المركز الوطني
للتصديق الرقمي
NATIONAL CENTER FOR DIGITAL CERTIFICATION

TIME-STAMP POLICY

Document Classification:

Public

Version Number: 1.1

Issue Date: November 8, 2020

Copyright © 2020 National Center for Digital Certification, Kingdom of Saudi Arabia. This document is intended for use only by the National Center for Digital Certification and authorized Saudi National PKI participants. This document shall not be duplicated, used, or disclosed in whole or in part for any purposes without prior consent.

Table of Contents

1. Introduction

This Time-Stamp Policy and Practice Statement of the NCDC has been prepared for explaining the technical and legal requirements met by the NCDC Time-Stamp Authority (hereafter referred as “NCDC TSA”). Time-Stamping is gaining an increasing interest and it is becoming an important component of digital signatures.
NCDC time-stamping service uses public key infrastructure and reliable time sources to provide reliable time-stamps and in accordance with patterns globally accepted.

2. Scope

The NCDC TSA uses public key infrastructure of Government-CA and trusted time sources to provide reliable, standards-based time-stamps in accordance with patterns globally accepted.
This Time-Stamp Policy and Practice Statement defines the operational and management practices of the TSA such that Subscribers and Relying Parties may evaluate their confidence in the operation of the time-stamping services.
The NCDC TSA aims to deliver time-stamping services to subscribers.

3. Definitions

The terms used in this document shall have the meanings as defined in NCDC Glossary, which can be found at https://www.ncdc.gov.sa

4. General Concepts

4.1 Time-Stamp Authority

NCDC TSA is responsible for provisioning of time-stamps services. It has the responsibility for the operation of the time-stamp unit that is creating and signing on behalf of the NCDC TSA.

Subscribers and Relying Parties trust this TSA for the issued time-stamp tokens.

Queries regarding NCDC TSA shall be directed at:

Email: info@ncdc.gov.sa

Telephone: +966 11 452 2197

4.2 Time-Stamping Services

The Time-Stamping Services consist of the infrastructure, the management and the provisioning of timestamp tokens.

The infrastructure used to generate the time-stamp tokens consists of:

- communication interface to collect time-stamp requests and return time-stamp tokens,
- Time-Stamping Unit (TSU) which creates specific time-stamp tokens, and
- time source providing accurate date and time values to be included in the time-stamp tokens.

The management of the Time-Stamping Services is the service component that monitors and controls the operation of the Time-Stamping Services to ensure that the service provided is as specified by the TSA.

The Time-Stamping Services assure subscribers and relying parties use of a reliable time source and proper management of all system components.

These services provided by the NCDC TSA to the subscribers are governed by the same organizational structure, operating procedures, facilities and computer environment as the Government-CA PKI infrastructure hosted at NCDC Shared Services Center.

4.3 TIME-STAMP AUTHORITY OBLIGATIONS

The NCDC Time-Stamp Authority is:

- Compliant with the Time-Stamp policy,
- Providing trustworthy time-stamp,
- Providing UTC time accuracy of ± 1 second,
- Performing internal and external audits to assure compliance to this policy,
- Ensuring that all requirements and procedures detailed in this document are implemented, and
- Ensuring that during service and maintenance, NCDC website have announcement of maintenance window.

4.4 SUBSCRIBER OBLIGATIONS

The subscriber shall verify that the time-stamp token has been signed correctly and that the digital certificate used to sign the time stamp token has not been compromised.

Additional requirements can be included in contractual agreements between the TSA and the subscriber.

4.5 RELYING PARTIES OBLIGATIONS

The terms and conditions made available to relying parties shall include an obligation on the relying party that, when relying on a time-stamp token, the relying party shall:

- verify that the time-stamp token has been correctly signed and that the private key used to sign the timestamp has not been compromised until the time of the verification;
- take into account any limitations on the usage of the time-stamp indicated by the timestamp policy;
- take into account any other precautions prescribed in agreements or elsewhere.

After expiry of the time-stamp certificate, the relying party should:

- verify that the TSA private key is not revoked, and
- verify that the cryptographic hash function and the signing algorithm used in the timestamp token are still considered secure.

4.6 LIABILITY

- The liability provisions stated in Government-CA CP are applicable.
- The NCDC disclaims all liability implicit or explicit due to the use of any time-stamp issued by the NCDC TSA to subscribers.
- NCDC TSA is not liable for the mistakes in the verification of the validity of time stamps or for the wrong conclusions conditioned by omissions or for the consequences of such wrong conclusions.
- NCDC TSA assumes no liability for the loss of value of the validity confirmation proof due to force majeure.

- NCDC TSA disclaims expressed or implied responsibility or guarantee for the availability or accuracy of the timestamp service.

5. Time-Stamp Policies

5.1 General

This NCDC TSA policy is set of rules that indicates the applicability of a time-stamp token to a particular community or class of application with common security requirements, which include:

- The TSA, private keys, and profiles of public key certificates comply with technical specifications of the RFC 3161 and RFC 3628.
- The Level of Assurance of TSA Signing Certificate is High and the Signature legal level of TSA Signing Certificate is Qualified.
- The Legal Effects of High Level of Assurance are mentioned in Electronic Transactions Law - Chapter 4 - Article 14
- The NCDC TSA holds private keys used in signing time-stamps.
- Time-Stamp tokens are issued with the accuracy of ± 1 second, as indicated in Section 6.2.2.

This document should be read in conjunction with the current version of the Government-CA CP, available for viewing at: https://www.ncdc.gov.sa , which regulates the operation of Government-CA and its digital certificate services.

5.2 Identification

The object identifier (OID) for the NCDC TSA is: 2.16.682.1.101.5000.1.3.1.1.1.1.9

Please refer to the latest OID Allocation document available on https://www.ncdc.gov.sa.

5.3 User Community and Applicability

The NCDC TSA may provide public timestamp services.

The community of users for timestamp services includes subscribers and relying parties.

NCDC TSA does not restrict the applicability of its time stamps.

6. Policies and Practices

6.1 Risk Assessment

TSA assets are subjected to an appropriate risk treatment; NCDC maintains an inventory of assets, with the corresponding risk ratings, in order to perform a consistent risk analysis. The security controls related to the time-stamping services are reviewed regularly as part of NCDC Risk Analysis exercise and NCDC management approves the Risk Assessment and accept the residual risk.

6.2 Trust Service Practice Statement

The Time Stamp Policy (“what is adhered to”) and the Time Stamp Practice Statement (“how it is adhered to”) have been merged into one document, the NCDC Time Stamp Policy and

Practice Statement. This document specifies a time-stamp policy and practice statement to meet general requirements for trusted time-stamping services. Detailed description of how TSA meets the technical, organizational, and procedural requirements are contained in additional documents that are available only to authorized personnel and auditors.

Monitoring of the implemented security controls is a continuous process. In addition, these controls are reviewed by an independent entity, with trustworthy and capable to verify the adherence of the security controls.

In order to ensure the quality, performance and operation of the time-stamping service following measures have been applied:

6.2.1 TIME STAMP FORMAT

The issued time-stamp token by TSA is compliant to RFC 3161 time-stamps. The service issues time stamps with an RSA algorithm and a key length of 2048, which accept any of the following hash algorithms:

- SHA256

6.2.2 TIME ACCURACY

The time signal is provided via GPS-NTP. The time-stamping service uses this time signal and a set of NTP servers as source of time. With this configuration, the time-stamping service reaches an accuracy of the time of +/-1s or better with respect to UTC.

6.2.3 LIMITATIONS OF THE SERVICE

The current policy does not define any limitations on subscribers or applicability of the services delivered.

6.2.4 APPLICABLE LAW

The laws of the Kingdom of Saudi Arabia govern the NCDC TSA.

6.3 INFORMATION SECURITY POLICY

NCDC has implemented an Information Security Management System throughout the organization as per ISO27001. The Governance and Compliance Committee reviews information security policy on a regular basis and when significant changes occur. NCDC management approves the changes in the information security policy.

6.4 OBLIGATIONS

TSA obligations are as defined in the section 4.3 in this document.

6.5 LIABILITY

The Liability provisions are as described in the section 4.6 in this document.

7. TSA MANAGEMENT AND OPERATIONS

NCDC has implemented an Information Security Management System to maintain the security of the time-stamp service.

7.1 INTERNAL ORGANISATION

NCDC is having well defined organizational structure and roles to manage Time-Stamp and PKI services. This organization structure, policies, procedures and controls are equally applicable to TSA. All persons managing time-stamping operations are selected on the basis of skills, loyalty, trustworthiness, and integrity.

7.2 PERSONNEL SECURITY CONTROL

All information relating to personnel security management are as described in section 5.3 of Government-CA CPS.

7.3 ASSET MANAGEMENT

NCDC maintains an inventory of all assets and a classification consistent with the risk assessment.

All media is handled securely as described in the NCDC Cryptographic Device Life Cycle Management Policy and Procedure.

7.4 SYSTEM ACCESS MANAGEMENT

All information relating to access management of the systems are mentioned in sections 5 and 6 of Government-CA CPS.

7.5 CRYPTOGRAPHIC CONTROLS

All information relating to key lifecycle management is as described in section 6 of Government-CA CPS.

7.6 TIME-STAMPING

NCDC TSA offers time-stamping services using RFC 3161 “Time Stamp Protocol (TSP)” and ensures that time-stamp tokens are issued securely and include the correct time. In particular:

- The time-stamp token includes an identifier for the time-stamp policy.
- Each time-stamp token has a unique identifier.
- The TSU uses 2048-bit RSA keys generated exclusively for signing time-stamp tokens.
- The time included in the time-stamp token is synchronized with UTC within the accuracy defined in this policy
- The time-stamp generation system automatically reject any attempt to issue time-stamps if the signing private key has expired.
- TSA logs all issued time-stamp tokens.

7.7 Clock Synchronization

The TSA clock is synchronized with UTC Time within the declared accuracy with the following particular requirements:

- The calibration of the TSU clocks is maintained such that the clocks do not drift outside the declared accuracy.
- The declared accuracy shall be of +/-1 second.
- TSA has protected its TSU clocks against threats, which could takes it outside its calibration.
- TSA ensure that time-stamp issuance will be stopped in case of drifts or jumps out of synchronization with UTC.

7.8 Physical and Environmental Security

All information relating to physical and environmental security are mentioned in sections 5 of Government-CA CPS.

7.9 Network Security

All information relating to network security are mentioned in sections 6.7 of Government-CA CPS.

7.10 Incident Management

All information relating to incident management are mentioned in sections 5.7.1 and 5.7.2 of Government-CA CPS.
NCDC has defined an incident management procedure that includes a reporting and a notification process in order to respond efficiently to problems by responsible team.

7.11 Business Continuity Management

All information relating to business continuity management are mentioned in sections 5.7 of Government-CA CPS.

7.12 Compliance

NCDC TSA ensures compliance with applicable law at all times.

7.13 Dispute Resolution Procedure

Any dispute arising out of or related to the time-stamp services provided by the NCDC TSA shall initially be submitted to voluntary mediation. If mediation is not successful, then the dispute will be resolved by binding arbitration, in accordance with NCDC Dispute Resolution Policy.

All information relating to dispute resolution are mentioned in sections 9.13 of Government-CA CPS.

7.14 TSA Termination

In the event, NCDC TSA terminates its operations for any reason whatsoever; it will carry out following actions:

- NCDC TSA will come out with an up-to-date termination plan,
- a timely notice will be provided for community of users of time-stamp services that includes subscribers and relying parties in order to minimize any disruptions that are caused because of the termination of the services, and
- Continued maintenance of information required to verify the correctness of trust services, for a reasonable period, will be provided.