2.2 Publication of Information of the Certification Services Provider

AVIVA publishes the following information, in its Deposit:

- The Certification Practice Statement for time stamping service.
- Policy disclosure statements (PDS).
- The public key of the TSU certificate.
- References to the validation service of Time Stamps.

2.3 Frequency of Publication

The information of the certification services provides, including the policies and the Certification Practice Statement, is published when available.

The changes on the Certification Practice Statement shall be governed by the established in the change management procedure and in accordance with the applicable regulations.

2.4 Access Control

AVIVA does not limit the read access to the information established in the section 2.2, but establishes controls to prevent non-authorized people to add, modify or delete registrations of the Deposit, to protect the integrity and authenticity of the information.

AVIVA uses reliable systems for the Deposit, in such a way that:

- Only authorized persons could do annotations and modifications.
- The authenticity of the information could be verified.

- Any technical change affecting the security requirements could be detected.

3. Identification and Authentication

3.1 Initial Registration

3.1.1. Type of Names

All the certificates used in the Time Stamping provision, hereinafter "TSU Certificate", contain a distinguished name (DN) X.501 in the field Subject including a component Common Name (CN=).

The TSU Certificates are issued by Uanataca, S.A., hereinafter "UANATACA", these certificates are issued according to the article 38 and the Annex III of the 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 and repealing Directive 1999/93/EC and they are compliant with the technical regulations identified with the references ETSI EN 319 412-3, ETSI EN 319 421 y ETSI EN 319 422.

3.1.2. Meaning of the Names

The names in the fields of the certificates SubjectName and SubjectAlternativeName are understandable in natural language, in accordance with the provisions of the previous section.

3.1.3. Use of anonymous and pseudonymous

N/A

3.1.4. Interpretation of name formats

AVIVA is compliant with the requirements of the X.500 standard.

3.1.5. Uniqueness of names

The distinguished name of the TSU Certificates will be unique.

3.2 Initial Identity Validation

N/A

3.3 Identification and Authentication of Renewal Requests

N/A

3.4 Identification and Authentication of Revocation, Suspension or Reactivation Request

N/A

4. Operational Requirements

4.1 Requests for Time Stamp

4.1.1. Legitimation to apply for the issuance

The requester or user of the Time Stamping service, a natural or legal person, can make a request of a qualified time stamp by a direct request to AVIVA or through the available TSA server, which allow the time stamping of the documents.

The requester or user of the Time Stamping service can use their own application or software through the protocol defined in RFC 1361 and in accordance with ETSI 319 422, all by connecting to a web address and using credentials provided by AVIVA.

Once the request has been accepted, registered and the appropriate verifications have been done, the timestamp is issued and sent to the requester.

4.1.2. Registration Procedure and Responsibilities

AVIVA receives requests for the time stamping service, made by persons, entities, companies or organization of public or private law.

Applications are made directly through the AVIVA computer systems.

4.2 Processing the Request

The requester submits through the established procedures, the application of the time stamp for an electronic document directly to the time stamping service / server in charge of the sealing. First the petition shall be made, after the document shall be send to the corresponding web direction, after the documents will be duly sealed and returned.

4.3 Time Stamp Issue

The qualified time stamps are automatically issued through the system or server which is providing the time stamping service. After the approval of the time stamp request, the time stamp is issued securely and made available to the subscriber.

During the process, AVIVA:

- Protects the confidentiality and integrity of the registration data that owns.
- Uses reliable systems and products that are protected against every disturbance and guarantee the technical security and, in its case, cryptographic security of the processes of certification to which they support.
- Indicates the date and hour in which a time stamp was issued.

4.4 Certificate Delivery and Acceptance

The delivery and acceptance of the TSU Certificates follow the processes and indications established in the Certification Practice Statements and the PDS of UANATACA as Certification Authority, all available on the website: www.uanataca.com.

4.5 Key Pair and Certificate Usage

The TSU Certificate is exclusively used for the service of issuing qualified electronic time stamps.

4.6 Certificate Modification

N/A

4.7 Revocation, Suspension or Reactivation of certificates

The revocation of a certificate means the definitive withdrawal of the certificate and it is irrevocable.

The suspension (or temporal revocation) of a certificate means the temporal withdrawal of it and it is reversible. Only end entity certificates will be able to be stopped.

The reactivation of a certificate is the transition from a hold status to an active state.

The procedures for revocation, suspension and reactivation of the TSU Certificates follow the processes and indications established in the Certification Practice Statements and the PDS of UANATACA, all available on the website: www.uanataca.com.

4.7.1. Causes of Certificate Revocation

AVIVA will revoke the TSU Certificate when any of the following causes occur:

1. Circumstances affecting the information contained in the certificate:
    a. Modification of any of the data contained in the certificate, after the corresponding issue of the certificate including amendments.
    b. Discovery that any of the data contained in the certificate application is incorrect.
    c. Discovery that any of the data contained in the certificate is incorrect.
2. Circumstances affecting the security of the key or certificate:
    a. Compromise of the private key, infrastructure or systems certification service provider that issued the certificate, provided that it affects the reliability of the certificates issued from that incident.
    b. Infringement, by AVIVA, of the requirements of the certificate management

procedures established in this Certification Practice Statement.

c. Compromise or suspected compromise of the security key or certificate issued.

d. Unauthorized access or use, by a third-party private key corresponding to the public key contained in the certificate.

3. Other circumstances:

a. Termination of Certification Service of AVIVA.

b. The use of the certificate that is harmful and continued to AVIVA. In this case, it is considered that a use is harmful in terms of the following criteria:

i. The nature and number of complaints received.

ii. The identity of the entities filing complaints.

iii. The relevant legislation in force at all times.

iv. The response of the subscriber or of the person identified in the certificate to complaints received.

4.7.2. Reasons for suspension of certificates

TSU Certificates can be suspended if a key compromise is suspected, until it is confirmed. In this case, AVIVA must ensure that the certificate is not suspended for longer than necessary to confirm its compromise.

4.7.3. Reason for reactivation of certificates

The TSU Certificates can be reactivated.

4.7.4. Who can request the revocation, suspension or reactivation

The revocation, suspension or reactivation will be requested by AVIVA.

