TRUSTED NATIONAL INFRASTRUCTURE
TECHNICAL CA
TERMS OF USE OF TIMESTAMP CERTIFICATES

Document Status - Classification	Reference
En cours - Publique	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	31/08/2022	Modified version

Table of contents

1 PURPOSE

The purpose of these Terms of Use (or "Terms of Use for certificates", hereinafter referred to as "GTCs") is to set out the terms and conditions for the issuance and use of electronic timestamp certificates, offered by the Prince's Government (hereinafter referred to as the Government) as well as the respective commitments and obligations of the various parties involved.

These GTCs apply to any Applicant requesting the electronic timestamp certificates offered by the Government and using the said certificates.

The Certificate Manager confirms that he/she has read and understood the entirety of these GTCs before using the certificate 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.

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.

Applicant - The Applicant is the natural person who applies to a Registration Authority to obtain a timestamp certificate.

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].

Trusted National Infrastructure (TNI) - The TNI is the set of components, functions and procedures dedicated to the management of cryptographic keys and their certificates used by trusted services implemented by the Monaco Cyber Security Agency (AMSN) on behalf of the Prince's Government.

The TECHNICAL CA is one of the authorities attached to the TNI.

TNI Security Officer - The person who is responsible, under the orders of his or her employing authority, for establishing the security rules and instructions to be implemented with respect to persons and protected information or media and for verifying their implementation.

Timestamp token - See timestamp.

Certificate Revocation List (CRL) – List of certificates that have been revoked before the end of their validity period.

Timestamping Policy (TSP) - All 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.

The TSP of the Technical CA: 2.16.492.1.1.1.1.6.11.2

Certification Policy or CP : The CP of the Technical CA refers to the document that establishes the principles that apply to the Certification Authority, to subscribers Holders involved in the entire lifecycle of a certificate, (which can be consulted at the following address: https://mconnect.gouv.mc/technique)

The CP identifiers applicable to these GTCs are:

- The CP of Root Certification authority: 2.16.492.1.1.1.1.1.1.
- The CP of Technical CA: 2.16.492.1.1.1.1.6.1.

Certificate Manager or CM - The concept of Certificate Manager applies only to final certificates. The Certificate Manager is the person to whom has been delivered the certificate, whether via face-to-face or by e-mail.

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

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 "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 Certificates provided by the Digital Services Department can be made:

- By post: to the Digital Services (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 TYPES OF CERTIFICATES AND USES

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.

The Technical CA issues various certificate profiles, each identified by a specific OID. Their uses are indicated in the certificate template.

Certificate types and uses are described in the CP with the Object Identifier (OID) 2.16.492.1.1.1.1.6.11.2

Timestamping and authentication services (via MConnect) are available 24/7, 365 days a year, except in the event of force majeure, which will be announced on the website mconnect.gouv.mc.

Notifications are made on the reference site mconnect.gouv.mc in the event of problems that could affect the integrity and availability of the service.

5 LIMITATION OF USE

The CM must strictly respect the authorised uses of the key pair and the Certificates. In the case of fraudulent use, they may be held responsible.

The authorised use of the key pair and the associated Certificate is specified in the Certificate itself.

The use of the CM's private key and the associated Certificate, is strictly limited to the service defined by the identifier of his/her CP.

The CM, acknowledges that he/she has been informed that fraudulent use or use that does not comply with the present GTCs, as well as with the authorised use of the key pair and the Certificate, is a legitimate reason for revocation by the CA.

The use of Certificates is limited to the uses described in the CP.

6 CONDITIONS FOR OBTAINING AND USING THE CERTIFICATE

6.1 APPLICATION FOR CERTIFICATE AND SUPPORTING DOCUMENTS

6.1.1 *Application for certificate*

Applications for Timestamp Certificates must be made to the Technical CA of the Prince's Government by means of a registration file.

The registration service offered by the CA is available, by appointment, during the opening hours of the Digital Services Department.

6.1.2 *Enrolment and production of electronic certificates*

- Receipt of the timestamp certificate application form (with acceptance of these Terms of Use) by the Registration Operator (DSN)
- Verification of the identity (identity document: identity card, passport, or residence permit) and authorisation of the Applicant to apply for a Timestamp Certificate
- Generation of the timestamp certificate by the Registration Operator

The qualified certificate issuance service has been evaluated by an organisation accredited by the French Accreditation Committee (COFRAC). This service complies with the published CP.

6.2 ISSUANCE OF CERTIFICATE AND ACCEPTANCE

6.2.1 *Issuance of the timestamp certificate*

The process for issuance of the timestamp certificate is as follows:

- Issuance of the timestamp certificate (returned to the CM by email)
- Issuance of a delivery document and signature by the CM or Authorised Representative and the Registration Operator and archiving by the Registration Operator
- Archiving of the file

To guarantee the quality of the certificate issued by the Technical CA, the CM notes the certificate's attributes and checks that the fields are correct (Issuer, CA, validity dates, object, Key usage=digitalsignature (Digital signature) et Extended Key Usage = Timestamping)).

6.3 USE OF THE CERTIFICATE

The Certificate shall only be used for the purposes defined in Article 4 of the present GTCs.

6.4 RENEWAL OF CERTIFICATES

The electronic Certificates is valid for three (3) years.

The certificate will be renewed every year (1).

The procedure will be the same as for the initial application.

6.5 REVOCATION

The possible causes of a revocation are described in the CP.

When certificates are issued, the registration operator of the technical CA sends the CM a revocation code.

This revocation code is sent by email when the certificate is issued.

If the certificate is compromised or needs to be revoked for any other reason, the CM must contact the Registration Operator by email (service-horodatage@gouv.mc) (24/7), who will authenticate and revoke the certificate.

Authentication is performed by the Registration Operator, either:

- Via the revocation code (provided when the certificate was issued)
- Or using the personal questions entered in the timestamp certificate application form.

He then confirms for the CM that the certificate has been correctly revoked.

The request to revoke the Certificate may also be made by the Authorised Representative or the Legal Representative, who will be authenticated by the Registration Operator using the personal questions entered when the registration file was submitted.

The CA Manager, the C2SC Manager, or a judicial authority, may also send an official letter to the Registration Operator of the AE or the TNI Security Officer, to effect the revocation.

- Consulting the status of a Certificate:

The Certificate Manager may check the status of his/her Certificates at any time by consulting the available CRL (Certificate Revocation List), or by asking the online Certificate Status Service (OCSP), which features a "certificate revoked" response after the certificate's expiry date. Revoked certificates remain in the CRL even after their original expiration date. In the event of permanent cessation of CA activity, a final CRL will be issued with an end of validity date of 31 December 9999, 23h59m59s.

7 OBLIGATIONS

The CM is obligated to take all specific steps to ensure the security of the computer and hardware on which the timestamping certificate and media are used.

The CM undertakes to generate and store the certificate in a HSM corresponding to the category declared when the certificate application form was submitted, to preserve the integrity and confidentiality of his/her private key.

Knowledge of proven or suspected compromise of confidential data, failure to respect the present general conditions, the death of the CM, or modification of the data contained in the Certificate, by the CM, or by the DSN, entails an obligation, on their part, to request the revocation of the associated Certificate as soon as possible.

The CM undertakes to no longer use a Certificate following its expiration, a request for revocation or notification of the revocation of the Certificate, whatever the cause.

The CM undertakes to verify the use indicated in the Certificate.

Obligations of the CA:

In the event of a revocation requested by the Holder, respectively the CM, the DSN shall revoke the Certificate within less than twenty-four (24) hours after a request by the applicant.

The conditions for ending relations with the TECHNICAL CA are published in paragraph 4.11 of the CP.

Obligations of the TSA:

- Ensure that all the requirements detailed in the following chapters are met
- Guarantee the application of procedures under this policy, whether the TSA functions are outsourced or not
- Ensure that the resources employed fully meet the requirements of the TSP
- Undertake to keep the specified elements of the TSP confidential. As regards timestamp tokens, the TSA will ensure that the Timestamping Service:
    - Meets the requirements of the TSP
    - Accepts periodic audits of compliance with the TSP.

8 LIABILITY

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

The Certificate Manager undertakes to use the Certificates:

- 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.

To ensure that the certificate issued by the technical CA is compliant with requirements, the Certificate Manager checks the certificate's attributes and checks that the following fields are correct:

- Issuer
- CA
- Validity dates
- Object
- Key usage = digitalsignature
- Extended Key Usage = timestamping

The Certificate Manager acknowledges and accepts that the DSN cannot be held responsible for its certificate issuance activity, particularly in the event of alteration, any illicit or prejudicial use of the Certificate Manager, or a third party in the network by a third party.

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

The Administration is not responsible for the legality and conformity of the documents timestamped through its Service.

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

The Certificate Manager shall refrain from using or attempting to use the Certificate for the authorised functions or uses of key pair for any purpose other than those provided for herein and by the Certificate 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 Certificate Manager'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, intervene, in any way whatsoever, in the contractual relations that may be established between the CM, the TSA, Subscribers, and users of timestamps.

The DSN, as manager of the technical CA, does not assume any commitment or responsibility as to the form, sufficiency, accuracy, authenticity, or legal effect of the documents submitted at the time of the application for a Certificate.

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. The DSN, as manager of the technical CA, is not entrusted with the storage and/or protection of the private key of the Certificate.

The parties expressly agree that the DSN, as manager of the technical CA, cannot be held liable in any way if the Certificate Manager has not requested the revocation of the Certificate in accordance with the provisions of this document.

10 DATA RETENTION

Data is kept during the creation of the registration file as soon as the request to provide a Certificate is made.

Personal information is the nominative information of the applicant mentioned in the registration file.

This data is kept for ten (10) years. The storage period is seven (7) years after the expiration date of the Certificate (the lifetime of a Certificate is three (3) years).

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 June 2nd, 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 CA 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 CA 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 CA such as, but not limited to, certificate generation, revocation management and certificate status are performed independently and are therefore not subject to any pressure.