Dubai Electronic Security Center

Dubai PKI

Time-stamping Policy

Time-stamping Practice Statement

Project	DESC CA Project
Title	Time-stamping Policy, Time-stamping Practice Statement
Classification	PUBLIC
File name	Dubai PKI - Timestamping Policy Practice Statement_v1.2
Created on	18 May 2017
Revision	1.2
Modified on	6 April 2023

Document History

Date	Revision	Author(s)	Summary
18 May 2017	0.1	Khawla Hassan	Initial version
12 September 2017	0.2	Khawla Hassan	Changed Dubai Government PKI to Dubai PKI
30 January 2018	1.0	Khawla Hassan	Issue final version
28 June 2022	1.1	Khawla Hassan	- Full document review and aligment with ETSI EN 319 421, - Apply changes implied by changing the issuer of the Dubai Timestamping Authority certificate from DESC Devices CA to DESC Timestamping CA.
6 April 2023	1.2	Khawla Hassan	- Annual Review, - Changes in wording for more explicit alignment to CS BRs regarding logging and logging retention.

Table of Contents

1. Introduction

1.1 Overview

Dubai Electronic Security Center (DESC) manages a Public Key Infrastructure (PKI) referred to as the "Dubai PKI" that uses standard PKI technologies, policies, and operating procedures and application interfaces. The Dubai PKI comprises the Dubai Root Certification Authority (CA) that is the trust anchor of this PKI, which comes at the first level of the PKI hierarchy. The Dubai PKI also comprises DESC Subordinate Certification Authorities (CAs), which come at the second level of the PKI hierarchy. Certification services provided by this PKI enable citizens, residents and government entities in Dubai to conduct secure electronic transactions. This includes securing the machine-to-machine communication where devices can transact securely leveraging the PKI signing and encryption capabilities.

As part of the certifications services provided by the Dubai PKI, DESC also offers a Time-Stamping Service (TSS) named the "Dubai Time Stamping Authority (Dubai TSA)" (hereinafter, Dubai TSA), complying with the qualification requirements of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates for a Time-Stamping Service (TSS).

The terms "Dubai TSA Service" and "TSS" will be used interchangeably in this document.

The Dubai TSA Service uses PKI and a Trusted Time Source to provide reliable, standards-based Time-Stamp Tokens (TST). A Time-Stamp Token (TST) generated by The Dubai TSA service providing evidence of the existence of a hash value at a given date and time. The TSTs are generated and digitally signed by a Time-Stamping Unit (TSU) configured within the TSS. The TSU uses a certificate issued by the Dubai PKI Timestamping CA to sign TSTs.

Since the TST signing certificate is issued by the Dubai PKI Timestamping CA, references in this document to Certificate Policy (CP) or Certification Practice Statement (CPS) are specifically pointing to the Dubai PKI - DESC Subordinate CAs Certificate Policy and Dubai PKI - Timestamping CA Certification Practice Statement respectively.

The structure and contents of this document are based on ETSI EN 319 421[1].

This document is administered and approved by The Dubai PKI Policy Authority (PA), and should be read in conjunction with the current Dubai PKI Subordinate CA Certificate Policy and Dubai PKI Devices CA Certification Practice Statement. Both documents can be downloaded from https://ca-repository.desc.gov.ae/. The PA has also published the Dubai TSA disclosure statement for its subscribers of Time-Stamping.

1.2 Scope

This is document is the Dubai Time-Stamping Policy (TSP), specifying DESC commitments when, acting as TSA to deliver TSTs, it also specifies the obligations and requirements of Subscribers and Relying Parties.

This document also represents the Dubai Time-Stamping Practice Statement (TSPS), specifying the mechanisms and procedures implemented according to the TSP. In particular, the processes followed by the TSU when generating TSTs and maintaining time accuracy.

Subscribers and Relying Parties should consult with the Dubai PKI Policy Authority (PA) to obtain further details of how precisely this TSP/TSPS are implemented by DESC and how the service can be used by other Relying Parties.

This TSP/TSPS does not indorse requirements on establishing any link between the hash to be Time-Stamped and the contents of the original electronic data. Only the Subscriber of the TSS is responsible for this match.