4.7.5. Procedures for revocation, suspension or reactivation request

The procedures for revocation, suspension or reactivation of the TSU Certificates follow the processes and indications established in the Certification Practice Statements and the PDS of UANATACA, all available on the website: www.uanataca.com.

4.7.6. Temporary period of revocation, suspension or reactivation application processing

The temporary period of revocation, suspension or reactivation application processing follow the processes and indications established in the Certification Practice Statements and the PDS of UANATACA, all available on the website: www.uanataca.com.

4.7.7.Obligation to consult certificate revocation or suspension information

Third parties should check the status of those time stamp in which they wish to rely, to do this they shall check the status of the TSU Certificate. A method by which you can check the TSU certificate is by consulting the latest Certificate Revocation List issued by UANATACA.

The Certificate Revocation Lists are published in the Deposit of UANATACA and, as well as the following web addresses indicated in certificates:

- Certification Authority Subordinate - UANATACA CA1 2021

- http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
- http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl

The status of the certificate validity can also be checked by the OCSP protocol.

- http://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

4.7.8. Frequency of issuance of certificate revocation lists (CRLs)

UANATACA issues a CRL at least every 24 hours.

The CRL indicates the scheduled time of issuance of a new CRL, although it may issue an CRL before the deadline stated in the previous CRL, to reflect revocations.

The CRL is obliged to maintain the revoked or suspended certificate until it expires.

4.7.9. Maximum period of publication of CRLs

The CRLs are published in the Deposit within a reasonable period immediately after their generation, which in any case is no more than a few minutes.

4.7.10. Availability of the service checking in line with the state of the certificates

Alternatively, third parties who rely on the Time Stamps issued by AVIVA may consult UANATACA deposit certificates, which is available 24 hours 7 days a week on the web:

- https://www.uanataca.com/public/pki/crtlist

To check the latest CRL issued in each CA, the following may be downloaded:

- Certification Authority (CA) Intermediate 1 - UANATACA CA1 2021
  - http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
  - http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl

4.7.11. Obligation to check the consultation certificate status service

It is mandatory to check the status of the TSU certificates before relying on the Time stamps issued by AVIVA.

4.7.12. Special Requirements in case of compromise of the private key

The compromise of the private key of TSU Certificate of AVIVA is notified to all participants in certification services, as far as possible, by posting this in the website and, if deemed necessary, in other media, even on paper.

4.8 Completion of the Subscription

N/A

4.9 Deposit and Recovery of Keys

4.9.1. Policies and practices of deposit and key recovery

N/A

4.9.2. Policy and practices of encapsulation and recovery of key session

N/A

5. Physical Security Controls, Management and Operations

5.1 Physical Security Controls

AVIVA provides the trust services through the public key infrastructure of UANATACA, which has established physical and environmental security controls to protect the resources of the facilities where the systems are located, the systems and the equipment used for the operations for the provision of trustworthy electronic services.

Specifically, the security policy applicable to the trust electronic services has established requirements for the following contingencies:

- Physical access controls.
- Protection against natural disasters.
- Protective measures against fires.
- Failure of the support systems (electronic energy, telecommunications, etc.)
- Collapse of the building.
- Flooding.
- Antitheft protection.
- Unauthorized removal of equipment, information, media and applications relating to components used for the services of the service provider certification.

These measures are applicable to installations where the trust services are provided, which lends from its both mainstream and, where appropriate, operating in contingency high security installations that are properly audited periodically.

Facilities include preventive and corrective maintenance systems with assistance 24/7 all year round with assistance in the following 24 hours notice.

5.2 Location and Construction of Facilities

The facilities that make up the AVIVA Public Key Infrastructure are located in a rack / cabinet physically isolated from the rest of the infrastructure hosted at the Data Processing Centre of the technology service provider ADAM Ecotech (hereinafter ADAM), located in Barcelona, Spain.

Physical protection is achieved by creating clearly defined security perimeters around services. The quality and strength of building materials facility ensures adequate levels of protection against intrusion by brute force and located in an area of low risk of disasters and allows quick access.

The room where the cryptographic operations are performed in the Data Processing Centre has redundancy in its infrastructure, as well as several alternative sources of power and cooling in an emergency.

Facilities are available to physically protect the provision of services approval of applications for certificates and revocation management, compromise caused by unauthorized access to systems or data access and disclosure thereof.

5.2.1. Physical Access

There are three levels of physical security (building entrance where the CPD is found, access to the room of the CPD and access to the rack) for service of protecting the certificate generation and must be accessed from the lower to the upper levels.

Physical access, where certification is processed, is limited and protected by a combination of physical and procedural measures are carried out as such:

- Limited to expressly authorized persons, with identification at the time of access and registration thereof, including filming by CCTV.
- Access to the rooms is done with ID card readers and managed by a computer system that keeps a log of inputs and outputs automatically.
- To access the rack where the cryptographic processes are located, prior authorization is necessary to have the key to open the cage.

5.2.2. Electrical Power and Air Conditioning

The facilities have current-stabilising equipment and power system doubled with generator equipment.

The rooms housing IT equipment have temperature control systems with air conditioners.

5.2.3. Exposure to water

The facilities are located in an area of low risk of flooding.

The rooms where computers are housed have a moisture detection system.

5.2.4. Fire prevention and protection

The facilities and assets have automatic detection and firefighting systems.

5.2.5. Backup Storage

Only authorized individuals have access to support storage.

The most highly classified information is stored in a safe offsite Data Processing Centre.

5.2.6. Waste Management

The elimination of media, both paper and magnetic, is made by mechanisms that guarantee the impossibility of retrieving information.

In the case of magnetic media, it proceeds to formatting, permanent deletion, or physical destruction of the support. For paper documents, paper shredders or specially arranged bins for later destruction are used, under supervision.

5.2.7. Offline Backup

It is available a secure external storage for the safekeeping of documents, magnetic and electronic devices that are independent of the operations center.

5.3 Procedure Controls

It is guaranteed that its systems are operated safely, for which it has establish and implemented procedures for the functions which affect the supply of its services.

The staff runs the administrative and management procedures according to the security policy procedures.

