TRUSTED NATIONAL INFRASTRUCTURE TECHNICAL CA

TERMS OF USE OF TIMESTAMPS TOKENS

Document Status - Classification	Reference
Current - Public	2.16.492.1.1.1.1.6.3

Version	Date	Description
1.0	4/11/2021	Initial version
1.1	04/03/2022	Modified version
1.2	07/09/2022	Modified version

Table of contents

1 PURPOSE

The purpose of these Terms of Use (or “Terms of Use” of timestamps tokens, hereinafter referred to as "GTCs"), which serve as the TSA Disclosure Statement as defined by ETSI, is to set out the procedures for issuing and using timestamp tokens, also known as timestamps, offered by the Time Stamping Authority (TSA) of Prince's Government (hereinafter referred to as the Government) as well as the respective commitments and obligations of the various parties involved.

The TSA’s timestamping service is responsible for generating and managing timestamps with respect to Subscribers and Users of these timestamps.

These GTCs apply to any subscriber and User of a timestamp token who requests and/or uses the tokens generated by the Government’s timestamping service.

Subscriber and timestamp User confirm that he/she has read and understood the entirety of these GTCs before requesting and/or using a timestamp token and undertakes to adhere to them.

2 DEFINITIONS

The following words and phrases, beginning with a capital letter, in the singular or plural, are employed herein with the meanings specified below:

Subscriber – Entity needing to have data time stamped by a Time Stamping Authority, and which has accepted the terms of use of said authority’s services. This notion is valid for scenarios where the time stamp is requested directly from the TSA.

Certification Authority (CA) - Entity issuing Certificates after checks on the identity of the person or representative of the application system, or the procedure leading to their identification. The CA is responsible for all the material, human, and organisational components used in the process of creating and managing Certificates.

Time Stamping Authority (TSA) - Entity responsible for managing the timestamping environment and the production of timestamp tokens on data presented to it, to certify the existence of those data on the date of the timestamp.

Terms of Use or GTCs - Refers to these Terms of Use (GTCs).

Timestamp or timestamp token - Signed datum that links a representation of a datum to a given time, expressed in UTC, thus proving that the datum existed at that point in time.

Universal Time Coordinated (UTC) - Time scale based on the second, as defined in ITU-R TF.460-5 [TF.460-5] recommendation.

N.b. For most uses, UTC time is equivalent to mean solar time at the prime meridian (0°). More accurately, UTC time is a compromise between atomic time (International Atomic Time – IAT), which is particularly stable, and solar time derived from the Earth’s irregular rotation linked to Greenwich Mean Sidereal Time (GMST) by a conventional relationship.

Timestamping - Service which securely associates an event and a time, to reliably establish the time at which the event took place.

Electronic timestamping - Data in electronic format which associate other data in electronic format with a given time, proving that the data concerned existed at that time.

Qualified electronic timestamping - Electronic timestamping that meets the requirements stipulated in Articles 32 and 33 of the [RGSP].

Timestamp token - See timestamp.

Certificates Revocation List (CRL) – List of certificates that have been revoked before the end of their validity period.

Timestamping Policy (TSP) - All of the rules, identified by a name (OID), which define the requirements met by a TSA when establishing and providing its services, indicating the applicability of a timestamp to a particular community and/or class of applications with common security requirements. A TSP may also, if necessary, identify obligations and requirements for other parties, including subscribers and users of timestamps.

Timestamping service - All the services required to generate and manage timestamps.

Timestamping system - All the timestamping units and administration and supervision components used to provide timestamping services.

Timestamping Unit (TSU) - All the hardware and software used to create timestamps, characterised by an identifier of the timestamping unit granted by a CA, and a unique timestamp signing key.

UTC(k) - Reference time realised by a "k" laboratory and precisely synchronised with UTC time, in order to achieve an accuracy of ±100 ns, according to recommendation S5 (1993) of the Consultative Committee for definition of the Second (Rec. ITU-R TF.536-1 [TF.536-1]).

N.b. A list of UTC(k) laboratories can be found in section 1 of Circular T published by the BIPM and on the BIPM website (www.bipm.org).

Timestamp user - Entity (person or system) who trusts a timestamp issued under the Timestamping Policy of a given Time Stamping Authority.

3 CONTACT DETAILS

Requests for information regarding the issuance of timestamp tokens by the Government's TSU carried out by the Digital Services Department can be made:

- By post: to the Digital Services Department (Direction des Services Numériques - DSN), whose headquarters are at 2 rue du Gabian, Immeuble "Les Industries", BP 673 MC, 98014 Monaco Cedex.
- By email to the following address: service-horodatage@gouv.mc

4 USE OF TOKENS

Electronic timestamping is a trusted service used to certify that data in electronic format exist at a given point in time.

This service entails associating an unequivocal representation of the data concerned with a given point in time, to a predefined degree of accuracy based on universal time.

The electronic timestamping service is requested by Subscribers wishing to obtain a timestamp certificate, and who are responsible for providing timestamps to their users.

Technically, a timestamp token is a digitally signed structure that contains, specifically:

- The Timestamping Policy identifier under which the timestamp token was generated
- The hash value and hash algorithm of the timestamped data
- The date and UTC time
- The certificate identifier of the TSU that generated the timestamp (the certificate also identifies the TSA)

The validity of the private signature keys used to sign the timestamp token is one (1) year, and the keys are renewed annually. The associated Timestamp Certificate is valid for three (3) years to enable autonomous verification of timestamps throughout the period.

The hash function used to create the timestamped object is SHA 256.

5 LIMITATION OF USE

Use of tokens is limited to the purposes described in Article 4 of these GTCs.

6 CONDITIONS FOR OBTAINING AND USING TOKENS

6.1 REQUESTING A TOKEN

The service for issuing timestamp tokens has been evaluated by an organisation accredited by the French Accreditation Committee (COFRAC). This service complies with the published TSP.

6.1.1 *Requesting a timestamp token*

For subscribers:

Requests for timestamp tokens should be submitted to the Timestamping Service of the Prince's Government's TSA in accordance with the [RFC 3161] protocol via the URL https://time.mconnect.mc.

Timestamp Users:

Applications for timestamp tokens are handled by the Subscriber's Service.

6.1.2 *Token generation process*

The Subscriber accesses https://time.mconnect.mc and requests a timestamp token for the application for which the Subscriber wants the token.

The platform issues the token.

Timestamps are issued at the discretion of the TSA.

6.2 USE OF TIMESTAMP TOKENS

Timestamp tokens are used only for the purposes set out in Article 4 of these GTCs.

Notifications are published on the reference website mconnect.gouv.mc in the event of problems likely to impair the integrity and availability of the service.

The timestamping service is available 24/7, 365 days a year, except in the event of force majeure, which will be announced on the website mconnect.gouv.mc.

7 OBLIGATIONS

Obligations of the Time Stamping Authority

The TSA generates and signs timestamps in accordance with the following documents: the TSP and these GTCs.

The TSA guarantees compliance for all stakeholders involved in the management of timestamps with regard to the requirements and procedures set out in the TSP.

The TSA fulfils all its commitments, as stipulated in these Terms of Use.

The TSA guarantees the conformity of the requirements and procedures defined in the TSP.

The TSA makes available to subscribers and users all the information required to verify timestamps.

The TSA respects the conditions for availability of the timestamping service contractually agreed with subscribers.

The TSA maintains information on the compromise of the TSU key pair.

Obligations of the Subscriber:

The Subscriber shall verify that the timestamp certificate issued by the certification chain of the Prince's Government's Root Certification Authority, used to issue tokens, has not been revoked.

The Subscriber shall also check that the data to which the timestamp is applied are the data sent for timestamping.

The Subscriber must be declared and authorised by the TSA to request timestamps.

The timestamp User and the Subscriber assure the Administration that they own the documents that they are timestamping.

Obligations of the timestamp User:

Timestamps Users must respect the [RFC 3161] protocol.

It is recommended that users validate the timestamp tokens received.

Timestamp Users are obliged to take all measures required to ensure the security of the computer on which the timestamp tokens are used.

Any timestamp User may verify whether the timestamp Certificate used to sign the timestamp has been revoked. Users may verify whether the certificate is included in the Certificate Revocation List (CRL) specified by the distribution point in the timestamp Certificate associated with the timestamp.

If the timestamp Certificate has been revoked, it is the responsibility of the recipient of the signed document to determine if the Certificate can reasonably be trusted.

The DSN cannot, under any circumstances, be held liable if the certificate is revoked.

Revoked certificates continue to be included in the CRL even after their original expiry date has passed. If the TSA permanently ceases activity, a final CRL will be issued with an expiry date set to 31 December 9999, 23h59m59s.

Timestamp Users must consider the limitations on the use of timestamps mentioned in the Terms of Use.

Timestamp Users and Subscribers ensure the Administration that they own the documents that they are timestamping.

Obligations of the CAs supplying TSU certificates

TSU certificates are qualified. They are issued by the TECHNICAL CA.

The conditions for terminating the relationship with the TSA are published in paragraph 3.7 of the TSP.

8 LIABILITY

Tokens must not be used in an abusive or malicious manner.

The user undertakes to use tokens:

- In compliance with the laws and regulations of Monaco, and the rights of third parties
- Fairly and in accordance with their use
- At their own risk.

The timestamps issued in compliance with the applicable TSP must be a Timestamp Token structure in accordance with [RFC3161].

To ensure the quality of the timestamp token, the end user notes the certificate's attributes and checks that the following fields are correct:

Field	Comments	Value
	Version of the format	1
policy	OID of the TSP	2.16.492.1.1.1.1.6.11.2
	OID of the hash algorithm (imprint)	Hash algorithm: sha256
	Hash of data to be timestamped (message data)	Identical to the values included in the request
serialNumber	Unique timestamp identifier	Generated by the TSU
	Time of the timestamp	Time of the TSU at the moment of generation
accuracy	Declared accuracy	1 second
	Ordering information	false

nonce	Anti-replay data	Identical to that in the request if there is a nonce present
	TSU identifier	"subject" field of the TSU timestamp certificate
extensions	Optional supplementary extensions	No supplementary extension

The timestamp User acknowledges and accepts that the DSN cannot be held responsible as part of the timestamp token issuing service in the event of alteration, or any use that is illicit or prejudicial to a timestamp User or a third party in the network by a third party.

The timestamp User assumes full responsibility for any consequences resulting from his/her faults, errors, or omissions.

The timestamp User assures the Administration that the User owns the documents that he or she is timestamping. The Administration is not responsible for the legality and conformity of the documents signed through its Timestamping Service.

The Administration is not responsible if the timestamp token of a document does not comply with the timestamping conditions for this type of document.

The timestamp User bears sole responsibility for the lifecycle of the documents that he or she timestamps, from their creation until the end of their retention period.

The timestamp User shall refrain from using or attempting to use the timestamp token for any purpose other than those provided for herein and by the token itself.

The terms of these GTCs may also be amended at any time, without prior notice, according to modifications made by the DSN, changes in legislation or any other reason deemed necessary. It is the timestamp User's responsibility to inform him/herself of the said terms.

9 LIMITS OF GUARANTEES AND LIABILITY

Under no circumstances does the DSN, as manager of the technical CA, nor the Prince's Government, intervene, in any way whatsoever, in the contractual relations that may be established between the Users of timestamps, and recipients of timestamped documents.

The DSN, as manager of the technical CA, assumes no responsibility or liability for the consequences of any delay or loss in the transmission of any electronic message, letter, or document, or for any delay, corruption, or other error that may occur in the transmission of any electronic communication.

The DSN, as manager of the technical CA, cannot be held responsible for compromise of the private key or the accidental or unintentional failure of the TSA's Timestamping Service. The DSN, as manager of the technical CA, is not entrusted with the storage and/or protection of the private key of the Certificate.

10 DATA RETENTION

No personal data is retained during the creation of timestamps for timestamp Users.

Data from Subscriber registration files is retained for the duration of their subscription. Personal information belonging to Subscribers is the nominative information of the manager of the application service mentioned in the registration file.

Data retention is undertaken in compliance with the level of protection appropriate to the personal data whose management is the subject of paragraph 12.

The technical logs are kept in a secure space for a period of one year and are then erased.

11 INTELLECTUAL PROPERTY

The trademarks and/or logos owned by the DSN, as manager of the technical CA, appearing on all media, are trademarks protected by the legal provisions applicable in Monaco.

Any representation or reproduction, whether total or partial, is prohibited and constitutes a criminal offence that will be punished by the Monaco courts, unless express permission is obtained from the Administration.

12 PROTECTION OF PERSONAL DATA

The DSN processes personal data for the following purpose: “Provision of trusted services for the digital identity”, for which the relevant Decision was issued on 2 June 2021 with a favourable opinion:

Délibération n° 2021-112 du 2 juin 2021 de la Commission de Contrôle des Informations Nominatives portant avis favorable à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « Fourniture des services de confiance pour l'identité numérique » dénommé « MConnect et MConnect Mobile » exploité par la Direction des Services Numériques et présenté par le Ministre d'État.

13 APPLICABLE LAW, DISPUTE SETTLEMENT

The parties expressly agree that only Monegasque legislation and regulations are applicable.

They undertake to seek an amicable agreement in the event of a dispute. At the initiative of the requesting party, a meeting will be held. Any agreement to settle the dispute must be recorded in writing on a document signed by an accredited representative of both parties.

In the event of a dispute relating to the interpretation, formation or performance of the Contract and failing to reach an amicable agreement, the parties hereby give express and exclusive jurisdiction to the competent courts of the Principality of Monaco.

14 INDEPENDENCE OF THE PARTIES AND NON-DISCRIMINATION

The organisation implemented by the TSA is dedicated to its activities and ensures the separation of roles. It preserves the impartiality of operations and ensures that the trusted activities provided are undertaken in an equivalent manner for all beneficiaries who have accepted the general conditions of use of the service and who respect the obligations incumbent upon them.

Wherever possible, the TSA shall implement appropriate approaches to make its service accessible to all persons, including those with disabilities, considering the specificities of each applicant on a case-by-case basis.

In general, the services provided by the TSA such as the generation of timestamp tokens are performed independently and are therefore not subject to any pressure.