2. References

[1] ETSI EN 319 421 V1.1.1 (2016-03): Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

[2] ETSI EN 319 422 V1.1.1 (2016-03): Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and Time-Stamp token profiles

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

[4] RFC 5816, ESSCertIDv2 Update for RFC 3161.

[5] CA/Browser Forum Baseline Requirements for Code Signing (“Baseline Requirements for Code Signing”).

[6] Subordinate CA Certificate Policy (https://ca-repository.desc.gov.ae/).

[7] Timestamping CA Certification Practice Statement (https://ca-repository.desc.gov.ae/).

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

3. Definitions and Abbreviations

3.1 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 Dubai TSA.

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

Additional definitions are provided in the CP/CPS.

3.2 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
PTB	Physikalisch-Technische Bundesanstalt (http://www.ptb.de)
RFC	Request for Comments
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RSA	Rivest Shamir Adleman Algorithm
SHA	Secure Hash Algorithm
TSA	Time-stamping Authority
TST	Time-stamping Token
TSU	Time-stamping Unit
UTC	Coordinated Universal Time

4. General Concepts

4.1 General Policy Requirements

The TSA (Time-Stamping Authority) is the authority trusted by the users of the TSS (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.

A Time-Stamp Token (TST) generated by The TSS provides evidence of the existence of a hash value at a given date and time. A TST is meant to establish unequivocally this link, a TST is a digitally signed structure including the following:

- hash value, hash algorithm, date and universal time (UTC),
- identifier of the TSU certificate that has generated the TST,
- identifier of the TSA (within the Time-Stamp certificate),
- identifier of the CA that has signed the private keys installed on the TSU.

The TSS relies on the Dubai PKI certification services where the TSU certificate is issued by the Dubai PKI Timestamping CA.

The clock synchronization system of the TSS ensures the issuance of a TSTs with an accuracy of less than one second with respect to UTC.

4.2 Time-Stamping Service

The Time-Stamping Service (TSS) 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 DESC.

4.3 Time-Stamping Authority

The authority trusted by the users of the TSS (i.e., Subscribers as well as Relying Parties) to issue 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 Unit), which create and sign on behalf of the TSA. In case of the Dubai TSA, only one TSU is operated as part of the TSS.

DESC operates the Dubai TSA Service as part of the Dubai PKI.

4.4 Time-Stamping Service participants

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 should use a method or software toolkit approved by DESC to request Time-Stamps, unless otherwise specifically authorized in writing by DESC.

4.5 Time-Stamp Policy and TSA Practice Statement

A Time-Stamp policy is defined as a named set of rules that indicates the applicability of a Time-Stamp token to a particular 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 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.

5. Time-Stamping Policies

5.1 General

This Time-stamping Policy defines a set of processes for the trustworthy creation of timestamp tokens in accordance with ETSI EN 319 421 [1]. The private keys and the TSU meet the technical specifications of ETSI EN 319 422 [2] and RFC 3161.

The Dubai TSA signs Time-Stamps using private keys that are reserved specifically for that purpose. Each TST shall contain an identifier to this 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 RFC 3161.

The URL for Dubai TSA is: https://ca-services.desc.gov.ae/adss/tsa.

5.2 Identification

The object identifier (OID) of this Dubai PKI Time-stamping Policy is: 2.16.784.1.2.2.100.1.3.1.1

This OID is referenced in every Dubai TSA issued Time-Stamp.

5.3 User Community and Applicability

The user community for Dubai TSA Time-Stamps includes Dubai PKI Subscribers and their Relying Parties. All Subscribers are automatically deemed to be Relying Parties.

The Dubai PKI TSP/PS is intended to deliver Time-Stamps that correspond to the requirements for high assurance electronic signatures. However, Dubai TSA Time-Stamps may be applied to any application requiring proof that a datum existed before a particular time.

6. Policies and practices

6.1 Risk Assessment

DESC conducts an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Timestamp data or Timestamp management processes,
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that DESC has in place to counter such threats.

DESC also performs regular vulnerability assessment and penetration testing covering the Dubai PKI systems (including the TSS). Assessments focus on internal and external threats that could result in unauthorized access, tampering, modification, alteration, or destruction of the certificate issuance process. Evidence of the vulnerability assessment and penetration testing activities' execution are collected and archived by the Dubai PKI PA Information Security function.

