AGCE PKI

Time-stamping Policy & Practice Statement

Document Management

Information

Group of document	AGCE PKI
Title	Time-stamping Policy & Practice Statement
Project reference:	**Algeria National PKI**
Annex:	n.a.

Version control

Version	Date	Description / Status	Responsible
V0.1	08/10/2019	Initial document preparation	AGCE
V0.2	20/03/2020	Various enhancement including the injection of final URLs and documentation references + typos correction	AGCE
V1.0	25/10/2020	Released version aligned to the Infrastructure CA CPS	AGCE
V1.1	10/10/2021	Annual review	AGCE
V2.0	23/06/2022	Released with alignment to latest AGCE CPSs	AGCE

Document Signoff

Version	Date	Responsible	Validated By	Reviewed and Approved By
V2.0	23/06/2022	AGCE	AGCE (PKI GB)	AGCE (PKI GB) 25 / 06 / 2022

Table of contents

1. Introduction

1.1 Overview

The Algeria National PKI is implemented as two separate PKI domains (Government and Commercial) established under the Algeria NR-CA. With this National PKI, the Algerian Government aims to provide a framework to facilitate the establishment of Trust Service Providers (TSP) offering digital certification and trust services to government and non-government entities.

The Algeria PKI hierarchy comprises a hierarchy of Certification Authorities (CAs).

The NR-CA sits at the top level of the hierarchy and acts as the trust point (anchor) for the Algerian PKI. The National Authority for Electronic Certification (Autorité Nationale de Certification Electronique – ANCE) is established by the Algerian government to operate the NR-CA. As the National PKI governance body, the ANCE's mandate is to operate the Policy Management Authority (PMA).

The Government Authority for Electronic Certification (Autorité Gouvernementale de Certification Electronique – AGCE) is established by the Algerian Government to operate the GOV-CA and to offer related trust services to the Algerian government domain. As such the AGCE operates as a Trust Services Provider (TSP) offering its services through a hierarchy of CAs, implemented under the National Root CA as follows:

- **Government CAs:**

  Five (05) Intermediate CAs **(GOV-CA hereafter)** certified by the Root CA, namely: **Government CA, Government TLS CA, Government CS CA, Government SMIME CA, Government TS CA.**

  Each Government CA certifies one issuing CA to cover particular extended Key usages:

  - **Corporate CA:** will issue Digital Signature and Authentication certificates to natural persons (government employees) and legal persons (government entities).
  - **OV TLS Server CA:** will issue organization validated Server Authentication certificates to non-natural entities such as servers and VPN device certificates. It will also issue Client Authentication certificates to non-natural organization end entities (devices).
  - **SMIME CA:** will issue email protection (SMIME) certificates to natural persons (government employees).
  - **Code Signing CA:** will issue code signing certificates to legal persons (government entities).
  - **Trust services CA:** will issue timestamping certificates for AGCE and Government TSPs operating Timestamping services. It will also issue signing certificates for digital signature verification service operated by governmental TSPs.

In addition to the above issuing CAs, there is a scenario where a Governmental TSPs can establish their own certification services under the Government CA. The GOV-CA will certify an issuing CA operated by the TSP. This CA shall be technically constrained where the CA certificate (issued by the GOV-CA) will be populated with a combination of extended key usage and name constraint extensions to limit the scope within which the issuing CA from the TSP may issue end-user certificates;

The AGCE is responsible for the supervision and authorization of the TSP that shall successfully complete an authorisation process.