5.3.1. Trust Roles

It is identified, according with its security policy, the following trust functions and roles:

- Internal Auditor: Responsible for compliance with operating procedures. This is an external person to the Department of Information Systems. The tasks of Internal Auditor are incompatible in time with tasks and incompatible with Certification Systems. These functions will be subordinate to the head of operations, reporting both this technical direction.
- System Administrator: Responsible for the proper functioning of hardware and software support platform certification.
- System Operator: Responsible, together with the Systems Administrator, for the correct functioning of the hardware and software supporting the certification platform. The operator is responsible for backup procedures and maintenance of the daily operations of the systems.
- Security Manager: Responsible for coordinating, monitoring and enforcing security measures as defined by the security policies of UANATACA. This individual should be responsible for

aspects related to information security: logic, physics, networking, organization, etc.

Persons holding previous posts are subject to procedures of investigation and specific control. Additionally, it is applied a policy criteria for the segregation of duties, as preventive measure to fraudulent activities.

5.3.2. Identification and authentication for each role

The individuals assigned for each role are identified by the internal auditor will ensure that each person performs the operations for which they are assigned.

Each person only controls the assets required for its role, ensuring that no person access unallocated resources.

Access to resources is performed depending on the asset through cryptographic cards and activation codes.

5.3.3. Roles requiring separation of task

Trust roles are established under the principle of minimum privilege, ensuring a segregation of functions, so that the person holding a role does not have total or especially extensive control of all certification functions, ensuring due control and surveillance, limiting thus any type of fraudulent behavior internally.

The granting of the minimum privilege for trust functions will be done considering the best development of the activity and will be as limited as possible, considering the organizational structure at all times.

5.4 Personnel Controls

5.4.1. History, qualification, experience and authorization requirements

All staff is qualified and has been properly instructed to perform operations that they have been assigned.

Staff in positions of trust has no personal interests that conflict with the development of the role that has been entrusted.

In general, AVIVA withdraws an employee from their duties when knowledge of the existence of the commission of any criminal act that could affect the performance of its functions.

AVIVA does not assign to a reliable site management a person who is not suitable for the position, especially for having been convicted of a crime or minor affecting their suitability for the position.

For this reason, a previous investigation, to the extent permitted by applicable law, on the following is done:

- Studies, including alleged degree.
- Previous work up to five years, including professional references.
- Professional references.

5.4.2. Procedures of history investigation

Before hiring a person or before that person has access to the job, performs the following checks:

- References of the past years jobs
- Professional references
- Studies, including qualifications

AVIVA obtains the unequivocal consent of the affected to such previous research, and processes and protects all his personal data in accordance with General Data Protection Regulation and every national regulations applicable.

All checks are made up to be allowed by the applicable law. The reasons that may lead the candidate rejection of a job are the followings:

- Falsehoods on the job application, done by the candidate.
- Very negative professional references or not very reliable.

5.4.3. Training requirements

AVIVA trains the staff in reliable and management jobs, until they reach the required qualification, keeping reports of the training.

Training programs are updated and improved periodically.

Training includes, at least, the following contents:

- Principles and mechanisms of security of the certification hierarchy, and the user environment of the person to train.
- Tasks the person must do.
- Policies and security procedures of AVIVA. Use and operation of machinery and installed applications.
- Management and processing of incidents and security compromise.
- Procedures of business continuity and emergency.

- Process management and security regarding the processing of personal data.

5.4.4. Retraining frequency and requirements

AVIVA, updates the staff training in accordance with the needs, and with enough frequency to comply their functions in a competent and satisfactory way, especially when doing the substantial modifications in the certification tasks.

5.4.5. Job rotation frequency and sequence

N/A

5.4.6. Sanctions and authorized action

AVIVA has a disciplinary system, to debug the responsibilities arising from unauthorized actions, appropriate to the applicable labor legislation.

Disciplinary actions include suspension and loss of employment of the person responsible for the harmful action, proportionate to the gravity of the unauthorized action.

5.4.7. Professional contracting requirements

The staff hired to perform reliable tasks sign a previous confidentially agreement and the operational requirements used by AVIVA. Any action that may compromise the security of the accepted processes could, once evaluated, lead to the termination of the employment contract.

In case all or part of the certification services were performed by a third party, the previsions and controls performed in this section, or other parts of the Certification Practice Statement, will be applied and complied by the third party who performs the operation functions of the certification services, notwithstanding, the certification authority will be responsible in any case for the effective implementation. These aspects are concretized in the legal instrument used to arrange the certification services provision by a third party different tan AVIVA.

5.4.8. Documentation supplied to personnel

The certification services provider will provide the documentation strictly needed by the staff at any moment, to perform their job in a competent and satisfactory form.

5.5 Security Audit Procedures

5.5.1. Types of recorded events

It is produced and safely registered, at least, of the following events related to the entity security:

- Booting and shutting down of systems.

- Attempts to create, delete, set passwords or change privileges.
- Attempts to login and logout.
- Attempted unauthorized access to the TSA system through the network.
- Attempts of unauthorized access to the file system.
- Physical access to the logs.
- Changes in the configuration and maintenance of the system.
- Records of TSA applications.
- Turning on and off the TSA application.
- Changes in the details of the TSA and / or its codes.
- Records of the destruction of the media containing the keys, activation data.
- Events related to the life cycle of the cryptographic module, such as receiving, using and uninstalling it.
- The key generation ceremony and the key management databases.
- Physical access records.
- Maintenance and system configuration changes.
- Staff changes.
- Commitments and discrepancies reports.
- Records of the destruction of material containing key information, activation data or personal information of the subscriber, in case of individual certificates, or of the natural person identified in the certificate, in case of organization certificates.
- Complete reports of physical intrusion attempts in the infrastructures that support the service.
- Events related to synchronization and recalibration of the clock.

Log entries include the following elements:

- Login date and time.
- Serial number or entry sequence, in the automatic records.
- Identity of the entity entering in the register.
- Type of entrance.

5.5.2. Frequency of processing Audit Logs

It is reviewed its logs when a system alert motivated by the existence of any incident occurs.

Processing audit logs is a review of the records including the verification that confirm they have not been tampered, a brief inspection of all log entries and a deeper investigation of any alert or irregularities in the logs. The actions from the audit review are documented.

It is kept a system that guarantees:

- Enough space for logs storage.
- Logs files are not rewritten.
- Information held includes, at least: type of event, date and time, user running the event and result of the operation.
- Logs files will be held in structured files susceptible to incorporate into a DB for further exploration.