6.2 Trust Service Practice Statement

DESC applies implements various measures to ensure the trustworthiness of the Dubai TSA and its underlying infrastructure.

These measures are reviewed regularly by a dedicated function with the Dubai PKI PA, whilst a qualified trustworthy personnel check the effectiveness of those measures.

6.2.1 Digest algorithm

The service issues TSTs signed using one of the following digest algorithm:

- SHA-256
- SHA-384
- SHA-512

6.2.2 Accuracy of time

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

The time of timestamping is not the timestamping request acceptance moment, but the timestamping system processing moment.

6.2.3 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. Refer to section 6.2.5 of this document for more details on the timestamp verification.

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

Subscribers should use a method or software toolkit approved by DESC to create Time-Stamps, unless otherwise specifically authorized in writing by DESC.

6.2.4 Relying Party Obligations

Before placing any reliance on a Time-Stamp, subject to Section 8 (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. Refer to section 6.2.5 of this document and section 9.6.4 of the Timestamping CA CPS [7].

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.

6.2.5 Timestamp verification

DESC ensures that Relying Parties can obtain information needed to verify the digital signature of TSTs. The TSU and Issuing CA certificate (Dubai PKI Timestamping CA) are published to allow Relying Parties to verify that Timestamps are issued by the Dubai TSA. The certificates can be found at DESC public repository: https://ca-repository.desc.gov.ae/.

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

6.2.6 Service availability

DESC is committed to provide high availability access to Dubai TSA systems except in the case of planned technical interruptions, loss of time synchronization, and causes outlined in Section 9.16.5 (Force Majeure) of the CP/CPS.

DESC aims to provide 99% service availability per year.

6.2.7 Applicable law

The laws of Dubai shall govern the enforceability, construction, interpretation and validity of the present TSP/TSPS.

6.3 Terms and Conditions

For Subscribers, please refer to the obligations in section 6.2.3.

For Relying Parties, please refer to the obligations in section 6.2.4.

6.4 Information security policy

DESC implements an information security policy that is applicable to the PKI employees, suppliers and contractors. The information security policy is reviewed on a regular basis and maintained by the Dubai PKI PA Information Security function.

6.5 TSA obligations

6.5.1 General

DESC shall ensure that all requirements on TSA, as detailed in Section 8, are implemented as applicable to this TSP/TSPS.

DESC shall ensure conformance with the procedures prescribed in this policy, even when the TSA functionality is undertaken by subcontractors.

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

DESC shall provide all its Time-Stamping services consistent with the Dubai PKI Timestamping CA Certificate Practice Statement.

6.5.2 TSA Obligations towards Subscribers

DESC shall undertake the following obligations toward the TSA Subscribers:

- To operate in accordance with this TSP/TSPS, and the CP/CPS
- To ensure that TSUs maintain a minimum AST time accuracy of plus or minus 1 second
- To undergo internal and external reviews to assure compliance with relevant legislation, and DESC internal policies and procedures
- To maintain service availability as specified in section 6.2.6.

6.6 Information for relying parties

Please refer to the obligations of Relying Parties in section 6.2.4.

7. TSA Management and Operation

7.1 Introduction

DESC applies implements various policies and controls to ensure the trustworthiness of the Dubai TSA and its underlying infrastructure.

The following subsections elaborate on those policies and controls that are defined as part of the Dubai PKI governance framework.

7.2 Internal Organization

The Dubai TSA is provided by DESC as part of the overall Dubai PKI services. Therefore, the Dubai TSA TSS is protected by DESC PKI security management program that covers:

- Physical security and environmental controls,
- System integrity controls, including configuration and change management, patch management, vulnerability management and malware/virus detection/prevention,
- Maintaining an inventory of all assets (PKI and non-PKI) and manage the assets according to their classification,
- Network security and firewall management, including port restrictions and IP address filtering,
- User management, separate trusted-role assignments, education, awareness, and training, and,
- Logical access controls, activity logging and monitoring, and regular user access review to provide individual accountability.

7.3 Personnel Security

Since the Dubai TSA is operated as part of Dubai PKI infrastructure, provisions in Section 5.3 (Personal Controls) of the CP/CPS shall also apply for the TSA.