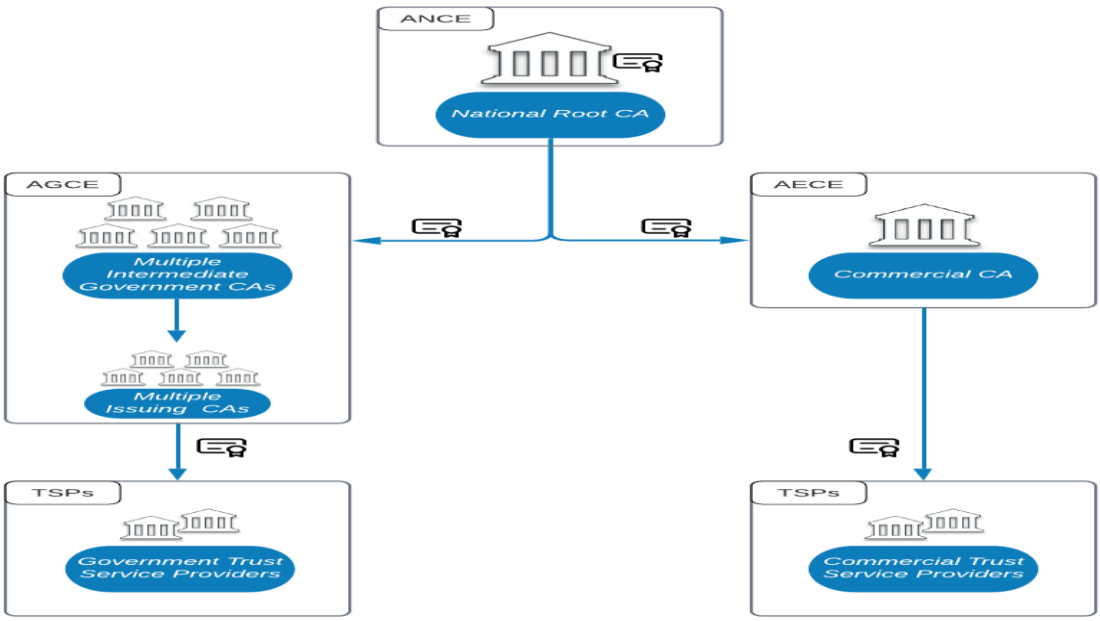

Figure 1: The Algerian National PKI hierarchy

As part of the certification services provided by the AGCE, AGCE also offers a time-stamping service named the "AGCE Timestamp Authority", further referred to as "AGCE TSA", in accordance with ETSI TS 102 023 "Policy requirements for time-stamping authorities" and ETSI TS 101 861 "Time Stamping Profile" with regard to the time-stamping profile.

The AGCE Time-stamping Policy (TSP) and Time-stamping Practice Statement (the present document), describing general rules, which shall be followed by the Time-stamping Service. This document is administered and approved by AGCE and should be read in conjunction with the current Trusted Service Provider (TSP) Certificate Policy and the **AGCE CPS for devices**. Both documents can be downloaded from https://ca.pki.agce.dz/repository.

The AGCE TSA response signing certificate is issued by the Trust services CA , hence references in this document to Certificate Policy (CP) or Certification Practice Statement (CPS) are specifically pointing to the Trusted Service Provider (TSP) Certificate Policy and the **AGCE CPS for devices** respectively.

2. Scope

This document specifies the policy requirements relating to the operation of AGCE Time-stamping Authority (TSA), such that subscribers and relying parties may have confidence in the operation of the time-stamping services.

The AGCE PKI Time-stamping Authority uses PKI and trusted time sources to provide reliable, standards-based time-stamps. This Time-stamping Policy document defines the operational and management requirements of the AGCE TSA such that Subscribers and Relying Parties may evaluate their confidence in the operations of the AGCE TSA services.

The policy requirements are aimed to provide time-stamping to any application requiring to prove that the data under consideration existed before a particular time.

Subscribers and Relying Parties should consult with the AGCE PKI GB to obtain further details of how precisely this Time-stamping Policy is implemented by AGCE and how the service can be used by other Relying Parties.

3. References

CEN Workshop Agreement 14167-2: “Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures — Part 2 Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)”.

ETSI TS 102 023, V1.2.1 (2003-01), Policy Requirements for time-stamping authorities.

ETSI TS 101.861, V1.2.1 (2002-03), Time Stamping Profile.

RFC 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

FIPS PUB 140-1 (1994): "Security Requirements for Cryptographic Modules."

ISO/IEC 15408 (1999) (parts 1 to 3): “Information technology — Security techniques Evaluation criteria for IT security”.

CA Security Council Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates.

TSP Certificate Policy (https://ca.pki.agce.dz/repository/tsaps).

AGCE CPS for devices (https://ca.pki.agce.dz/repository/cps).

4. Definitions and Abbreviations

4.1 Definitions

“Certificate Policy” or **“CP”** is a named set of rules that indicates the applicability of a certificate to a particular community/class of application with common security requirements.

“Certificate Practice Statement” or **“CPS”** is a statement of the practices that a certification authority employs in issuing certificates.

“Time-Stamp Authority” or **“TSA”** means a trusted authority, which issues time-stamp tokens.

“Time-Stamp Policy/Practice Statement” or **“TSP/PS”** (this document) means a set of rules that indicate the applicability of a time-stamp token to a particular community or class of application with common security requirements.

“Time-Stamp Token” or **“TST”** means a data object that binds representation of a datum to a particular time with a digital signature, thus establishing evidence.

“Time-Stamp Unit” or **“TSU”** means a set of hardware and software, which is managed as a unit and has a single private signing key active at a time.

“TSA Disclosure Statement” means an overview of the policies and practices of a TSA that require particular emphasis to subscribers and relying parties.

“Relying Party” means an entity (an individual or organization), which relies on a Time-stamp Token provided by AGCE TSA.

“Subscriber” means an entity (an individual or organization) that requires the services provided by a TSA and has entered into AGCE TSA Subscriber Agreement.

“Coordinated Universal Time” or **“UTC”** means the time scale, based on the second, as defined by the International Telecommunications Radio Committee (ITU-R) TF.460-5 and roughly corresponding to Greenwich Mean Time (GMT).

“UTC(k)” means a time scale realized by a laboratory **“k”** as defined in Circular T of Le Bureau International des Poids et Mesures (BIPM) and kept in close agreement with UTC.

4.2 Abbreviations

AST	Arabian Standard Time
CA	Certification Authority
CP	Certificate Policy
CDP	CRL Distribution Point
CPS	Certification Practice Statement
CRL	Certificate Revocation List
ETSI	European Telecommunications Standards Institute
ETSI TS	ETSI Technical Specification
FIPS	Federal Information Processing Standards
GPS	Global Positioning System
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
RFC	Request for Comments
TSA	Time-stamping Authority
TST	Time-stamping Token
TSU	Time-stamping Unit
UTC	Coordinated Universal Time

5. General Concepts

The TSA (Time-stamp Authority) is the authority trusted by the users of the time-stamping services (i.e., Subscribers as well as Relying Parties) to create TSTs (Time-stamp Token). The TSA has the overall responsibility for the provision of the time-stamping services.

The TSA is identified in the TSTs, and in the certificates used to verify the signature on those TSTs, as the Time-stamp issuer and its private key are used to sign the TST.

5.1 Time-stamping Services

The time-stamping service is broken down in the present document into the following component services for the purposes of classifying requirements:

- **Time-stamping provision:** This service component generates time-stamp tokens.
- **Time-stamping management:** The service component that monitors and controls the operation of the time-stamp services to ensure that the provided service is as specified by the TSA. This service component has the responsibility for the installation and uninstallation of the time-stamping provision service. For example, time-stamping management ensures that the clock used for time-stamping is correctly synchronized with UTC.

This subdivision of services is only for the purpose of clarifying the requirements specified in the current document and places no restrictions on any subdivision of an implementation of the time-stamp services provided by AGCE.

5.2 Time-stamping Authority

The authority trusted by the users of the time-stamp services (i.e., Subscribers as well as Relying Parties) to issue time-stamp tokens (TSTs) is called the Time-stamping Authority (TSA).

The TSA shall have the overall responsibility for the provision of the time-stamp services identified in Section 5.1.

The TSA shall have the responsibility for the operation of one or more TSUs (Time-stamp Units), which create and sign on behalf of the TSA.

The TSA responsible for issuing a TST shall be identified (see Section 8.3.1).

A TSA may operate several identifiable TSUs.

AGCE operates the AGCE TSA as part of the AGCE PKI. The AGCE TSA is identified in the Digital Certificate used in the time-stamping service.

5.3 Subscribers

The subscriber may be an organization comprising several end users or an individual end-user.

When the subscriber is an organization, some of the obligations that apply to that organization will be applicable to the end-users as well. In any case, the organization shall be held responsible if the obligations from the end users are not correctly fulfilled and therefore such an organization is expected to inform its end users as required.

When the subscriber is an end user, the end user shall be held directly responsible if its obligations are not correctly fulfilled.

Subscribers must use a method or software toolkit approved by AGCE to request time-stamps, unless otherwise specifically authorized in writing by AGCE.

5.4 Time-stamp Policy and TSA Practice Statement

This section explains the relative roles of the Time-stamp Policy and TSA Practice Statement.

5.4.1 Purpose

A Time-stamp Policy is defined as a named set of rules that indicates the applicability of a Time-stamp Token to a community and/or class of applications with common security requirements.

The TSA Practice Statement is defined as the statement of the practices that a TSA employs in issuing the Time-stamp Tokens.

The relationship between the Time-stamp Policy and the TSA Practice Statement is similar in nature to the relationship of other business policies, which state the requirements of the business, while operational units define the practices and procedures of how these policies are to be carried out.

For additional details on the AGCE TSA Practice Statements, refer to the **AGCE CPS for devices**.

See ETSI 102 023 Section 4.4.2 for considerations on the level of specificity and Section 4.4.3 for the approach of a Time-stamping Policy versus TSA Practice Statements.

5.4.2 Level of Specificity

This AGCE PKI Time-stamping Policy extends the TSP Certificate Policy, which regulates the operations of the TSPs in Algeria.

6. Time-stamping Policies

6.1 Overview

This Time-stamping Policy defines a set of processes for the trustworthy creation of Time-stamp Tokens in accordance with ETSI TS 102 023. The private keys and the TSU meet the technical specifications of ETSI TS 101 861 and RFC 3161.

The AGCE TSA shall sign time-stamps using private keys that are reserved specifically for that purpose. Each TST shall contain an identifier to the applicable policy and the TSTs shall be issued with time accurate to plus or minus 1 second of UTC.

The time-stamps shall be requested through Hypertext Transfer Protocol (HTTP), as described by the RFC 3161.

The URL for AGCE TSA is: https://tsa-dz.pki.agce.dz

6.2 Identification

The object identifier (OID) of the baseline AGCE PKI Time-stamping Policy is: **2.16.12.3.2.1.4**

This OID is referenced in every AGCE TSA issued time-stamp.

6.3 User Community and Applicability

The user community for AGCE TSA time-stamps includes AGCE PKI Subscribers and their Relying Parties. All Subscribers are automatically deemed to be Relying Parties.

AGCE does not impose restrictions on applicability of its time-stamps, with the exception of prohibited uses outlined in Section 1.4.2 (Prohibited Certificate Uses) of the **AGCE CPS for devices**.

The AGCE PKI TSP/PS is designed to deliver time-stamps that correspond to the requirements for qualified electronic signatures. However, AGCE TSA time-stamps may be applied to any application requiring proof that a datum existed before a particular time.

6.4 Conformance

The AGCE TSA shall reference the policy identifier in Section 6.2 (Identification) of this document in all time-stamps to indicate conformance with this policy.

The AGCE TSA is subject to periodic independent internal and external reviews to demonstrate that the TSA meets its obligations defined in Section 7.1 (TSA Obligations) and has implemented appropriate controls in line with Section 8 (TSA Practices).

7. Obligations and Liability

7.1 TSA Obligations

7.1.1 General Obligations

AGCE shall ensure that all requirements on TSA, as detailed in Section 8, are implemented as applicable to the selected trusted time-stamping policy.

AGCE shall ensure conformance with the procedures prescribed in this policy.

AGCE shall also ensure adherence to any additional obligations indicated in the TST either directly or incorporated by reference.

7.1.2 TSA Obligations toward Subscribers

AGCE shall undertake the following obligations toward the TSA Subscribers:

- To operate in accordance with this Time-stamping Policy, and the **AGCE CPS for devices**
- To ensure that TSUs maintain a minimum TST time accuracy of plus or minus 1 second
- To undergo internal and external reviews to assure compliance with relevant legislation, and AGCE internal policies and procedures
- To provide high availability access to AGCE TSA systems except in the case of planned technical interruptions, loss of time synchronization, and causes outlined in Section 9.8 (Limitations of Liability) of the AGCE Infrastructure CA CPS

7.2 Subscriber Obligations

When obtaining a TST, the Subscriber shall verify that the TST has been correctly signed and that the private key used to sign it has not been compromised.

Time-stamps shall be requested through HTTP, as described by RFC 3161.

Subscribers shall use a method or software toolkit approved by AGCE to create time-stamps, unless otherwise specifically authorized in writing by AGCE.

7.3 Relying Party Obligations

Before placing any reliance on a time-stamp, subject to Section 8.1.2 (TSA Disclosure Statement) of this document, Relying Parties must verify that the TST has been correctly signed and that the private key used to sign the TST has not been compromised until the time of verification.

The Relying Party should take into account any limitations on usage of the time-stamp indicated by this time-stamping policy and any other precautions prescribed in this agreement or otherwise.

During and after the TSU certificate validity-period, the status of the private key can be checked using the Certificate Revocation List (CRL) referenced in CRL Distribution Point (CDP) extension or using Online Certificate Status Protocol (OCSP) server referenced in Authority Information Access (AIA) extension of the TST signing certificate.

7.4 Liability

Refer to Section 9.8 (Limitations of Liability) of the AGCE CPS for devices.

8. TSA Practices

The provision of a Time-stamp Token in response to a request is at the discretion of AGCE, depending on agreements with the Subscriber.

8.1 Practice and Disclosure Statements

8.1.1 TSA Practice Statement

This Time-stamping Policy establishes the general rules governing the operation of the AGCE TSA. The **AGCE CPS for devices** and additional internal documents define how AGCE meets the technical, organizational and procedural requirements identified in this Time-stamping Policy.

This Time-stamping Policy, the AGCE CPS for devices, and other public documents may be found at https://ca.pki.agce.dz/repository

Internal documents may be provided only under strictly controlled conditions. Notice will be given regarding any changes to this AGCE Time-stamping Policy.

AGCE conducts risk assessments to evaluate threats and to determine the necessary security controls and operational procedures. Additional details may be found in Section 5.4.8 (Vulnerability Assessment) of the AGCE CPS for devices.

The AGCE PKI management has the responsibility for maintaining and approving all AGCE PKI policies and practices according to the terms of Section 1.5 (Policy Administration) of the AGCE CPS for devices. AGCE PKI management has the responsibility to ensure that the practices are properly implemented.

8.1.2 TSA Disclosure Statement

The TSA Disclosure Statement is a document that discloses all Subscribers and potential Relying Parties, the terms and conditions regarding the use of the AGCE TSA services.

The summarized elements of the AGCE TSA Disclosure Statement are provided below:

a. The TSA contact information

b. The Time-stamp Policy being applied

c. At least one hashing algorithm, which may be used to represent the data being time-stamped

d. The expected lifetime of the signature used to sign the TST (depends on the hashing algorithm being used, the signature algorithm being used and the private key length)

e. The accuracy of the time in the TSTs with respect to UTC

f. Any limitations on the use of the time-stamping service

g. The Subscriber’s obligations as defined in Section 7.2, if any

h. The Relying Party's obligations as defined in Section 7.3

i. Information on how to verify the TST such that the Relying Party is considered to “reasonably rely” on the TST (see Section 7.3) and any possible limitations on the validity period

j. The period during which TSA event logs (see Section 8.4.11) are retained

k. The applicable legal system, including any claim to meet the requirements on time-stamping services under the Algerian National Law

l. The limitations of liability

m. The procedures for complaints and dispute settlement

n. Whether or not the TSA has been assessed to be conformant with the identified Time-stamp Policy and if so by which independent body

This information shall be available through a durable means of communication and in a readily understandable language. It may be transmitted electronically.

8.2 Key Management Life Cycle

8.2.1 TSA Key Generation

AGCE shall generate the cryptographic keys used in its TSA services under dual control by authorized personnel in a secure physical environment. The personnel authorized to carry out this function shall be limited to those requiring doing so under AGCE practices.

Additional information is provided in Section 6.1 (Key Generation and Installation) of the AGCE CPS for devices. The keys shall be generated within TSU Hardware Security Modules (HSMs) that are certified to FIPS 140-1 Level 3. Algorithms and key sizes are described in Section 6.1.5 (Key Sizes) of the AGCE CPS for devices.

8.2.2 TSU Private Key Protection

AGCE shall take specific steps to ensure that TSU private keys remain confidential and maintain their integrity. These include use of Hardware Security Modules (HSMs) certified to FIPS 140-1 Level 3 to hold and sign with the keys.

When TSU private keys are backed up, they shall be copied, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment. The personnel authorized to carry out this function shall be limited to those requiring doing so under AGCE practices.

8.2.3 TSU Public Key Distribution

Digital Certificates used in the AGCE TSA shall be issued by the trust services CA according to a Certificate Policy that provides a level of security equivalent to this Time-stamping Policy. Additional information is provided in Section 6.1 (Key Generation and Installation) of the AGCE CPS for devices.

8.2.4 Rekeying TSU's Key

TSU private signing keys shall be replaced before the end of their validity period. Additional information is provided in Section 4.7 (Certificate Re-key) of the AGCE CPS for devices.

8.2.5 End of TSU Key Life Cycle

TSA private signing keys shall be replaced upon their expiry. The TSA shall reject any attempt to issue time-stamps once a private key has expired. After expiry, private keys are destroyed.

8.2.6 Life Cycle Management of the Cryptographic Module Used to Sign Time-stamps

AGCE has procedures in place to ensure that Hardware Security Modules (HSMs) intended for non-repudiation services are not tampered with in shipment or storage.

Acceptance testing is performed to verify that cryptographic hardware is performing correctly.

Installation and activation are performed based on dual control of authorized personnel with trusted roles, and the devices operate in a physically secured environment.

Additional information is provided in Section 6.6 (Life Cycle Technical Controls) of the AGCE CPS for devices.

8.3 Time-stamping

8.3.1 Time-stamp Token

AGCE has technical prescriptions in place to ensure that TSTs are issued securely and include the correct time. In line with the protocols referenced in Section 3 of this document, each TST includes:

- A representation (e.g., hash value) of the datum being time-stamped as provided by the requestor
- A unique serial number that can be used to both order TSTs and to identify specific TSTs
- An identifier for the Time-stamp Policy
- The time calibrated to within 1 second of UTC, traceable to a UTC(k) source
- An electronic signature generated using a key used exclusively for time-stamping
- An identifier for the TSA and the TSU

AGCE maintains audit logs for all calibrations against the UTC(k) references.

8.3.2 Clock Synchronization with UTC

AGCE shall provide time with plus or minus 1 second of UTC by calibration with an NTP server.

AGCE shall have technical measures in place to ensure that the time of its TSU is synchronized with UTC within the declared accuracy. Audit and calibration records are maintained by the TSU operated by AGCE.

AGCE shall ensure that clock synchronization is maintained when a leap second occurs as notified by the appropriate body.

The TSU operated by AGCE shall also monitor time drift outside present boundaries and request additional recalibrations as needed. If the TSU clock drifts outside the declared accuracy, and recalibration fails, the TSU operated by AGCE must not issue time-stamps until correct time is restored.

8.4 TSA Management and Operation

8.4.1 Security Management

AGCE has an active security management program designed to document, implement and maintain adequate security provisions for the AGCE PKI according to the best practice and the requirements of relevant standards.

Additional information is provided in Section 5 (Management, Operational and Physical Controls) and Section 6 (Technical Security Controls) of the AGCE CPS for devices.

8.4.2 Asset Classification and Management

In order to ensure that information and other assets receive appropriate security treatment, AGCE shall maintain an inventory of all assets and assign a classification for the protection requirements to those assets consistent with the risk analysis. Additional information is provided in Section 6.6 (Life Cycle Technical Controls) of the AGCE CPS for devices.

8.4.3 Personnel Security

Since the AGCE TSA is operated as part of AGCE PKI infrastructure, provisions in Section 5 (Management, Operational and Physical Controls) and Section 6 (Technical Security Controls) of the AGCE CPS for devices shall also apply for the TSA.

8.4.4 Physical and Environmental Security

Since the AGCE TSA is operated as part of AGCE PKI infrastructure, provisions in Section 5 (Management, Operational and Physical Controls) and Section 6 (Technical Security Controls) of the AGCE CPS for devices shall also apply for the TSA.

8.4.5 Operations Management

The operations management controls for the AGCE TSA are incorporated within the overall AGCE PKI operations management controls. Additional information in relation to operations management is provided in Section 5 (Management, Operational and Physical Controls) of the AGCE CPS for devices.

8.4.6 System Access Management

AGCE shall maintain appropriate physical and logical access controls for affected facilities, hardware, systems and information.

The systems' access management controls for the AGCE TSA are incorporated within the overall AGCE PKI systems access management controls. Additional information is provided in Section 5 (Management, Operational and Physical Controls) of the AGCE CPS for devices and Section 6 (Technical Security Controls) of the AGCE CPS for devices.

8.4.7 Trustworthy Systems Deployment and Maintenance

AGCE shall use trustworthy systems that are protected against modification. The systems deployment and maintenance controls for the AGCE TSA are incorporated within the overall AGCE PKI systems deployment and maintenance controls. Additional information is provided in Section 6 (Technical Security Controls) of the AGCE CPS for devices.

8.4.8 Compromise of TSA Services

In the event of compromise of a TSA private key, AGCE shall follow the procedures outlined in Section 5.7 (Compromise and Disaster Recovery) of the AGCE CPS for devices . This includes revoking the relevant certificate and adding it to trust services CA CRL.

The TSA will not issue time-stamps if its private key is not valid.

The TSA will not issue time-stamps if its clock is outside the declared accuracy from reference UTC, until steps are taken to restore calibration of time.

As described in Section 8.4.11 (Recording of information concerning operations of time-stamping services) of this document, AGCE shall maintain audit trails to discriminate between genuine and backdated tokens.

8.4.9 TSA Termination

In case of termination of the AGCE TSA, AGCE shall follow the procedures in Section 5.8 (CA or RA Termination) of the AGCE CPS for devices and also more detailed internal AGCE termination procedures.

These include at a minimum informing subscriber, revoking TSA certificates and transferring obligations to a reliable party for maintaining event log and audit archives as well as access to private keys.

8.4.10 Compliance with Legal Requirements

The AGCE TSA shall comply with applicable legal requirements as applicable in Algeria.

8.4.11 Recording of Information Concerning Operations of Time-stamping Services

AGCE shall maintain records of all relevant information concerning the operations of the AGCE TSA for a period of seven years, in accordance with the AGCE PKI business practices.

Records shall be protected for their data integrity and moved to a protected server for storage and subsequent archiving.

Records shall be treated as confidential in accordance with the AGCE CPS for devices. No personal data relating to Subscribers is transmitted between jurisdictions.

Records concerning the operation of time-stamping services shall be available at the request of Subscribers or if required by court order or another legal requirement.

AGCE shall maintain records, including precise time of:

- Time-stamp requests and created time-stamps
- Events related to TSA administration (including certificate management, key management and clock synchronization)
- Events relating to the life cycle of TSA keys and certificates

8.5 Organizational

AGCE organizational structure, policies, procedures and controls apply to the AGCE TSA.

9. Profiles

The requirements from RFC 3161 and ETSI 101 861 Section 5.1 “Profile for the format of the request” and 5.2 “Profile for the format of the response”, and Section 6 “Profile for the transport protocols to be supported” shall apply.