5.5.3. Period of retention of audit logs

It is held the logs information for a period of between 1 and 15 years, depending on the type of information recorded.

5.5.4. Audit logs protection

The systems logs:

- Are protected from manipulation by signing the files that contain them.
- Are stored in fireproof devices.
- Availability is protected through its storage in facilities out of the center where the CA is located.

Access to logs files is reserved only to authorized persons. Also, devices are handled at all times by authorized personnel.

There is an internal procedure where management processes devices containing the data of the audit logs are detailed.

5.5.5. Audit log backup procedures

There is a proper backup procedure so that, in case of loss or destruction of relevant files, were available in a short period of time the corresponding logs backup.

It is implemented a secure backup procedure of audit logs, making a copy of all logs weekly in an external source. Additionally, a copy is held in a custody external center.

5.5.6. Location of the audit logs storage system

The information of the audit events is collected internally and in an automated way by the operating system, network communications and software certificate management, in addition to the data generated manually, will be stored by the authorized personnel. All this composes the storage system of audit logs.

5.5.7. Notification of the audit event to the subject that caused the event.

When the log audit accumulation system records an event, it is not necessary to send a notification to the individual, organization, device or application that caused the event.

5.5.8. Vulnerability analysis

The audit processes cover vulnerability analysis. Vulnerability analysis must be run, reviewed and revised by an examination of these monitored events. This analysis must be run daily, monthly and annually in accordance with the internal procedure intended for this purpose.

Audit data systems are stored in order to be used in the investigation of any incident and to locate vulnerabilities.

5.6 Information Files

5.6.1. Retention period for the files

It is saved the mentioned logs above for at least 15 years, or the period defined in the current law.

5.6.2. Protection of the file

The file is protected so only the duly authorized persons can access to it. The file is protected against visualization, modification erased or any other manipulation through its storage in a reliable system.

It is ensured a proper protection of the files by assigning qualified personnel for its treatment and its storage in secure fireproof boxes and external facilities.

5.6.3. File Backup procedures

There is an external storage center to ensure the availability of the file backups of electronic files. The physical documents are stored in safe places restricted to authorized personnel.

At least, It is made incremental daily backups of support of all its electronic documents and makes weekly full backups for data recovery cases.

In addition, in cases where there is a need to keep a copy of the documents on paper, they are stored in a safe place.

5.6.4. Requirements of timestamping

Records are dated with a reliable source via NTP.

There is no need to sign this information digitally.

5.6.5. Location of the file system

It is available a centralized system of gathering information of the activity of the equipment involved in the certificate management service.

5.6.6. Procedures to obtain and verify file information

It is available a procedure where describes the process to verify that the stored information is correct and reachable. AVIVA provides the information and means of verification to the auditor.

5.7 Key Renewal

Each key pair of the TSU Certificates used for the time stamping service is associated with the system that provides such service. Prior to the use of the private key of the TSU certificate expire, a key change is made before the expiration or revision of the current ones.

5.8 Compromised Key and Disaster Recovery

5.8.1. Management procedures of incidents and compromise

It is developed security policies and business continuity, which allows the management and backup of the systems in case of compromise or disaster of its operations.

5.8.2. Resources, applications or data corruption

When resources, applications or data corruption events happen, the proper management procedures will begin, which contemplate scaling, investigation and response to the incident. Procedures of compromise of the keys or disaster recovery will begin, if necessary.

5.8.3. Compromised private key of the entity

In case of suspicion or knowledge of the compromise, key compromise procedures will be activated in accordance to the security policies, incident management and business continuity, which allow the recovery of the critical systems, and if necessary, in an alternative data center.

5.8.4. Business continuity capabilities after a disaster

It will be restored the critical services in accordance with the contingency and business continuity plan restoring the normal operation of the previous services within 24 hours of the disaster.

It is available an alternative center for the operation of certification schemes described in the business continuity plan, if necessary.

5.9 Service Termination

AVIVA ensures that possible interruptions to subscribers of the service and to third parties are minimal as a consequence of the cessation of the services of the certification service provider. In this sense, AVIVA guarantees a continuous maintenance of the defined records and for the time established in accordance with this Time Stamping Certification Practices Statement.

Notwithstanding the foregoing, if applicable, AVIVA will execute all actions necessary to transfer to a third party or a notarial repository, the maintenance obligations of the specified records during the corresponding period according to this Time Stamping Certification Practices Statement or the corresponding legal forecast.

Before the services cessation, AVIVA develops a termination plan, with the following provisions:

- Provide the necessary funds, including civil liability insurance, to continue the completion of the revocation activities.
- Inform all Subscribers of the service, Third party that they trust and, in general, any third party with whom they have agreements or other type of termination relationship with a minimum anticipation of 2 months.
- Destroy or disable for use the private keys in charge of the time-stamping service.
- Execute the tasks necessary to transfer the maintenance obligations of the registration information and the event log files during the respective time periods.
- Communicate to the corresponding Spanish Supervisory Body, at least 2 months in advance, the cessation of its activity.
- Likewise, it will inform you of the opening of any bankruptcy proceeding against AVIVA, as well as any other relevant circumstance that may prevent the continuation of the activity.

6. Technical Security Controls

In the provision of trust services, reliable systems and products are used, protected against any alteration and that guarantee the technical and cryptographic security of the certification, which are used as support.

6.1 Generation and Installation of Their Pair Keys

6.1.1. Generation of the key pair

The key pair of the TSU Certificate is generated by the Trust Service Provider Uanataca, S.A., in accordance with its Certification Practices Statement and its disclosure text, available on the website: https://web.uanataca.com.

Likewise, the key ceremony procedures have been followed, within the high security perimeter assigned to this task. The activities carried out during the key generation ceremony have been registered, dated and signed by all the individuals participating in it, with the presence of an Auditor. These records are kept for audit and monitoring purposes during an appropriate period determined by AVIVA.

For the generation of the key of the TSU certificate, devices with the certifications FIPS 140-2 level 3 and Common Criteria EAL4 + are used.

The keys are generated using the RSA public key algorithm, with a minimum length of 2048 bits

TSU certificates	2.048 bits	Up to 8 years

*Note: AVIVA VOICE will continue using its 2048-bit Timestamping Unit until December 31 2025, after which that Timestamping Unit will no longer be used. Consequently, it will switch to its 3072-bit Timestamping Unit.

6.1.2. Sending of the public key to the certificate issuer

The method of remission of the public key to the relying electronic certification services provider is PKCS#10, other equivalent cryptographic test or any other method approved by AVIVA.

6.1.3. Public key distribution of the certification services provider

AVIVA's keys are communicated to third parties who trust in certificates, ensuring the integrity of the key and authenticating its origin, through its publication in the Deposit.

Users can access to the Deposit to obtain the public keys, and additionally, in applications S/MIME, the data message may contain a chain of certificates, which are distributed to the users in this way.

The certificate of the CA root and subordinated will be available on the UANATACA web page.

6.1.4. Key Sizes

The length of the TSU Certificates keys are 2048 bits.

> *Note: AVIVA VOICE will continue using its 2048-bit Timestamping Unit until December 31 2025, after which that Timestamping Unit will no longer be used. Consequently, it will switch to its 3072-bit Timestamping Unit.

6.1.5. Generation of public key parameters

The TSU certificates public key are encrypted in accordance with RFC 5280.

6.1.6. Quality check of the public key parameters

- Module Length= 4096 bits

> *Note: AVIVA VOICE will continue using its 2048-bit Timestamping Unit until December 31 2025, after which that Timestamping Unit will no longer be used. Consequently, it will switch to its 3072-bit Timestamping Unit.

- Algorithm of keys generation: rsagen1
- Cryptographic functions of Summary: SHA256.

6.1.7. Key generation in IT applications or in equipment goods

All keys are generated in equipment goods, in accordance with the indicated in section 6.1.1.

6.1.8. Hash Algorithms Used in the Service

• Hash used on the data for which the timestamp will be generated:

o The identifier of the hash algorithm used to generate the evidence fingerprint. In this case, the permitted algorithms are:

- SHA-256 (secure hash algorithm, 256-bit, OID: 2.16.840.1.101.3.4.2.1)
- SHA-384 (secure hash algorithm, 384-bit, OID: 2.16.840.1.101.3.4.2.2)
- SHA-512 (secure hash algorithm, 512-bit, OID: 2.16.840.1.101.3.4.2.3)

• Timestamp signature algorithm:

o In this case, the algorithm used is RSA (SHA256rsa, OID: 1.2.840.113549.1.1.11).

6.2 Private Key Protection

6.2.1. Cryptographic modules standards

The modules that manage the keys of AVIVA are compliant with the certification FIPS 140-2 level 3 and Common Criteria EAL4+.

6.2.2. Private key multi-person (n of m) control

A multi-person control is required for activating the private key of the TSU Certificate. In case of this Certification Practice Statement, in detail there is a policy of 3 of 6 persons for the keys activation.

Cryptographic devices are physically protected, as determined in this document.

6.2.3. Private key backup

It is made a backup copy of the TSU certificate private key that makes their recovery in case of disaster, loss or deterioration thereof. Both generation of the copy and the recovery thereof need at least two people participation.

These recovery files are stored in fireproof cabinets and in the external custody center.

6.2.4. Private key transfer into a cryptographic module

Private keys are directly generated in the cryptographic modules in the public key infrastructure.

The private keys of the TSU Certificates are stored encrypted in the cryptographic modules of the public key infrastructure.

6.2.5. Method of activating the private key

The private key management procedures of the AVIVA's TSU Certificate is activated by executing the corresponding secure start procedure of the cryptographic module, by people who perform reliable functions.

6.2.6. Method of deactivating the private key

Before destroying the keys, a revocation of the certificate of the public keys associated with them will be issued.

Devices that have stored any part of AVIVA private keys are physically destroyed or reset to low level. For disposal, the same steps outlined in the corresponding manual of the cryptographic equipment are followed.

Finally, the backups will be destroyed in a safety way.

6.2.7. Cryptographic modules classification

See section 6.2.

6.3 Computer Security Controls

It is used reliable systems to provide certification services. It has made controls and computer audits to establish its proper computer activity management with the level of security required in the system management of electronic certification.

Regarding the information security, UANATACA as the Public Key Infrastructure provider applies the certification scheme controls on management systems ISO 27001.

Used equipment's are initially configured with appropriate security profiles of UANATACA staff system, in the following aspects:

- Setting up the operating system.
- Setting up the application security.
- Correct sizing of the system.
- User and permissions settings.
- Setting event Log.
- Backup and recovery plan.
- Antivirus settings.
- Requirements of network traffic.

Each server includes the following features:

- Imposition of separation of tasks for the management of privileges.
- Identification and authentication of roles associated with identities.
- Audit of events related to security.
- Key recovery mechanisms and the TSA system.

The exposed functionalities are realized through a combination of operating system, PKI software, physical protection and procedures.

6.4 Life Cycle Technical Controls

6.4.1. System development controls

The applications are developed and implemented in accordance with the development and change control standards.

The applications have methods for verifying the integrity and authenticity, as well as the correction of the version to use.

6.4.2. Security management controls

It is developed activities for training and employee awareness of security. The materials used for training and descriptive documents processes are updates after approval by a group for security management. An annual training plan is used.

It is required by contract security measures equivalent to any external provider involved in the certification tasks of the relying electronic service.

6.4.2.1. Classification and management of information and goods

There is an inventory of assets and documentation and a procedure for the management of this material to guarantee its use.

There is a security policy details the procedures of information management where it is classified according to its level of confidentiality.

The documents are classified into three levels: UNCLASSIFIED, INTERNAL USE and CONFIDENTIAL.

6.4.2.2. Management Operations

There is an appropriate process management and incident response, by implementing a warning system and the generation of periodic reports.

In the security document the incident management process is developed in detail.

AVIVA has documented all the procedure relative to the roles and responsibilities of the staff involved in the control and manipulation of elements contained in the certification process.

6.4.2.3. Treatment of support and safety

All supports are treated safely in accordance with the requirements of the classification of information. The supports that contain sensitive information are destroyed safely if they are not going to be required again.

6.4.2.4. Planning Systems

Systems department keeps track of the capabilities of the equipment. In conjunction with the implementation of resources control each system can provide a possible downsizing.