7.4 Asset Classification and Management

In order to ensure that information and other assets receive appropriate security treatment, DESC maintains 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 CP/CPS.

7.5 System Access Management

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

The systems' access management controls for the Dubai TSA are incorporated within the overall Dubai PKI systems access management controls. Additional information is provided in Section 5 (Facility, management and operational controls) of the CP/CPS and Section 6 (Technical security controls) of the CP/CPS.

7.6 Cryptographic controls

7.6.1 TSU Key Generation

DESC shall generate the cryptographic keys used in its TSU service 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 to do so under the Dubai PKI practices.

Additional information is provided in Section 6.1 (Key generation and installation) of the CP/CPS. The keys shall be generated within TSU Hardware Security Modules (HSMs) that are certified to FIPS 140-1 Level 3. Algorithms and key size are described in Section 6.1.6 (Key sizes) of the CP/CPS.

7.6.2 TSU Private Key Protection

DESC 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 to do so under the Dubai PKI practices.

7.6.3 TSU public key distribution

The current TSU certificate is published on DESC public repository: https://ca-repository.desc.gov.ae/.

The TSU doesn't not issue TSTs before its signature verification (public key) certificate is loaded into the TSU and its HSMs.

7.6.4 Rekeying TSU's Key

TSU private signing keys is replaced every 15 months. Additional information is provided in Section 4.6, Certificate renewal and Section 4.7 (Certificate re-key) of the CP/CPS.

7.6.5 Life cycle management of signing cryptographic hardware

DESC has procedures in place to ensure that hardware security modules 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 is performed based on dual control of authorized personnel with trusted roles, and the devices operate in a physically secured environment.

TSU private signing keys stored on TSU HSMs shall be erased upon device retirement in a way that it is impossible to recover them.

Additional information is provided in Section 6.6 (Life cycle technical controls) of the CP/CPS.

7.6.6 End of TSU key life cycle

TSA private signing keys shall be destroyed upon their expiry.

The TSA shall reject any attempt to issue time-stamps once a private key has expired.

The TSU key/certificate validity period is defined in section 7.1 of the Timestamping CA CPS [7].

7.7 Time-Stamping

7.7.1 Time-stamping

DESC 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

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

7.7.2 Clock Synchronization with UTC

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

TSUs shall have technical measures in place to ensure that their time is synchronized with UTC within the declared accuracy. Audit and calibration records are maintained by DESC.

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

The TSA 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 TSA must not issue time-stamps until correct time is restored.

7.8 Physical and Environmental Security

Since the Dubai TSA is operated as part of Dubai PKI infrastructure, provisions in Section 5 (Facility, management and operational controls) and Section 6 (Technical security controls) of the CP/CPS shall also apply for the TSA.

7.9 Operation Security

The operations security controls for the Dubai TSA are incorporated within the overall Dubai PKI operations management controls. Additional information in relation to operations management is provided in Section 5 (Facility, management and operational controls) of the CP/CPS.

7.10 Network Security

Since the TSS is deployed on the same infrastructure of the Dubai PKI, network security controls as the same applied for the Dubai PKI that are specified in section 6.7 of the CP/CPS.

7.11 Incident Management

The incident management procedures for the TSS are the same that followed for the Dubai PKI which are specified in section 5.7 of the CP/CPS. The below system critical activities are particularly monitored:

- Abnormal system activities that indicate a potential security violation, including intrusion into the network, are detected and reported as alarms,
- Desynchronization of the TSS clocks,
- Start-up and shutdown of the logging functions,
- Availability and utilization of cores services within the PKI network.

7.12 Collection of Evidence

DESC shall maintain records of all relevant information concerning the operation of the Dubai TSA at least two years after the revocation or renewal of the TSU Certificate private key, this includes the following:

1. Time-stamp requests and created time-stamps,
2. Events related to TSA administration (including certificate management, key management and clock synchronization),
3. Events relating to the life cycle of TSA keys and certificates,
4. Physical or remote access to a timestamp server, including the time of the access and the identity of the individual accessing the server,
5. History of the timestamp server configuration,
6. Any attempt to delete or modify timestamp logs,
7. Security events, including:
    a) Successful and unsuccessful Timestamp Authority access attempts;
    b) Timestamp Authority server actions performed;
    c) Security profile changes;
    d) System crashes, hardware failures, and other anomalies; and
    e) Firewall and router activities;
8. Revocation of a timestamp certificate,
9. Major changes to the timestamp server's time,
10. System startup and shutdown.