6.4.2.5. Reports of incidents and response

There is a procedure for follow-up of incidents and its resolution, where the answers and an economic evaluation are registered, which supposes the resolution of the incident.

6.4.2.6. Operational proceedings and Liabilities

It is defined activities assigned to persons with a role of trust, other than those responsible for performing daily operations that do not have character of confidentiality.

6.4.2.7. Access system management

It is made all efforts that are reasonable available to confirm that the system access is limited to authorized persons.

In particular:

- There are controls based on firewalls, antivirus and IDS in high availability.
- Sensitive data is protected by cryptographic techniques or access controls with strong identification.
- A data management procedure is taken into account.
- Procedures are in place to ensure that operations are respected in the role policy.
- Each person has a role to perform the certification operations.
- The staff is responsible for their actions through the commitment of confidentiality with the company.

6.4.2.8. Life cycle management of cryptographic hardware

AVIVA ensures that the cryptographic hardware used for signing certificates is not handled during its transport by inspecting the delivered material.

The cryptographic hardware moves on prepared supports to prevent any manipulation.

It is recorded all relevant device information to add to the catalogue of assets.

The use of cryptographic hardware for signature certificates requires the use of at least two trusted employees.

It is made periodic tests to ensure the correct functionality of the device.

Only reliable personnel manipulate the cryptographic hardware device.

AVIVA TSU Certificate private key stored in the cryptographic hardware will be erased once the device is removed.

The system configuration, as well as its modifications and updates are documented and controlled.

Changes or updates are authorized by the security officer and they are reflected in the corresponding team's working minutes. At least, two reliable persons perform these settings.

6.5 Network Security controls

There is protection to the physical access to network management devices and has an architecture that directs the traffic generated based on its features of security, creating clearly defined network sections. This division is performed with firewalls.

Confidential information is transferred through unsecured networks; it is performed in an encrypted way using SSL protocols or VPN system with dual factor authentication.

6.6 Engineering controls of Cryptographic Modules

Cryptographic modules are subject to engineering controls provided in the standards indicated along this section.

The key generation algorithms used are commonly accepted for the use of the key to which they are intended.

All cryptographic operations are performed in modules with FIPS 140-2 level 3 certification.

6.7 Time Sources

It is available a procedure of time synchronization coordinated via NTP, that has access to two independent services:

- The first synchronization is a service based on GPS antennas and receivers that allow a level of trust of STRATUM 1 (with two high availability systems).
- The second one has a complementary synchronization, via NTP, with the Spanish Royal Institute and Observatory of the Navy (ROA).

6.8 Electronic Qualified Time Stamp Time Accuracy

AVIVA's Qualified Time Stamping service is based on the use of the TSP protocol over HTTP, defined in the RFC 3161 standard "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

AVIVA has a reliable source of time in high availability that allows a confidence level of STRATUM 3, via NTP, with the CSUC.

The accuracy of the AVIVA Qualified Time Stamping service is 1 second with respect to UTC.

6.9 Change of State of a Qualified Signature Creation Device

In the case of modification of the status of the certification of the qualified signature creation devices (QSCD) that support the provision of trust services, the following procedure will be followed:

1. A list of certified QSCDs is available, as well as a close relationship with suppliers of said devices, in order to guarantee alternatives to possible loss of certification status of QSCD devices.

2. In the event of termination of the period of validity or loss of certification, said QSCDs will not be used for the provision of the time-stamping service.

3. Proceed immediately to change to QSCD devices with valid certification.

4. In the event that it is proven that a QSCD device has never been a qualified device, either by falsification or any type if fraud, it will proceed immediately to inform the clients and the national regulator about the revocation of the electronics certificates issued by these devices. Subsequently it will proceed to replace them by a valid QSCD device.

7. TSU Certificate Profile

The TSU certificate profile for the provision of the time stamp service follows the processes and indications established in the Certification Practice Statements (CPS) of UANATACA and its disclosure text (PDS), all available on the website: www.uanataca.com.

7.1 Certificate Profile

The TSU Certificates are compliant with the standard X.509 version 3, RFC 3739 and the ETSI EN 319 422.

7.1.1. Version Number

The certificate is X.509 Version 3.

7.1.2. Certificate extensions

Certificates extensions are detailed in the profile's documents, which are accessible from UANATACA's web (https://www.uanataca.com).

In this way, it is allowed to keep more stable versions of the Certification Practice Statement and decouple them from frequent adjustments in the profiles.

7.1.3. Object Identifier (OID) of the algorithms

The object identifier of the signature algorithm is:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

The object identifier of the public key algorithm is:

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4. Names Format

Certificates must contain the required information for its use, as determined by the appropriate policy.

7.1.5. Names Restriction

Los nombres contenidos en los certificados están restringidos a "Distinguished Names" X.500, que son únicos y no ambiguos.

7.1.6. Object Identifiers (OID) of certificates types

All certificates include an identifier of the certificates policy under which they have been issued.

7.2 Certificate Revocation List Profile

The procedure of revocation, suspension and / or reactivation of TSU certificates follow the processes and indications established in the Certification Practice Statement and Disclosure Text (PDS) of UANATACA, all available on the website: www.uanataca.com.

7.2.1. Version Number

CRLs issued by UANATACA are from version 2.

7.2.2.OCSP profile

According to standard IETF RFC 6960.

8. Compliance Audit

AVIVA has communicated the beginning of its activity as a trust service provider by the National Supervisory Body, currently the Ministry of Industry, Trade and Tourism, and is subject to the control reviews that this body considers necessary.

8.1 Frequency of Compliance Audit

AVIVA conducts a compliance audit annually, in addition to internal audits carried out at its own discretion or at any time, due to a suspected breach of any security measure.

8.2 Identification and Qualification of the Auditor

An external independent audit signature performs the audits, demonstrating technical competence and experience in computer security, information systems security and compliance audits of public key certification services and related elements.

8.3 Auditor Relationship to Audited Entity

Audit firms are of renowned prestige, with specialized departments in conducting IT audits, so there is no conflict of interest that could undermine its performance in relation to AVIVA.

8.4 Topics Covered by Audit

The Audit verifies with reference to AVIVA that:

1. The entity has a management system, which ensures the quality of service.
2. The entity complies with the requirements of the Certification Practice Statement and other documentation related to the issuance of the various digital certificates.
3. The Certification Practice Statement and other related legal documentation comply with the agreed with AVIVA and the established in the current regulation.
4. The entity properly manages its information systems.

8.5 Actions taken as a result of Lack of Conformity

Once the management has received the auditor's compliance report, the deficiencies found are analyzed with the audit entity. This report also develops and implements the corrective policies that tackle these deficiencies.

If AVIVA is unable to develop and/or implement the corrective measures or if the deficiencies found suppose an immediate threat to the system security or integrity, shall immediately inform to the security responsible which can perform the following actions:

- Cease operation temporarily.

- Revoke the TSU certificate key and regenerate the infrastructure.
- Terminate the TSA service.
- Other complementary actions needed.

8.6 Treatment of Audit Reports

The audit reports are delivered to the responsible team of the security in a timelimit of 15 days after the audit.

9. Business and Legal Requirements

9.1 Fees

9.1.1. Timestamping service fees

AVIVA can establish a fee for the time-stamping service, from which, if applicable, the subscribers will be informed in a timely manner.

9.1.2. Timestamping status information Access fees

AVIVA has not established any fee for access to status information for time stamps.

9.1.3. Fees for other services

Not Stipulated.

9.1.4. Refund Policy

Not Stipulated.

9.2 Financial Capacity

AVIVA has enough economic resources to keep its operations, to comply with its obligations and to confront the risk of liability for claim and damages, as established in the applicable regulation, in relation to the management of the services finalization and termination plan.

9.2.1. Insurance coverage

AVIVA has warranty coverage of its civil liability, with an insurance of professional civil liability that complies with the current regulation applicable.

9.2.2 Other assets

Not stipulated.

9.2.3. Insurance Coverage for subscribers and relying third parties in certificates

AVIVA has a warranty coverage of its civil liability, with an insurance of professional civil liability, for relying electronic services, with the minimum insured of 1,500,000 Euros.

9.3 Confidentiality

9.3.1. Confidential Information

The following information is kept confidential by AVIVA:

- The service requests, as well as any other personal information obtained for the provision of the service, except for the information indicated in the following section.
- Transaction records, including complete records and audit records of transactions.
- Internal and external audit records.
- Business continuity and emergency plans.
- Security plans.
- Documentation of operations, file, monitoring and other analogous.
- All other information identified as "Confidential".

9.3.2. Legal disclosure of information

AVIVA only discloses the confidential information in the cases legally foreseen.

9.4 Personal Data Protection

AVIVA is compliance with current regulations on the protection of personal data, as reflected in the General Data Protection Regulation No. 2016/679 and in general any applicable national regulations.

In compliance with, AVIVA has documented in this Certification Practice Statement the security and organizational aspects and procedures, in order to guarantee that all the personal data to which it has access are protected against its loss, destruction, damage, forgery and illegal or unauthorized processing.

The following is a detail of all the necessary information regarding the processing of personal data made by AVIVA:

Data Controller

The personal data given by reason of the Service would be treated by **Aviva Voice Systems and Services SL,** who is configured as the Data Controller and whose data are detailed here:
Aviva Voice Systems and Services SL

C/ Golfo de Salónica 27 5ª planta 28033 Madrid

+34 912339082

info@avivavoice.com

Purposes of data processing

AVIVA has the duty to inform users that all their personal data provided are treated for the following purposes:

• Provision of Electronic Trust Services. The data is collected through the appropriate contract and is processed with the purpose of carrying out the electronic services requested and contracted by the users, all based on the provisions of this Certification Practice Statements.

• Address inquiries and requests. The data is collected through the contact form available on the website and will be used exclusively to manage the queries and requests received.

AVIVA informs that the personal data provided will only be processed for the purposes described above and will not be treated in a manner incompatible with them.

Lawfulness of processing

In accordance with the indicated data purposes, the legal basis for the treatment of personal data of users is:

- The legitimation of the data processing for the provision of electronic trust services is the execution of the contract for the services requested, where the user is part of it.
- The legitimacy of the data processing to attend to inquiries and requests is based on the consent of the interested party, who gives it expressly and unequivocally, through positive action and prior to sending, upon accepting the conditions and the privacy policy. Such consent can be withdrawn at any time by sending an email to dpo@avivavoice.com

Processed data and conservation

The categories of personal data processed by AVIVA, including but not limited to, include identifying data (name, surname and identity) and contact information (postal address, email and telephone).

Personal data will be kept and retained as long as they are necessary to respond to inquiries and requests, until the end of the contractual relationship and subsequently, for a period of 15 years from the expiration of the certificate, without prejudice to additional legally required periods.

Data transfer

Personal data will not be transferred to third parties without legal obligation, nor will international transfers be made.

User Rights

- Confirmation. All users have the right to obtain confirmation on whether AVIVA is processing personal data concerning them.

- Access and rectification. Users have the right to access all their personal data, as well as request the rectification of those that are inaccurate or erroneous.
- Suppression / cancellation. Users may request the deletion / cancellation of data when, among other reasons, these are not necessary for the purposes for which they were collected.
- Limitation and opposition. The user may request the limitation of the treatment so that their personal data is not applied in the corresponding operations. In certain circumstances and for reasons related to their particular situation, the user may object to the data processing, being AVIVA obliged to stop treating them, except for compelling legitimate reasons, or the exercise or defense of possible claims.
- Portability Interested parties may request that their personal data be sent to them or else be transmitted to another person in charge, in a structured electronic format and of habitual use.

To exercise their rights, users can send a request to the e-mail address dpo@avivavoice.com or send a letter to the address indicated in the information section of the person responsible for processing. In this petition, they must attach a copy of their identity document and clearly indicate which right they wish to exercise.

9.5 Intellectual Property Rights

AVIVA is the only one that has intellectual property rights of this Certification Practice Statement.

9.6 Obligations and Civil Liability

9.6.1. AVIVA Obligations

AVIVA guarantees, under full responsibility that complies with all requirements established in the Certification Practice Statement, and it is responsible for ensuring compliance with the procedures described, according to the instructions contained in this document.

AVIVA provides relying electronic services in accordance with this Certification Practice Statement.

AVIVA informs the subscriber of the terms and conditions related to the use of the certificate, price and use limitations, through a subscriber contract that includes by reference the disclosure texts (PDS) of each of the acquired certificates.

The disclosure text document, also known as PDS, meets the content of Annex A of ETSI EN 319 411-1 v1.1.1 (2016-02) this document can be transmitted by electronic media, using a sustainable communication method, and in accessible language.

AVIVA binds subscribers, key holders and third parties that trust in certificates through the disclosure text or PDS, in written and understandable language, with the minimum following contents:

- Requirements to comply with the provisions established in this document.
- Limits on the use of time stamps.
- Information on how to validate a time stamp, including the requirement to check the status of the stamp, and the conditions under which it can reasonably be relied upon, which is applicable when the subscriber acts as a trusted third party.
- The way in which the liability of the Certification Authority is guaranteed.
- Limitations of liability, including the uses for which the Certification Services Provider accepts or excludes liability.
- Period of archiving audit records.
- Applicable dispute resolution procedures.
- Applicable law and competent jurisdiction.

9.6.2. Guarantees offered to subscribers and relying third parties in certificates

AVIVA in the documentation between subscribers and third parties that trust, establishes and rejects guarantees, and applicable limitations of liability.

AVIVA guarantees the subscriber that the time stamps comply with all the material requirements established in this Certification Practice Statement, as well as the reference standards.

AVIVA guarantees the third party that relies on the qualified electronic time stamp that the information contained or incorporated by reference in the seal is correct, except when indicated otherwise.

9.6.3. Rejection of other guarantees

AVIVA rejects any other guarantee that is not enforceable under the laws, except those contemplated in this document.

9.6.4. Limitation of liability

AVIVA limits its responsibility to the provision of the service of issuing qualified electronic time stamps, which will be regulated by the appropriate contract.

AVIVA does not perform any verification of the document for which the Time Stamp is requested, since it is sent directly by the Subscriber under its own and exclusive responsibility.

AVIVA does not assume any obligation with respect to the monitoring of the content, type and / or format of the documents and the hash sent by the time stamping process.

AVIVA will not be responsible for any direct damage and / or by third parties because of the misuse of the qualified time stamps duly issued in accordance with this document.

9.6.5. Fortuitous event and force majeure

AVIVA includes in the disclosure text or PDS, clauses that limit its responsibility in fortuitous event or force majeure.

9.6.6. Applicable Law

AVIVA establishes, in the subscriber contract and in the disclosure text or PDS, that the applicable law of services provision, including the policy and practices of certification, is the Spanish Law.

9.6.7. Severability, survival, entire agreement and notification clauses

AVIVA establishes, in the subscriber's contract and in the disclosure text or PDS, the severability, survival, entire agreement and notification clauses:

- Under the severability clause, the invalidity of a clause will not affect the rest of the contract.
- Under the survival clause, certain rules will remain in force after the completion of the regulatory service of the legal relationship between the parties. For this purpose, the Certification Authority ensures that the requirements of sections 9.6.1 (Obligations and liability), 8 (Compliance audit) and 9.3 (Confidentiality), remain in force after the termination of the service and the general conditions of issuance/use.
- Under the entire agreement clause it is understood that the regulatory legal service contains the full will and all agreements between the parties.
- Under the notification clause, it will be established the procedure by which the parties mutually report incidents.

9.6.8. Competent Jurisdiction Clause

AVIVA establishes, in the subscriber's contract and in the disclosure text or PDS, a jurisdiction clause, indicating that the international jurisdiction corresponds to the Spanish judges.

The territorial and functional jurisdiction shall be determined under the regulations of international private law and procedural law that may be applied.

9.6.9. Resolution of conflicts

AVIVA establishes, in the subscriber's contract, and in the disclosure text or PDS, mediation and resolution procedures of applicable disputes.

Annex I – Acronyms

AC	Autoridad de Certificación. Certification Authority
CA	Certification Authority. Autoridad de Certificación
RA	Autoridad de Registro. Register Authority
CN	Common Name
CP	Certificate Policy
CPD	Centro de Procesamiento de Datos. Data Processing Center
CPS	Certification Practice Statement. Declaración de Prácticas de Certificación
CRL	Certificate Revocation List. Lista de certificados revocados
CSR	Certificate Signing Request. Petición de firma de certificado
DES	Data Encryption Standard. Estándar de cifrado de datos
DN	Distinguished Name. Nombre distintivo dentro del certificado digital
DPC	Declaración de Prácticas de Certificación. Certification Practice Statement
DSA	Digital Signature Algorithm. Estándar de algoritmo de firma
DCCF	Dispositivo Cualificado de Creación de Firma. Qualified Signature Creation Device
ETSI	European Telecommunications Standards Institute o Instituto Europeo de Normas de Telecomunicaciones
QSCD	Qualified Signature Creation Device. Dispositivo Cualificado de Creación de Firma
FIPS	Federal Information Processing Standard Publication. Publicación estándar de procesamiento de información federal
ISO	International Organization for Standardization. Organismo Internacional de Estandarización
LRC	Listas de Revocación de Certificados. Certificate Revocation Lists
LDAP	Lightweight Directory Access Protocol. Protocolo de acceso a directorios
NTP	Network Time Protocol. Protocolo de tiempo de red

OCSP	On-line Certificate Status Protocol. Protocolo de acceso al estado de los certificados
OID	Object Identifier. Identificador de objeto
PA	Policy Authority. Autoridad de Políticas
PC	Política de Certificación. Certification Policy
PDS	Texto de divulgación – Policy Disclosure Statement
PIN	Personal Identification Number. Número de identificación personal
PKCS	Public-Key Cryptography Standards. Estándares de criptografía de clave pública
PKI	Public Key Infrastructure. Infraestructura de clave pública
PSC	Prestador de Servicios Electrónicos de Certificación / Confianza. Trust Services Provider.
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
SHA	Secure Hash Algorithm. Algoritmo seguro de Hash
SSL	Secure Sockets Layer
TCP/IP	Transmission Control. Protocol/Internet Protocol
TSA	Autoridad de Sellado de Tiempo – Time Stamping authority
TSP	Trust Service Provider. Prestador de Servicios Electrónicos de Certificación / Confianza
TSU	Unidad de Sellado de Tiempo – Time Stamping Unit