Records shall be time-stamped to protect data integrity and moved to a protected server for storage and subsequent archiving.

Records shall be treated as confidential in accordance with the CP/CPS. 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 other legal requirement.

7.13 Business continuity management

DESC disaster recovery plan defines the steps to be taken in case of (suspected) compromise of a TSU's private signing key or loss of calibration of a TSU clock.

In case of compromise, The TSU shall not issue Timestamps until steps are taken to recover from the compromise.

In case of compromise of the operations, (suspected) compromise or loss of calibration, DECS will make available, as appropriate, a description of compromise that occurred to Subscribers and Relying Parties.

In case of major compromise of the operations or loss of calibration, DECS will make available, as appropriate, to Subscribers and Relying Parties, information which can be used to identify the Timestamps which may have been affected, unless this breaches the privacy of the TSAs users or the security of the TSA services.

7.14 TSA Termination

In the case of termination of the Dubai TSA, DESC shall follow the procedures in Section 5.8 (Certificate authority and/or registration authority termination) of the CP/CPS and also more detailed internal DESC termination procedures.

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

7.15 Compliance

The Dubai TSA shall comply with applicable legal requirements as applicable in Dubai.

The Dubai TSA Service complies with the IETF RFC 3161 and RFC 5816 specifications. It also supports ETSI EN 319 422 time stamping profile and ETSI EN 319 421 policy requirements for time stamping authorities.

8. TSA disclosure statement

8.1 TSA contact info

Inquiries, suggested changes or notices regarding this document and the Dubai TSA should be directed to **Dubai PKI Policy Authority:**

Dubai Electronic Security Center

PO Box 36996, Dubai, UAE

Phone +97144150400

E-mail pa@desc.gov.ae

8.2 Time stamp tokens and usage

Supported signing algorithms is sha256WithRSAEncryption (RSA 2048).

Acceptable Time Stamp Request Hashes include SHA-256, SHA-384 and SHA-512. The digital signature on the Time-Stamp Token (TST) has a validity period of Five (5) years. The signatures are generated within a high-quality and high-security HSM (Hardware Security Module) with FIPS 140-2 Level 3 certification.

8.3 Reliance limits

The accuracy of the time reference included in time-stamp tokens is ± 1 second, with reference to UTC (Universal Time Coordinated).

8.4 Obligations of subscribers

Refer to section 6.2.3 of this document.

8.5 Obligations of relying parties

Prior to relying on a TST issued by the Dubai TSA, it is the responsibility of the relying party to verify that the time-stamp token is correctly signed (that is, it contains a valid electronic signature) and that the TSU certificate is not revoked, by checking the suitable CRL or OCSP responder as specified within the TSU certificate.

Refer to section 6.2.4 for more details.

8.6 Warranty and liability

DESC makes no express or implied representations or warranties relating to the availability or accuracy of the time-stamping service.

DESC shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use

of any computer or other equipment save as may arise directly from breach of this TSP/TSPS, applicable CP/CPS, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term “loss” means a partial loss or reduction in value as well as a complete or total loss.

8.7 Applicable policies and practices

The Timestamping Policy/Practice Statement (this document),

Subordinate CA Certificate Policy [6],

Timestamping CA Certification Practice Statement [7].

The above documents are published on DESC public repository: https://ca-repository.desc.gov.ae/.

8.8 Privacy Policy

Refer to sections 9.3.3 and 9.4 of the CP/CPS.

8.9 Refund Policy

DESC does not refund fees for time-stamp services.

8.10 Applicable law, complaints and conflict resolution

The laws of Dubai shall govern the enforceability, construction, interpretation and validity of the present TSP/TSPS. All disputes associated with this document will be in all cases resolved according to the laws of Dubai.

8.11 TSA Audit

The Dubai PKI (Particularly the Dubai TSA) is subject to compliance with the below requirements published at https://www.cpacanada.ca:

- WebTrust Principles and Criteria for Certification Authorities,
- WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements.