TIME-STAMPING CERTIFICATION PRACTICE STATEMENT



Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

General information

Document control

Security classification:	**Public**
Version:	**2.3**
Issue date:	**25/11/2026**
File:	**3GMG_DPC_TSA_v2.3**

Formal status

Prepared by:	**Reviewed by:**	**Approved by:**
Name: Roger Callarisa Fecha: 25/11/2026	Name: José María Del Olmo Gil Fecha: 25/11/2026	Name: José Antonio Santiso Martínez Fecha: 25/11/2026

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

Version control

Version	Sections changed	Description of change	Author of change	Date of change
Version	Sections changed	Description of change	Author of change	Date of change
1.0	Original	Creation of the document	Alejandro Grande	12/07/2021
1.1	6.8	A section is added on the accuracy of the time in the qualified time-stamp	Alejandro Grande	27/09/2021
1.2	1.3	Section 1.3, on the Participants in the certification service, is amended to add, in item "1.3.1 Certification Service Provider", the hierarchy of Certification Authorities	Laura Paniagua	15/07/2025
	1.3.5.1.	Section 1.3.5.1 is added, on the obligations of the Public Key Infrastructure Provider.		
	6.1.8	Section 6.1.8 is added, on the hash algorithms used in the service.		
	6.4.2.9	Section 6.4.2.9 is added, on the life-cycle management of the cryptographic hardware.		
	9.4.1, 9.4.1.1; 9.4.1.2; 9.4.1.3; 9.4.1.4	Sections are added on Notification to the Supervisory Body.		
	9.4.2; 9.4.2.1; 9.4.2.2; 9.4.2.3; 9.4.2.4	Sections are added on Notification to the data protection authority		
2.0	1.3.2	The details of the 3GMG Certificate Hierarchy are added.	Roger Callarisa	28/08/2026
	4.7.7	Section 4.7.7 is amended, establishing the obligation to check the revocation or suspension status information of the certificates.		
	6.1, 6.1.4, 6.2.1, 6.6	All sections relating to the Common Criteria certifications of the HSMs, as well as to key length, are amended.		

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

	6.7 AND 6.9 6.8 AND 6.10	The following sections are amended, correctly establishing the time sources of the 3GMG time-stamping service The sections have been duly updated, defining the Secure Signature Creation Devices (SSCD)		
2.1	1.3.2.3	The details of the new 3GMG TSU Certificate "3G QUALIFIED TSU 01 2026" are added.	Roger Callarisa	14/10/2026
2.2	1.3.1, 1.3.2, 1.4.1, 1.5, 5.7, 5.9, 6.1.1, 6.1.8, 6.2.6, 6.2.8, 8.1	A complete review of the Document has been carried out, covering the sections on the full identification of the TSU 01 2026 certificate and of 3G QUALIFIED TSU 01 at 2,048; the declared time-stamping policies; the period of use of the private key; the SHA3-256 and SHA3-512 algorithms; and key withdrawal, revocation and destruction. The regulatory framework, the deadline for notifying the Supervisory Body of cessation, and the audit frequency have been updated.	Roger Callarisa	23/11/2026
2.3	5.7	The CPS has been reviewed to correctly establish the renewal and validity of the keys.	Roger Callarisa	25/11/2026

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

Index

Contents

GENERAL INFORMATION 2

DOCUMENT CONTROL 2

FORMAL STATUS 2

VERSION CONTROL 3

INDEX 5

1. INTRODUCTION SCOPE 11

1.2 SCOPE 11

1.3 DOCUMENT NAME AND IDENTIFICATION 11

1.3 PARTICIPANTS IN THE CERTIFICATION SERVICES 11

1.3.1. Certification Service Provider 11

1.3.2. Time-Stamping Authority 12

1.3.3. Subscribers of the certification service 13

1.3.4. Relying parties 14

1.3.5. Public Key Infrastructure Services Provider 14

1.4. USE OF THE TIME-STAMPING SERVICE 15

1.4.1. Permitted uses 15

1.4.2. Limits and prohibitions on use 16

1.5. POLICY ADMINISTRATION 16

1.5.1. Organisation administering the document 16

1.5.2. Contact details of the organisation 16

1.5.3. Document management procedures 17

2. PUBLICATION AND PRESERVATION 18

2.1 REPOSITORY 18

2.2 PUBLICATION OF INFORMATION BY THE CERTIFICATION SERVICE PROVIDER 18

2.3 FREQUENCY OF PUBLICATION 18

2.4 ACCESS CONTROL 18

3. IDENTIFICATION AND AUTHENTICATION 20

3.1. INITIAL REGISTRATION 20

3.1.1. Types of names 20

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

3.1.2. Meaning of names 20
3.1.3. Use of anonyms and pseudonyms 20
3.1.4. Interpretation of name formats 20
3.1.5. Uniqueness of names 20
3.2. INITIAL IDENTITY VALIDATION 21
3.3. IDENTIFICATION AND AUTHENTICATION FOR RENEWAL REQUESTS 21
3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION, SUSPENSION OR REACTIVATION REQUESTS 21
4. OPERATIONAL REQUIREMENTS 22
4.1 REQUEST FOR THE ISSUANCE OF TIME-STAMPS 22
4.1.1. Standing to request the time-stamping service 22
4.1.2. Registration procedure and responsibilities 22
4.2 PROCESSING OF THE REQUEST 22
4.3 ISSUANCE OF THE TIME-STAMP 22
4.4 DELIVERY AND ACCEPTANCE OF THE CERTIFICATE 23
4.5 USE OF THE KEY PAIR AND THE CERTIFICATE 23
4.6 MODIFICATION OF CERTIFICATES 23
4.7 REVOCATION, SUSPENSION OR REACTIVATION OF CERTIFICATES 23
4.7.1. Causes for revocation of certificates 24
4.7.2. Causes for suspension of a certificate 25
4.7.3. Causes for reactivation of a certificate 25
4.7.4. Who can request revocation, suspension or reactivation 25
4.7.5. Procedures for requesting revocation, suspension or reactivation 25
4.7.6. Time limit for requesting and processing revocation, suspension or reactivation 25
4.7.7. Obligation to check certificate revocation or suspension information 26
4.7.8. Frequency of issuance of Certificate Revocation Lists (CRLs) 26
4.7.9. Maximum publication time of CRLs 27
4.7.10. Availability of online certificate status checking services 27
7.4.11. Obligation to consult certificate status checking services 28
7.4.12. Special requirements in the event of compromise of the private key 28
4.8. TERMINATION OF THE SUBSCRIPTION 28
4.9. KEY ESCROW AND RECOVERY 28
4.9.1. Key escrow and recovery policy and practices 28

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

4.9.2. Session key encapsulation and recovery policy and practices 29

5. PHYSICAL, MANAGEMENT AND OPERATIONAL SECURITY CONTROLS 30

5.1 PHYSICAL SECURITY CONTROLS 30

5.2 LOCATION AND CONSTRUCTION OF THE FACILITIES 31

5.2.1. Physical access 31

5.2.2. Electricity and air conditioning 32

5.2.3. Exposure to water 32

5.2.4. Fire prevention and protection 32

5.2.5. Media storage 32

5.2.6. Waste disposal 32

5.2.7. Off-site backup 33

5.3 PROCEDURAL CONTROLS 33

5.3.1. Trusted roles 33

5.3.2. Identification and authentication for each role 34

5.3.3. Roles requiring segregation of duties 34

5.4 PERSONNEL CONTROLS 35

5.4.1. Background, qualifications, experience and authorisation requirements 35

5.4.2. Background investigation procedures 35

5.4.3. Training requirements 36

5.4.4. Training refresher requirements and frequency 36

5.4.5. Job rotation sequence and frequency 36

5.4.6. Sanctions for unauthorised actions 37

5.4.7. Requirements for contracting professionals 37

5.4.8. Provision of documentation to personnel 37

5.5 SECURITY AUDIT PROCEDURES 37

5.5.1. Types of events recorded 37

5.5.2. Frequency of audit log processing 38

5.5.3. Retention period for audit logs 39

5.5.4. Protection of audit logs 39

5.5.5. Backup procedures 39

5.5.6. Location of the audit log accumulation system 40

5.5.7. Notification of the audit event to the cause of the event 40

5.5.8. Vulnerability assessment 40

5.6. INFORMATION ARCHIVING 40

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

5.6.1. Retention period for records 40
5.6.2. Protection of the archive 40
5.6.3. Backup procedures 41
5.6.4. Date and time-stamping requirements 41
5.6.5. Location of the archive system 41
5.6.7. Procedures to obtain and verify archive information 41
5.7. KEY RENEWAL 41
5.8. KEY COMPROMISE AND DISASTER RECOVERY 41
5.8.1. Incident and compromise management procedures 42
5.8.2 Corruption of resources, applications or data 42
5.8.2. Compromise of the entity's private key 42
5.8.3. Business continuity after a disaster 42
5.9 TERMINATION OF SERVICE 42
6. TECHNICAL SECURITY CONTROLS 44
6.1 KEY PAIR GENERATION AND INSTALLATION 44
6.1.1. Key pair generation 44
6.1.2. Delivery of the public key to the certificate issuer 45
6.1.3. Distribution of the certification service provider's public key 45
6.1.4. Key sizes 45
6.1.5. Public key parameters generation 45
6.1.6. Public key parameters quality checking 45
6.1.7. Key generation in software or in hardware 45
6.1.8. Hash algorithms used in the service 45
6.2. PRIVATE KEY PROTECTION 46
6.2.1. Cryptographic module standards 46
6.2.2. Multi-person control (n out of m) of the private key 46
6.2.3. Private key backup 46
6.2.4. Entry of the private key into the cryptographic module 46
6.2.5. Private key activation method 47
6.2.6. Private key deactivation method 47
6.2.7. Cryptographic module rating 47
6.3. COMPUTER SECURITY CONTROLS 48
6.4. LIFE CYCLE TECHNICAL CONTROLS 48
6.4.1. System development controls 48

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

6.4.2. Security management controls *49*
6.5. NETWORK SECURITY CONTROLS 51
6.6. CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 51
6.7. TIME SOURCES 52
6.8. ACCURACY OF THE TIME IN THE QUALIFIED ELECTRONIC TIME-STAMP 52
6.9. CHANGE OF STATUS OF A QUALIFIED SIGNATURE CREATION DEVICE (SSCD) 53
7. TSU CERTIFICATE PROFILE 54
7.1. 54
CERTIFICATE PROFILE 54
7.1.1. Version number *54*
7.1.2. Certificate extensions *54*
7.1.3. Algorithm object identifiers (OID) *54*
7.1.4. Name formats *54*
7.1.5. Name constraints *54*
7.1.6. Certificate type object identifier (OID) *55*
7.2. CERTIFICATE REVOCATION LIST PROFILE 55
Version number *55*
OCSP profile *55*
8. COMPLIANCE AUDIT 56
8.1. 56
FREQUENCY OF THE COMPLIANCE AUDIT 56
8.2. IDENTIFICATION AND QUALIFICATION OF THE AUDITOR 56
8.3. RELATIONSHIP OF THE AUDITOR WITH THE AUDITED ENTITY 56
8.4. LIST OF ELEMENTS SUBJECT TO AUDIT 56
8.5. ACTIONS TO BE TAKEN AS A RESULT OF A NON-CONFORMITY 56
8.6. HANDLING OF AUDIT REPORTS 57
9. COMMERCIAL AND LEGAL REQUIREMENTS 58
9.1. 58
FEES 58
9.1.1 Time-stamping service fee *58*
9.1.2. Fee for access to time-stamp status information *58*
9.1.3 Fees for other services *58*

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

9.1.4. Refund policy *58*
9.2. FINANCIAL CAPACITY 58
9.2.1. Insurance coverage *58*
9.2.2. Other assets *58*
9.2.3. Insurance coverage for subscribers and relying parties on time-stamps *58*
9.3. CONFIDENTIALITY 59
9.3.1. Confidential information *59*
9.3.2. Legal disclosure of information *59*
9.4. PERSONAL DATA PROTECTION 59
9.4.1. Notification to the Supervisory Body *62*
9.4.2. Notification to the national data protection authority *63*
9.5. INTELLECTUAL PROPERTY RIGHTS 65
9.6. OBLIGATIONS AND CIVIL LIABILITY 65
9.6.1. Obligations of 3G *65*
9.6.2. Warranties offered to subscribers and relying parties *66*
9.6.3. Disclaimer of other warranties *67*
9.6.4. Limitation of liability *67*
9.6.5. Fortuitous event and force majeure *67*
9.6.6. Governing law *67*
9.6.7. Severability, survival, entire agreement and notice clauses *67*
9.6.8. Competent jurisdiction clause *68*
9.6.9. Dispute resolution *68*
10. ANNEX I – ACRONYMS AND GLOSSARY 69

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

1. Introduction Scope

1.2 Scope

This document sets out the Certification Practice Statement for the Qualified Electronic Time-Stamp Issuance Service issued by 3G SOLUCIONES MOVILIDAD, S.L., hereinafter 3G, through the operation of the public key infrastructure (PKI) of Uanataca, S.A.U

1.3 Document name and identification

This document is the “3G Time-Stamping Certification Practice Statement”.

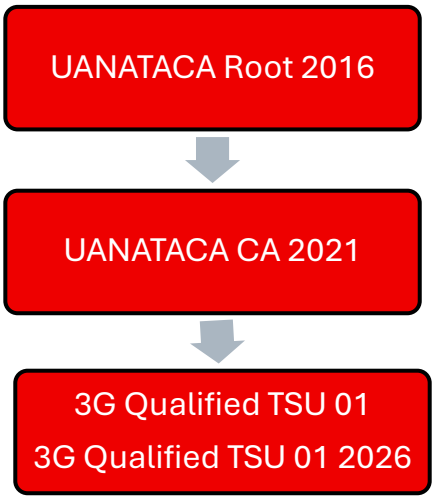
1.3 Participants in the certification services

1.3.1. Certification Service Provider

The Electronic Certification Service Provider, hereinafter “CSP”, is the natural or legal person that provides one or more trust services. Likewise, 3G is an electronic Trust Service Provider that acts in accordance with Regulation (EU) 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23
July 2014 on electronic identification and trust services for electronic transactions in the internal market, as amended by Regulation (EU) 2024/1183, with Law 6/2020 of 11 November, regulating certain aspects of electronic trust services, and with the Implementing Regulations applicable to qualified trust service providers, in particular Implementing Regulation (EU) 2025/1929 on qualified electronic time-stamps and Implementing Regulation (EU) 2025/2530, as well as the ETSI technical standards applicable to the issuance of qualified electronic time-stamps, principally ETSI EN 319 401, EN 319 421 and EN 319 422, in order to facilitate compliance with the legal requirements and the international recognition of its services.

For the provision of the certification service, 3G has established a hierarchy of Certification Authorities:

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00



1.3.2. Time-Stamping Authority

The Time-Stamping Authority, hereinafter "*TSA*" is the trusted third party that provides the service of issuing qualified electronic time-stamps. 3G is the Certification Service Provider that acts as Time-Stamping Authority for the issuance of qualified electronic time-stamps.

1.3.2.1 Uanataca CA Root 2016

This is the Root Certification Authority of the hierarchy, which issues certificates to other certification authorities and whose public key certificate is self-signed.

Identification data:

CN:	UANATACA ROOT 2016
Fingerprint:	6d c0 84 50 a9 5c d3 26 62 c0 91 0f 8c 2d ce 23 0d 74 66 ad
Valid from:	Friday, 11 March 2016
Valid until:	Monday, 11 March 2041
RSA key length:	4,096 bits

1.3.2.2 UANATACA CA1 2021

This is the Certification Authority within the hierarchy that issues the certificates to end entities and the electronic time-stamping certificates, and whose public key certificate has been digitally signed by UANATACA ROOT 2016.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

Identification data:

CN: UANATACA CA1 2021
Fingerprint: a1 db ea 6c 10 7a a3 e8 1e 16 c9 af 8e 55 7f ed 3d 90 cf 98
Valid from: Thursday, 3 June 2021
Valid until: Saturday, 3 June 2034
RSA key length: 4,096 bits

1.3.2.3 3G QUALIFIED TSU 01

Identification data:

CN: 3G QUALIFIED TSU 01
Fingerprint: 24 16 8C C3 5D 89 02 F0 94 E7 19 A6 31 7B 4F 74 01 94 D1
DFValid from: Wednesday, 30 July 2025, 16:49:47
Valid until: Saturday, 30 July 2033, 16:49:47
RSA key length: 2,048 bits

1.3.2.4 3G QUALIFIED TSU 01 2026

Identification data:

CN: 3G QUALIFIED TSU 01 2026
Fingerprint: D1 A9 61 0A 11 A8 98 6E 91 DE 64 BB D9 96 06 1A 11 B2 6F C9
Valid from: Monday, 5 October 2026, 16:54:12
Valid until: Saturday, 3 June 2034, 12:52:31
RSA key length: 3,072 bits

1.3.3. Subscribers of the certification service

Subscribers are the end users of the qualified electronic time-stamps issued by 3G. The subscribers of the service may be:

- Companies, entities, corporations or organisations that apply to 3G (directly or through a third party) for use within their corporate, business or organisational sphere.
- Natural persons who apply for the service for themselves.

The subscriber of the electronic certification service is therefore the customer of the Certification Service Provider.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

1.3.4. Relying parties

Relying parties are the persons and organisations that receive the qualified electronic time-stamps.

Before relying on the time-stamps, relying parties must verify them, as established in this Certification Practice Statement.

1.3.5. Public Key Infrastructure Services Provider

3G and UANATACA, S.A.U. have entered into a technology services agreement under which UANATACA will provide the public key infrastructure (PKI) that underpins 3G's trust service. UANATACA also makes available to 3G the technical personnel necessary for the proper performance of the trusted roles of a Trust Service Provider.

That said, UANATACA is configured as the infrastructure services provider for certification services and provides its technology services to 3G so that 3G can carry out the services inherent to a Trust Service Provider, guaranteeing at all times the continuity of the services under the conditions and requirements demanded by the regulations.

It is also hereby stated that UANATACA is a Trust Service Provider accredited in accordance with the provisions of European Regulation No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation), as amended by Regulation (EU) 2024/1183.

The UANATACA PKI undergoes annual audits for the conformity assessment of qualified trust service providers in accordance with the applicable regulations, under the following standards:

a) ISO/IEC 17065:2012
b) ETSI EN 319 403
c) ETSI EN 319 421
d) ETSI EN 319 401
e) ETSI EN 319 411-2
f) ETSI EN 319 411-1

The UANATACA PKI also undergoes annual audits under the following security standards:

a) ISO 9001:2015

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

b) ISO/IEC 27001:2014

1.3.2.5 Obligations of the Infrastructure Services provider

The Public Key Infrastructure provider undertakes to make available to 3G the technology services necessary for the provision of certification services. In this regard:

- The provider shall have the hardware necessary for the aforementioned services to be provided with the security levels required by the regulations for such purposes.
- It shall have the software necessary for the aforementioned services to be provided with the security levels required by the regulations for such purposes.
- It shall guarantee the custody and hosting of the systems (hardware and software) in a Data Processing Centre (Data Center) with appropriate logical and physical security levels, in accordance with generally accepted international standards.
- It shall be responsible for carrying out all preventive, evolutionary, corrective and reactive maintenance and, in general, any other maintenance required by the technological infrastructure for the provision of the technology services.
- It shall be responsible for providing 3rd-level technical support, that is, it shall be responsible for providing technical support for anything that exceeds 3G's management capacity and that is directly linked to deficiencies and/or technical failures of the technological infrastructure.
- In providing the services to 3G, the provider shall make available the technical personnel necessary for the operation of the public key infrastructure, who shall perform the trusted roles dedicated to the administration and operation of the systems, specifically:
    - PKI Security Officer
    - Internal Auditor
    - System Administrator
    - System Operator
    - CA Administrator
    - CA Operator

1.4. Use of the Time-Stamping service

1.4.1. Permitted uses

The Time-Stamping Service issues time-stamps in order to prove that a series of data existed and has not been altered since a specific instant in time. Its use is limited to the applications and/or systems of the customers (natural or legal persons) that have contracted these services.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

The 3G Time-Stamping service is identified by the OID: 1.3.6.1.4.1.57615.2
The qualified time-stamps issued by 3G include in the policy field one of the following identifiers:

- 1.3.6.1.4.1.57615.2: 3G's own time-stamping service policy, which applies when the request expressly asks for it.
- 0.4.0.2023.1.1 (baseline-ts-policy, BTSP policy of ETSI EN 319 421): policy that the TSA applies when the request does not indicate any policy, and which it also accepts when expressly requested.

Any other requested policy identifier is rejected by the TSA. The service operates in accordance with the qualified time-stamping policy of ETSI EN 319 421 and the time-stamps include the statement esi4-qtstStatement-1 (0.4.0.19422.1.1) of ETSI EN 319 422, which identifies them as qualified.

1.4.2. Limits and prohibitions on use

The Time-Stamping Service shall not be used for purposes other than those specified in this document. Likewise, the service must be used only in
accordance with the applicable regulations.

1.5. Policy administration

1.5.1. Organisation administering the document

3G SOLUCIONES MOVILIDAD, S.L.,
Pasaje Gutierrez 3, 1º
47002 Valladolid
+34 983101932
soporte@3gmg.com

1.5.2. Contact details of the organisation

3G SOLUCIONES MOVILIDAD, S.L.,
Pasaje Gutierrez 3, 1º
47002 Valladolid
+34 983101932
soporte@3gmg.com

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

1.5.3. Document management procedures

The documentation and organisation system of 3G guarantees, through the existence and application of the corresponding procedures, the proper maintenance of this document and of the service specifications related to it.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

2. Publication and preservation

2.1 Repository

3G securely retains all the time-stamps generated for at least 15 years. It also has a Repository in which the information relating to the qualified electronic time-stamp issuance service is published.

This service is available 24 hours a day, 7 days a week, and,
in the event of a system failure outside 3G's control, 3G shall use its best efforts
to make the service available again in accordance with the deadlines and procedures established with respect to business continuity.

2.2 Publication of information by the certification service provider

3G publishes the following information in its Repository:

- The Time-Stamping Certification Practice Statement.
- The Disclosure Statement for the service.
- The public key of the electronic time-stamp certificate.
- References to the time-stamp validation mechanisms.

2.3 Frequency of publication

The information of the Certification Service Provider, including the Disclosure Statement and the Time-Stamping Certification Practice Statement, is published
as soon as it is available.

Changes to the Time-Stamping Certification Practice Statement are governed
by the provisions of the management procedure for this document and in accordance with the applicable regulations.

2.4 Access control

3G does not restrict read access to the information set out in section 2.2, but establishes controls to prevent unauthorised persons from adding, modifying

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

or deleting records in the Repository, in order to protect the integrity and authenticity of the information.

3G uses trustworthy systems for the Repository, such that:

- Only authorised persons can make entries and modifications.
- The authenticity of the information can be checked.
- Any technical change affecting the security
- requirements can be detected.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

3. Identification and authentication

3.1. Initial registration

3.1.1. Types of names

The electronic certificates used in the qualified electronic time-stamp issuance service are called Time-Stamping Unit Certificates, hereinafter "TSU Certificate/s", and contain a distinguished name (DN) conforming to the X.509 standard in the Subject field, including a Common Name (CN=) component.

The TSU Certificates are issued by UANATACA. These certificates are electronic certificates in accordance with Article 38 and Annex III of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standards identified by the references ETSI EN 319 412-3, ETSI EN 319 421 and ETSI EN 319 422.

3.1.2. Meaning of names

The names contained in the SubjectName and SubjectAlternativeName fields of the certificates are understandable in natural language, in accordance with the provisions of the preceding section.

3.1.3. Use of anonyms and pseudonyms

N/A

3.1.4. Interpretation of name formats

3G complies with the requirements of the X500 standard.

3.1.5. Uniqueness of names

The distinguished name of the TSU Certificates will be unique.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

3.2. Initial identity validation

N/A

3.3. Identification and authentication for renewal requests

N/A

3.4. Identification and authentication for revocation, suspension or reactivation requests

N/A

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

4. Operational requirements

4.1 Request for the issuance of time-stamps

4.1.1. Standing to request the time-stamping service

The applicant or user of the time-stamping service, whether a natural or legal person, may request the issuance of qualified time-stamps by direct request to 3G or through the available TSA servers, which allow the time-stamping of the documents they wish.

The applicant or user of the time-stamping service may use their own application or software through the protocol defined in RFC 3161 and in accordance with ETSI 319 422, connecting to a web address and using credentials provided by 3G.

Once the request has been accepted and registered and the appropriate checks have been carried out, the time-stamp is generated and sent to the applicant.

4.1.2. Registration procedure and responsibilities

3G receives requests for the time-stamping service made by persons, entities, companies or organisations under public or private law.

Requests are made directly through the 3G information systems.

4.2 Processing of the request

The applicant submits, through the established procedures, the request for the time-stamp
for an electronic document directly to the time-stamping service / server
in charge of time-stamping. The request is made and sent with the document, pointing to the corresponding address
and the time-stamped document is returned.

4.3 Issuance of the time-stamp

Qualified electronic time-stamps are generated automatically through the

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

system or server in charge of the time-stamping service. Following approval of the request, the time-stamp is issued securely and made available to the subscriber.

During the process, 3G:

- Protects the confidentiality and integrity of the registration data it holds.
- Uses reliable systems and products that are protected against any alteration and
- that ensure the technical and, where applicable, cryptographic security of the certification
- processes they support.
- Indicates the date and time at which a time-stamp was issued.

4.4 Delivery and acceptance of the certificate

The delivery and acceptance of the TSU Certificates follow the processes and instructions established in the Certification Practice Statement and Disclosure Statement of UANATACA as Certification Authority, all available on the website: https://web.uanataca.com/.

4.5 Use of the key pair and the certificate

The TSU Certificate is used solely and exclusively for the service of issuing qualified electronic time-stamps.

4.6 Modification of certificates

N/A

4.7 Revocation, suspension or reactivation of certificates

The revocation of a certificate entails the definitive loss of its validity, and is irreversible.

The suspension (or temporary revocation) of a certificate entails the temporary loss of its validity, and is reversible.

The reactivation of a certificate entails its change from suspended status to active status.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

The procedures for the revocation, suspension and reactivation of TSU Certificates follow the processes and instructions established in the Certification Practice Statement of UANATACA as Certification Authority, all available on the website: https://web.uanataca.com/.

4.7.1. Causes for revocation of certificates

3G will revoke the TSU Certificates when any of the following causes arises:

1. Circumstances affecting the information contained in the certificate:

    a. Modification of any of the data contained in the certificate, after the corresponding issuance of the certificate that includes the modifications.

    b. Discovery that any of the data contained in the certificate is incorrect.

2. Circumstances affecting the security of the key or the certificate:

    a. Compromise of the private key, of the infrastructure or of the systems of the Certification Service Provider that issued the certificate, provided that it affects the reliability of the certificates issued as from that incident.

    b. Breach by 3G of the requirements laid down in the certificate management procedures established in this Time-Stamping Certification Practice Statement.

    c. Compromise or suspected compromise of the security of the key or of the issued certificate.

    d. Unauthorised access to or use by a third party of the private key corresponding to the public key contained in the certificate.

3. Other circumstances:

    a. The termination of the certification service of 3G.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

b. Use of the certificate that is harmful and continued for 3G. In this case, a use is considered harmful on the basis of the following criteria:

   i. The nature and number of complaints received.

   ii. The identity of the entities submitting the complaints.

   iii. The relevant legislation in force at any given time.

   iv. The response of the subscriber or of the person identified in the certificate to the complaints received.

4.7.2. Causes for suspension of a certificate

TSU Certificates may be suspended if the compromise of a key is suspected, until it is confirmed. In this case, 3G must ensure that the certificate is not suspended for longer than necessary to confirm its compromise.

4.7.3. Causes for reactivation of a certificate

TSU Certificates may be reactivated.

4.7.4. Who can request revocation, suspension or reactivation

Revocation, suspension or reactivation will be requested by 3G.

4.7.5. Procedures for requesting revocation, suspension or reactivation

The procedure for requesting the revocation, suspension and/or reactivation of TSU Certificates follows the processes and instructions established in the Certification Practice Statement and Disclosure Statement of UANATACA, as Certification Authority, all available on the website: https://web.uanataca.com/.

4.7.6. Time limit for requesting and processing revocation, suspension or reactivation

The time limit for the request and for the processing thereof for the revocation, suspension and/or reactivation of TSU Certificates follows the processes and instructions established in the Certification Practice Statement and Disclosure Statement of UANATACA, as Certification Authority, all available on the website: https://web.uanataca.com/.

Requests will be processed within a period not exceeding 24 hours from their receipt.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

4.7.7. Obligation to check certificate revocation or suspension information

Relying parties must check the status of the qualified electronic time-stamps on which they wish to rely, for which purpose they must check the status of the TSU Certificate. One method by which the status of TSU Certificates can be verified is by consulting the most recent Certificate Revocation List issued by the UANATACA Certification Authority responsible for their issuance.

With regard to Certificate Revocation Lists, it is important that the user verify and check that the TSU Certificate appears in the Trusted List.

The Certificate Revocation Lists (CRLs; Spanish acronym LRC), in English *CRL)* are published on the UANATACA website, as well as at the following web addresses, indicated within the certificates:

- Subordinate Certification Authority - UANATACA CA1 2021

- http://crl1.modernpki.com/public/pki/crl/2021CA1sub.crl
- http://crl2.modernpki.com/public/pki/crl/2021CA1sub.crl

The validity status of the certificates can also be checked by means of the OCSP protocol.

- http://ocsp1.modernpki.com/public/pki/ocsp/
- http://ocsp2.modernpki.com/public/pki/ocsp/

3G establishes that subscribers and relying parties of the service must check the preferred method for verifying the status of certificates.

It is explicitly established that the checking of the status of certificates must be carried out primarily by means of the OCSP protocol. This mechanism offers real-time validation, ensuring greater efficiency and up-to-date information.

Consultation of the CRLs will be defined as a complementary or back-up method.

4.7.8. Frequency of issuance of Certificate Revocation Lists (CRLs)

To check the validity of a qualified electronic time-stamp issued by 3G, electronic signature and seal validation services in ordinary use in legal transactions may be used.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

3G has its own validator, accessible from https://vol.modernpki.com/es, from which the time-stamp can be validated.

In order to validate the time-stamp correctly, the user may carry out the following activities:

1. Verification of the issuer of the time-stamp: 3G is a trust service provider that acts in accordance with Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, as well as the applicable ETSI technical standards for the issuance of qualified electronic time-stamps, principally EN 319 421, with the aim of facilitating compliance with the legal requirements and the international recognition of its services.

2. Review of the status of the certificate of the Time-Stamping Unit that issued the time-stamp: 3G has its own OCSP, through which it can be checked whether the certificates used in the time-stamp have been revoked. The URL for access to this OCSP response service is found in the certificate used to sign the time-stamp.

UANATACA, as the Certification Authority issuing the TSU Certificates, issues a CRL at least every 24 hours. This CRL indicates the scheduled time for issuing a new CRL, although a CRL may be issued before the time indicated in the previous CRL, in order to reflect revocations.

The CRL must retain the revoked or suspended certificate until it expires.

4.7.9. Maximum publication time of CRLs

CRLs are published at https://web.uanataca.com/ and at the web addresses indicated, within a reasonable immediate period after their generation, which in no case exceeds a few minutes.

4.7.10. Availability of online certificate status checking services

Alternatively, relying parties on qualified electronic time-stamps may consult the UANATACA Repository of certificates, which is available 24 hours a day, 7 days a week, on the website:

- https://web.uanataca.com/

To check the latest CRL issued by each CA, the following must be downloaded:

- Root Certification Authority (UANATACA ROOT 2016):

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

- Subordinate Certification Authority - UANATACA CA1 2016

  - http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl
  - http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl

- Subordinate Certification Authority - UANATACA CA2 2016

  - http://crl1.uanataca.com/public/pki/crl/2016CA2sub.crl
  - http://crl2.uanataca.com/public/pki/crl/2016CA2sub.crl

- Subordinate Certification Authority - UANATACA CA1 2021

  - http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
  - http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl

- Subordinate Certification Authority - UANATACA CA2 2021

  - http://crl1.uanataca.com/public/pki/crl/2021CA2sub.crl
  - http://crl2.uanataca.com/public/pki/crl/2021CA2sub.crl

7.4.11. Obligation to consult certificate status checking services

It is mandatory to check the status of the TSU Certificates before relying on the qualified electronic time-stamps of 3G.

7.4.12. Special requirements in the event of compromise of the private key

The compromise of the private key of the TSU Certificates of 3G is notified to all participants in the certification services, as far as possible, by publishing this fact on the 3G website and, if considered necessary, in other media, including on paper.

4.8. Termination of the subscription

N/A

4.9. Key escrow and recovery

4.9.1. Key escrow and recovery policy and practices

N/A

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

4.9.2. Session key encapsulation and recovery policy and practices

N/A

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

5. Physical, management and operational security controls

5.1 Physical security controls

3G provides its trust services through the public key infrastructure of UANATACA, which has established physical and environmental security controls to protect the resources of the facilities where the systems are located, the systems themselves and the equipment used for the operations for the provision of the electronic trust services.

Specifically, the security policy applicable to the electronic trust services lays down provisions on the following:

- Physical access controls.
- Protection against natural disasters.
- Fire protection measures.
- Failure of support systems (electric power, telecommunications, etc.)
- Collapse of the structure.
- Flooding.
- Anti-theft protection.
- Unauthorised removal of equipment, information, media and applications
- relating to components used for the services of the Certification Service
- Provider.

These measures apply to the facilities from which the electronic trust services are provided, in their production and contingency environments, which are audited periodically in accordance with the applicable regulations and with the internal policies intended for this purpose.

The facilities have preventive and corrective maintenance systems with 24h-365 days a year support, with assistance within 24 hours following notification.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

5.2 Location and construction of the facilities

The facilities that make up the Public Key Infrastructure of the 3G Service are located in a rack / cabinet physically isolated from the rest of the infrastructures hosted in the Data Processing Centre of the technology service provider ADAM Ecotech (hereinafter ADAM), located in Barcelona, Spain.

Physical protection is achieved by creating clearly defined security perimeters around the services. The quality and solidity of the construction materials of the facilities guarantees adequate levels of protection against brute-force intrusion, and the facilities are located in a low disaster risk area and allow rapid access.

The room where the cryptographic operations are carried out in the Data Processing Centre has redundancy in its infrastructures, as well as several alternative sources of electricity and cooling in the event of an emergency.

Facilities are in place that physically protect the provision of the certification services, as well as the management of validation, from compromise caused by unauthorised access to the systems or to the data, and from the disclosure
thereof.

5.2.1. Physical access

There are three levels of physical security (Entrance to the Building where the Data Processing Centre is located,
access to the Data Processing Centre room and access to the Rack), and access must be gained from the lower levels
to the higher levels.

Physical access to the premises where certification processes are carried out is restricted and protected by a combination of physical and procedural measures.
Thus:

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

- It is restricted to expressly authorised personnel, with identification at the time of access and logging thereof, including closed-circuit television filming and its archiving.

- Access to the rooms is controlled by identification card readers and managed by a computer system that keeps an automatic log of entries and exits.
- Access to the rack housing the cryptographic processes requires prior authorisation from the administrators of the hosting service, who hold the key to open the cage.

5.2.2. Electricity and air conditioning

The facilities have power stabilisation equipment and a duplicated equipment power supply system backed by a generator set.

The rooms housing IT equipment have temperature control systems with air conditioning equipment.

5.2.3. Exposure to water

The facilities are located in an area with a low risk of flooding. The rooms housing IT equipment have a humidity detection
system.

5.2.4. Fire prevention and protection

The facilities and assets have automatic fire detection and extinguishing
systems.

5.2.5. Media storage

Only authorised personnel have access to the storage media. The information with the highest classification level is kept in a safe outside the premises of the Data Processing Centre.

5.2.6. Waste disposal

Media, both paper and magnetic, are disposed of by means of mechanisms that guarantee that the information cannot be recovered.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

Magnetic media are either discarded, in which case they are physically destroyed, or reused after a process of permanent erasure or formatting. Paper documentation is disposed of by means of shredders or in bins provided for the purpose,
to be subsequently destroyed, under control.

5.2.7. Off-site backup

A secure external store is used for the custody of documents and magnetic and electronic devices, which is independent of the operations centre.

5.3 Procedural controls

It is ensured that its systems are operated securely, for which purpose it has established and implemented procedures for the functions that affect the provision of its services. The personnel serving the Provision of Trust Services carry out the administrative and management procedures in accordance with the security policy.

5.3.1. Trusted roles

In accordance with its security policy, the following functions or roles have been identified as trusted:

- **Internal Auditor:** Responsible for compliance with the operating procedures. This is a person external to the Information Systems department. The tasks of the Internal Auditor are incompatible over time with the Certification tasks and incompatible with Systems. These functions are subordinate to the head of operations, reporting both to the latter and to the technical management.

- **System Administrator:** Responsible for the correct operation of the hardware and software supporting the certification platform.

- **Security Officer:** In charge of coordinating, controlling and enforcing the security measures defined by the security policies of 3G. Responsible for the aspects related to information security: logical, physical, network, organisational, etc.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

- **System Operator:** Responsible, jointly with the System Administrator, for the correct operation of the hardware and software supporting the certification platform. The operator is responsible for the backup procedures and for maintaining the daily operations of the systems.

The persons occupying the above positions are subject to specific investigation and control procedures. In addition, criteria for the segregation of duties are implemented in its policies as a measure to prevent fraudulent activities.

5.3.2. Identification and authentication for each role

The persons assigned to each role are identified by the Internal Auditor, who will ensure that each person carries out the operations for which they are assigned.

Each person controls only the assets necessary for their role, thus ensuring that no person accesses resources that have not been assigned to them.

Access to resources is made, depending on the asset, by means of user/password, digital certificate, physical access card and/or keys.

5.3.3. Roles requiring segregation of duties

Trusted roles are established under the principle of least privilege, guaranteeing a segregation of duties, so that the person holding a role does not have total or especially broad control over all the certification functions, thus ensuring due control and oversight and limiting any kind of fraudulent behaviour at the
internal level.

The granting of least privilege for trusted roles will take into
account the best performance of the activity and will be as limited as possible, considering the
organisational structure at any given time.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

5.4 Personnel controls

5.4.1. Background, qualifications, experience and authorisation requirements

All personnel are qualified and/or have been suitably trained to carry out the operations assigned to them.

Personnel in positions of trust have no personal interests that conflict with the performance of the function entrusted to them.

In general, an employee will be removed from their trusted functions when there is knowledge of the existence of conflicts of interest and/or the commission of any criminal act that could affect the performance of their duties.

3G will not assign to a trusted or management position a person who is not suitable for the post, especially because of a fault that affects their suitability for the post. For this reason, an investigation is carried out beforehand, to the extent permitted by the applicable legislation, concerning the following aspects:

- Studies, including the degree claimed.
- Previous jobs, up to five years, including professional references.
- Professional references.

5.4.2. Background investigation procedures

Before hiring a person or before they take up the post, the following checks are carried out:

- References from jobs held in recent years.
- Professional references.
- Studies, including the degree claimed.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

All checks are carried out to the extent permitted by the applicable legislation in force. The grounds that may lead to the rejection of a candidate for a trusted position are the following:

- Falsehoods in the job application made by the candidate.
- Very negative or very unreliable professional references in relation to the
- candidate.

5.4.3. Training requirements

3G trains personnel in trusted and management positions until they reach the necessary qualification, keeping a record of such training.

The training programmes are periodically reviewed, and are updated for their improvement and are enhanced periodically.

The training includes, at least, the following contents:

- Security principles and mechanisms of the certification hierarchy, as well as the
- user environment of the person being trained.
- Tasks to be performed by the person.
- Security policies and procedures. Use and operation of the machinery and
- applications installed.
- Management and handling of security incidents and compromises.
- Business continuity and emergency procedures.
- Management and security procedure in relation to the processing of
- personal data.

5.4.4. Training refresher requirements and frequency

3G updates the training of personnel according to needs, and with sufficient frequency to perform their duties competently and satisfactorily, especially when substantial modifications are made to the certification tasks.

5.4.5. Job rotation sequence and frequency

N/A

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

5.4.6. Sanctions for unauthorised actions

3G has a disciplinary system to establish responsibilities arising from unauthorised actions, in accordance with the applicable labour legislation.

Disciplinary actions include suspension, removal from duties and up to dismissal of the person responsible for the harmful action, in a manner proportionate to the seriousness of the unauthorised action.

5.4.7. Requirements for contracting professionals

Employees hired to perform trusted tasks sign beforehand the confidentiality clauses and the operational requirements used by 3G. Any action that compromises the security of the accepted processes could, once assessed, give rise to termination of the employment contract.

Where all or part of the certification services are operated by a third party, the controls and provisions set out in this section, or in other parts of the Certification Practice Statement, will be applied and complied with by the third party performing the operation of the certification services; notwithstanding this, the Trust Service Provider will in any case be responsible for their effective performance. These aspects are specified in the legal instrument used to agree the provision of the certification services by a third party other than 3G.

5.4.8. Provision of documentation to personnel

The Certification Service Provider will provide its personnel with the documentation strictly required at any given time, in order to perform their work competently and satisfactorily.

5.5 Security audit procedures

5.5.1. Types of events recorded

A record is produced and kept of, at least, the following events related to the security of the entity:

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

- System start-up and shutdown.
- Attempts to create, delete, set passwords or change
- privileges.
- Login and logout attempts.
- Attempts at unauthorised access to the TSA system through the network.
- Attempts at unauthorised access to the file system.
- Physical access to the logs.
- Changes to the system configuration and maintenance.
- TSA application records.
- TSA application start-up and shutdown.
- Changes to the TSA details and/or its keys.
- Records of the destruction of the media containing keys and activation data.
- Events related to the life cycle of the cryptographic module, such as its receipt, use and decommissioning.
- The key generation ceremony and the key management databases.
- Physical access records.
- System maintenance and configuration changes.
- Personnel changes.
- Reports of compromises and discrepancies.
- Records of the destruction of material containing key information, activation data or personal information of the subscriber, in the case of individual certificates, or of the natural person identified in the certificate, in the case of organisation certificates.
- Complete reports of attempted physical intrusions into the infrastructures that support the service.
- Events relating to clock synchronisation and recalibration.

The log entries include the following elements:

- Date and time of the entry.
- Serial or sequence number of the entry, in automatic records.
- Identity of the entity making the entry.
- Type of entry.

5.5.2. Frequency of audit log processing

The logs are reviewed when a system alert is raised due to the existence of an incident.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

The processing of the audit logs consists of a review of the logs that includes verification that they have not been tampered with, a brief inspection of all log entries and a more thorough investigation of any alerts or irregularities in the logs. The actions taken as a result of the audit review are documented.

A system is maintained that makes it possible to ensure:

- Sufficient space for log storage.
- That the log files are not overwritten.
- That the information kept includes at least: type of event, date and time, user executing the event and result of the operation.
- The log files will be kept in structured files that can be loaded into a database for subsequent analysis.

5.5.3. Retention period for audit logs

The information relating to logs is stored for a period of between 1 and 15 years, depending on the type of information recorded.

5.5.4. Protection of audit logs

The system logs:

- Are protected against tampering by means of the signing of the files containing them.
- Are stored on fireproof devices.
- Their availability is protected by storing them at facilities external to the centre.

Access to the log files is reserved only to authorised persons. Likewise, the devices are handled at all times by authorised personnel.

There is an internal procedure detailing the management processes for the devices containing audit log data.

5.5.5. Backup procedures

An appropriate backup procedure is in place so that, in the event of loss or destruction of relevant files, the corresponding backup copies of the logs are available within a short period of time.

A backup procedure for the audit logs is implemented, making a weekly copy of all the logs on an external medium. In addition, a copy is kept at an external custody centre.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

5.5.6. Location of the audit log accumulation system

The event audit information is collected internally and in an automated manner by the operating system, by the network communications and by the time-stamping software, as well as by manually generated data, which will be stored by duly authorised personnel. All of this makes up the audit log accumulation system.

5.5.7. Notification of the audit event to the cause of the event

When the audit log accumulation system records an event, it is not necessary to send a notification to the individual, organisation, device or application that caused the event.

5.5.8. Vulnerability assessment

Vulnerability assessments are covered by the audit processes. These must be executed, reviewed and revised by means of an examination of these monitored events. These assessments must be executed periodically in accordance with the internal procedure provided for this purpose.

The audit data of the systems are stored in order to be used in the investigation of any incident and to locate vulnerabilities.

5.6. Information archiving

5.6.1. Retention period for records

The records specified above are archived for at least 15 years, or the period established by the legislation in force.

5.6.2. Protection of the archive

The archive is protected so that only duly authorised persons can obtain access to it. The archive is protected against viewing, modification, deletion or any other tampering by being stored in a trustworthy system.

The correct protection of the archives is ensured by assigning qualified personnel to handle them and by storing them at secure external facilities.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

5.6.3. Backup procedures

An external storage centre is available to guarantee the availability of the copies of the archive of electronic files. Physical documents are stored in secure places with access restricted to authorised personnel only.

As a minimum, daily incremental backups of all its electronic documents are made, and full backups are made weekly for data recovery purposes.

In addition, where there is a need to keep a copy of paper documents, these are stored in a secure place.

5.6.4. Date and time-stamping requirements

The records are dated with a reliable source via NTP.

It is not necessary for this information to be signed.

5.6.5. Location of the archive system

A centralised system is in place for collecting information on the activity of the equipment involved in the certificate management service.

5.6.7. Procedures to obtain and verify archive information

A procedure is in place that describes the process for verifying that the archived information is correct and accessible. 3G provides the auditor with the information and means of verification.

5.7. Key renewal

Each key pair of the TSU Certificates used in the time-stamping service is associated solely with the system that provides that service. Before the use of the private key of the TSU Certificates expires, a key changeover will be carried out before the expiry or revocation of the current ones.

Period of use of the TSU keys. The private key of each TSU certificate is used to sign time-stamps for a maximum period of 8 years from its generation, which in no case exceeds the validity period of the corresponding certificate, nor the validity of the CA Certificate that issued it. At the end of that period the TSA stops signing with the key, which is deactivated, withdrawn and destroyed in accordance with sections 6.2.6 and 6.2.8.

5.8. Key compromise and disaster recovery

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

5.8.1. Incident and compromise management procedures

Security and business continuity policies have been developed that allow the management and recovery of the systems in the event of incidents and compromise of their operations.

5.8.2 Corruption of resources, applications or data

When an event of corruption of resources, applications or data occurs, the appropriate management procedures will be followed in accordance with the established security and incident management policies, which provide for escalation, investigation and response to the incident.

If necessary, the key compromise or disaster recovery procedures will be initiated.

5.8.2. Compromise of the entity's private key

In the event of suspected or known compromise, the key compromise procedures will be activated in accordance with the security, incident management and business continuity policies, allowing the recovery of critical systems, if necessary at an alternative data centre.

5.8.3. Business continuity after a disaster

Critical services will be restored in accordance with the existing incident and business continuity plan, restoring normal operation of the previous services within 24 hours following the disaster.

An alternative site is available, if necessary, for bringing into operation the certification systems described in the business continuity plan.

5.9 Termination of service

3G ensures that potential disruption to subscribers of the service and to third parties is minimal as a result of the cessation of the services of the Certification Service Provider. In this regard, 3G guarantees continuous maintenance of the records defined, for the period established, in accordance with this Time-Stamping Certification Practice Statement.

Nevertheless, where applicable, 3G will carry out all actions necessary to transfer to a third party or to a notarial repository the obligations to maintain the specified records for the corresponding period under this Time-Stamping Certification Practice Statement or the applicable legal provision.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

Before terminating its services, 3G will carry out a termination plan, with the following provisions:

- It will provide the necessary funds, including civil liability insurance, to continue completing the revocation activities.
- It will inform all subscribers of the service, relying parties and, in general, any third party with whom it has agreements or other types of relationship, of the cessation, at least 2 months in advance.
- It will destroy or disable for use the private keys responsible for the time-stamping service.
- It will carry out the tasks necessary to transfer the obligations to maintain the registration information and the event log files for the respective periods of time.
- It will notify the National Supervisory Body that holds the corresponding competences of the cessation of its activity, at least 3 months in advance.
- It will notify the National Supervisory Body of the opening of any insolvency proceedings against 3G, as well as of any other relevant circumstance that may prevent the continuation of the activity.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

6. Technical security controls

In the provision of Certification Services, trustworthy systems and products are used, protected against any alteration and guaranteeing the technical and cryptographic security of the certification processes that they support.

6.1 Key pair generation and installation

6.1.1. Key pair generation

The key pair of the TSU Certificate is generated by the Trust Service Provider UANATACA, in accordance with its Certification Practice Statement and its disclosure statement, which are available on the website: https://web.uanataca.com/

Likewise, key ceremony procedures have been followed, within the high-security perimeter intended for this task. The activities performed during the key generation ceremony have been recorded, dated and signed by all individuals taking part in it, in the presence of an Auditor. These records are kept for audit and monitoring purposes for an appropriate period determined by 3G.

For the generation of the TSU certificate key, nCipher nShield Solo XC cryptographic modules (version 12.60.15) are used, certified Common Criteria EAL4+ with firmware nShield5s Hardware Security Module v13.5.1 (EN 419 221-5), operated by UANATACA in the configuration covered by that certification.

The keys are generated using the RSA public key algorithm, with a length of 3,072 bits for newly issued TSU certificates. The TSU private key will be used for a maximum period of 8 years from the entry into production of the certificate, which will in any case be shorter than the validity period of the associated certificate (until 03/06/2034, the expiry date of the issuing CA). Once that period has elapsed, the TSU will stop issuing time-stamps with the key and the key pair will be renewed in accordance with section 5.7. The 2,048-bit key of the TSU 01 certificate will be used only until its withdrawal, before 31/12/2026.

Time-Stamping Unit Certificates	3,072 bits	Certificate validity: Until 03/06/2034, the expiry date of the issuing CA.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

6.1.2. Delivery of the public key to the certificate issuer

The method for submitting the public key to the electronic certification service provider is PKCS#10, another equivalent cryptographic proof, or any other method approved by 3G.

6.1.3. Distribution of the certification service provider's public key

The keys of 3G are communicated to relying parties on certificates, ensuring the integrity of the key and authenticating its origin, by publishing them in the Repository.

Users can access the Repository to obtain the public keys and, additionally, in S/MIME applications, the data message may contain a chain of certificates, which are thereby distributed to users.

6.1.4. Key sizes

The key length of the TSU Certificates is 3,072 bits. The exception is certificate 3G QUALIFIED TSU 01, of 2,048 bits, which will be withdrawn before 31/12/2026.

6.1.5. Public key parameters generation

The public key of the TSU certificates is encoded in accordance with RFC 5280.

6.1.6. Public key parameters quality checking

- Modulus length = 3,072 bits (2,048 bits only for the TSU 01 certificate being withdrawn)
- Key generation algorithm: rsagen1
- Cryptographic hash functions: SHA256.

6.1.7. Key generation in software or in hardware

All keys are generated in hardware, as indicated in section 6.1.1.

6.1.8. Hash algorithms used in the service

Hash used on the data for which the time-stamp is to be generated:

- The identifier of the hash algorithm used to generate the fingerprint of the evidence. In this case the permitted algorithms are:
    - SHA-256 (secure hash ALGORITHM 256-bit OID: 2.16.840.1.101.3.4.2.1)
    - SHA-384 (secure hash ALGORITHM 384-bit OID: 2.16.840.1.101.3.4.2.2)

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

- SHA-512 (secure hash ALGORITHM 512 -bit OID: 2.16.840.1.101.3.4.2.3)
- SHA3-256 (secure 256-bit SHA-3 hash, OID: 2.16.840.1.101.3.4.2.8)
- SHA3-512 (secure 512-bit SHA-3 hash, OID: 2.16.840.1.101.3.4.2.10)
- The MD5 and SHA-1 algorithms are not accepted; requests that use them are rejected.

- The time-stamp signature algorithm:
  - In this case the algorithm used is RSA (SHA256rsa 1.2.840.113549.1.1.11).

6.2. Private key protection

6.2.1. Cryptographic module standards

The cryptographic modules that manage the keys of 3G are nCipher nShield Solo XC modules (version 12.60.15) certified Common Criteria EAL4+ (EN 419 221-5, certificate CSA_CC_21008) and nShield 5c firmware modules, operated by UANATACA in the evaluated Security World configuration in Common Criteria mode. The inventory of modules and their assignment to each TSU key is maintained in UANATACA's infrastructure documentation.

6.2.2. Multi-person control (n out of m) of the private key

Multi-person control is required for access to the private key of the TSU Certificate. A minimum of two persons authenticated at the same time will be required.

Likewise, the cryptographic devices are physically protected as determined in this document.

6.2.3. Private key backup

A backup is made of the private keys of the TSU certificates, so as to make their recovery possible in the event of disaster, or of their loss or deterioration. Both the creation of the copy and its recovery require the participation of at least two persons.

These recovery files are stored in fireproof cabinets and at the external custody centre.

6.2.4. Entry of the private key into the cryptographic module

The private keys are generated directly in the cryptographic modules that make up the public key infrastructure.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

The private keys of the TSU Certificates are stored encrypted in the cryptographic modules that make up the public key infrastructure.

6.2.5. Private key activation method

The management procedures for the private key of the 3G TSU Certificate are activated by executing the corresponding secure start-up procedure of the cryptographic module, by persons performing trusted roles.

6.2.6. Private key deactivation method

Before the keys are destroyed, a revocation will be issued for the certificate of the public keys associated with them.

Any devices holding any part of the private keys of 3G will be physically destroyed or reset at a low level. For the reset, the steps described in the cryptographic equipment administrator's manual will be followed.

Finally, the backup copies will be securely destroyed.

Procedure for withdrawal and destruction of the private key of a TSU certificate (applicable to the 2,048-bit certificate 3G QUALIFIED TSU 01, to the TSU 02 certificate and to any other TSU certificate that is withdrawn):

a) Cessation of time-stamp issuance with the key, after the replacement certificate has been put into production and accepted by the National Supervisory Body and, in any case, before 31/12/2026 in the case of the 2,048-bit TSU 01 certificate.

b) Request to UANATACA for revocation of the certificate, prior to destruction of the key.

c) Erasure of the private key in the cryptographic modules (deletion of the key object protected by the TSA application key) and secure destruction of its backup copies and recovery files, with the participation of at least two persons in trusted roles.

d) Drawing up of a destruction record signed by the participants, identifying the key, the module, the date and the evidence (records), which is retained together with the other records of the service.

e) Notification to the National Supervisory Body of the completion of the withdrawal.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

6.2.7. Cryptographic module rating

See section 6.2.

6.3. Computer security controls

Trustworthy systems are used to provide its certification services. To this end, computer controls and audits have been carried out in order to establish management of its IT assets appropriate to the level of security required in the management of electronic certification systems.

With regard to information security, UANATACA applies the controls of the ISO 27001 certification scheme for information management systems.

The equipment used is initially configured with the appropriate security profiles by the systems staff, in the following aspects:

- Operating system security configuration.
- Application security configuration.
- Correct sizing of the system.
- Configuration of users and permissions.
- Configuration of log events.
- Backup and recovery plan.
- Antivirus configuration.
- Network traffic requirements.

Each server includes the following functionalities:

- Enforcement of separation of duties for privilege management.
- Identification and authentication of roles associated with identities.
- Auditing of security-related events.
- Key and TSA system recovery mechanisms.

The functionalities described are performed through a combination of operating system, PKI software, physical protection and procedures.

6.4. Life cycle technical controls

6.4.1. System development controls

Applications are developed and implemented in accordance with development standards and change control.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

Applications have methods for verifying integrity and authenticity, as well as the correctness of the version to be used.

6.4.2. Security management controls

Specific activities are carried out for the security training and awareness of employees. The materials used for training and the documents describing the processes are updated after their approval by a security management group. In carrying out this function, an annual training plan is in place.

Equivalent security measures are required by contract of any external supplier involved in electronic certification service tasks.

6.4.2.1. Classification and management of information and assets

An inventory of assets and documentation is maintained, together with a procedure for the management of this material to ensure its proper use.

The security policy details the information management procedures, in which information is classified according to its level of confidentiality.

Documents are catalogued in four levels: UNCLASSIFIED, PUBLIC, INTERNAL USE and CONFIDENTIAL.

6.4.2.2. Management operations

An adequate incident management and response procedure is in place, through the implementation of an alert system and the generation of periodic reports.

The incident management process is developed in detail in the security document.

3G has documented the entire procedure relating to the functions and responsibilities of the personnel involved in the control and handling of elements contained in the certification process.

6.4.2.3. Controls on the operation of the Public Key Infrastructure

A periodic review, at least annually, of the components and configurations of the public key infrastructure is carried out in order to check for possible changes, adaptations and configurations to it, whether these have undergone modifications, and to review those configurations.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

6.4.2.4. Media handling and security

All media are handled securely in accordance with the information classification requirements. Media containing sensitive data are securely destroyed if they are not going to be required again.

6.4.2.5. System planning

The Systems department in charge of the public key infrastructure maintains a record of the capacities of the equipment. Together with the resource control application of each system, possible resizing can be anticipated.

6.4.2.6. Incident reports and response

A procedure is in place for the tracking and resolution of incidents, in which the responses and an evaluation of the incident resolution process are recorded.

6.4.2.7. Operational procedures and responsibilities

Activities have been defined, assigned to persons holding a trusted role, that are separate from those of the persons in charge of performing the day-to-day operations, which are not of a confidential nature.

6.4.2.8. System access management

All the activities necessary to confirm that system access is restricted to authorised persons are carried out.

In particular:

- Controls based on firewalls, antivirus and IDS in high availability are in place.
- Sensitive data are protected by cryptographic techniques or access controls with strong identification.
- A documented procedure for the management of user registrations and de-registrations, and an access policy detailed in its security policy, are in place.
- Procedures are in place to ensure that operations are performed in compliance with the roles policy.
- Each person is assigned a role for performing certification operations.
- Personnel are accountable for their actions through the confidentiality undertaking signed with the company.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

6.4.2.9. Cryptographic hardware life cycle management

It is ensured that the cryptographic hardware used for the time-stamping service is not tampered with during transport, by inspection of the delivered equipment.

The cryptographic hardware is transported on media prepared to prevent any tampering.

All relevant information concerning the device is recorded in order to add it to the asset catalogue.

The use of the time-stamping cryptographic hardware requires the involvement of at least two trusted employees.

Periodic tests are carried out to ensure the correct operation of the device.

The cryptographic hardware device is handled only by trusted personnel.

The private key of the 3G TSU Certificate stored in the cryptographic hardware will be deleted once the device has been withdrawn.

The system configuration, as well as its modifications and updates, are documented and controlled.

Changes or updates are authorised by the Security Officer and are recorded in the corresponding work minutes. These configurations will be carried out by at least two trusted persons.

6.5. Network security controls

Physical access to the network management devices is protected, and there is an architecture that organises the traffic generated on the basis of its security characteristics, creating clearly defined network sections. This division is achieved through the use of firewalls.

Confidential information transferred over insecure networks is encrypted, using SSL protocols or the VPN system with two-factor authentication.

6.6. Cryptographic module engineering controls

The cryptographic modules are subject to the engineering controls provided for in the standards indicated throughout this section.

The key generation algorithms used are commonly accepted for the use of the key for which they are intended.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

All cryptographic operations are performed in modules with Common Criteria EAL4+ certifications (EN 419 221-5, certificate CSA_CC_21008) and nShield 5c firmware modules.

6.7. Time sources

A time synchronisation procedure coordinated via NTP is in place, which accesses two independent services:

- The first synchronisation is with a service based on GPS antennas and receivers, called CRONOS, located at the antenna of the data centre (CPD) of ADAM ECOTECH, S.L., which provides a trust level of STRATUM 4 (with two systems in high availability), and which is connected to the CSUC.
- The second is a complementary synchronisation, via NTP, with the Real Instituto y Observatorio de la Armada (ROA) with a trust level of STRATUM 1.

In the event of a change in the certification status of the secure signature creation devices (SSCD) that support the provision of Trust Services, the following procedure will be applied:

1. A list of several certified SSCDs is maintained, together with a close relationship with the suppliers of such devices, in order to guarantee alternatives to possible loss of certification status of SSCD devices.

2. Should the validity period end or the certification be lost, such SSCDs will not be used for the provision of the time-stamping service.

3. Switching to SSCD devices with valid certification will be carried out immediately.

Should an SSCD device be shown never to have been what it claimed to be, through forgery or any other type of fraud, its clients and the regulatory body will be notified immediately, the certificates issued in such devices will be revoked and replaced by issuing them in valid SSCDs.

6.8. Accuracy of the time in the qualified electronic time-stamp

The UANATACA Qualified Time-Stamping service is based on the use of the TSP protocol over HTTP, defined in the RFC 3161 standard “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)”.

3G has a reliable time source in high availability that provides a trust level of STRATUM 4, via NTP, with the CSUC, as well as a trust level of STRATUM 1 with the ROA.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

The accuracy of the Qualified Time-Stamping service of 3G is 1 second with respect to UTC.

6.9. Change of status of a Qualified Signature Creation Device (SSCD)

In the event of a change in the certification status of the secure signature creation devices (SSCD) that support the provision of Trust Services, the following procedure will be applied:

1. A list of several certified SSCDs is maintained, together with a close relationship with the suppliers of such devices, in order to guarantee alternatives to possible loss of certification status of SSCD devices.
2. Should the validity period end or the certification be lost, such SSCDs will not be used for the provision of the time-stamping service.
3. Switching to SSCD devices with valid certification will be carried out immediately.
4. Should an SSCD device be shown never to have been what it claimed to be, through forgery or any other type of fraud, its clients and the regulatory body will be notified immediately, the certificates issued in such devices will be revoked and replaced by issuing them in valid SSCDs.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

7. TSU Certificate profile

The TSU Certificate profile for the provision of the time-stamping service follows the processes and indications established in the UANATACA Certification Practice Statement and Disclosure Statement, all available on the website: https://web.uanataca.com/

7.1.Certificate profile

TSU Certificates comply with the X.509 version 3 standard, RFC 3739 and the EN 319 422 standard.

7.1.1. Version number

UANATACA issues X.509 Version 3 certificates

7.1.2. Certificate extensions

The certificate extensions are detailed in the profile documents that are accessible from the UANATACA website (https://web.uanataca.com/).

This makes it possible to keep more stable versions of the Certification Practice Statement and to decouple them from the frequent adjustments to the profiles.

7.1.3. Algorithm object identifiers (OID)

The object identifier of the signature algorithm is:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

The object identifier of the public key algorithm is:

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4. Name formats

Certificates shall contain the information necessary for their use, as determined by the corresponding policy.

7.1.5. Name constraints

The names contained in certificates are restricted to X.500 “Distinguished Names”, which are unique and unambiguous.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

7.1.6. Certificate type object identifier (OID)

All certificates include a certificate policy identifier under which they have been issued.

7.2. Certificate Revocation List profile

The procedure for revocation, suspension and/or reactivation of TSU Certificates follows the processes and indications established in the UANATACA Certification Practice Statement and Disclosure Statement as Certification Authority, all available on the website: https://web.uanataca.com/

Version number

The CRLs issued by UANATACA are version 2.

OCSP profile

According to the IETF RFC 6960 standard.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

8. Compliance audit

3G has notified the National Supervisory Body of the start of its activity as a Certification Service Provider and is subject to the control reviews that this body considers necessary.

8.1.Frequency of the compliance audit

3G undergoes a compliance audit every 24 months, with annual surveillance audits, in addition to the internal audits that it carries out at its own discretion or at any time owing to a suspected breach of any security measure.

8.2. Identification and qualification of the auditor

The audits are performed by an independent external audit firm that demonstrates technical competence and experience in IT security, in information systems security and in compliance audits of public key certification services, and related elements.

8.3. Relationship of the auditor with the audited entity

The audit firms are of recognised standing, with departments specialised in carrying out IT audits, and therefore there is no conflict of interest that could undermine their performance in relation to 3G.

8.4. List of elements subject to audit

The audit verifies, with respect to 3G:

a) That the entity has a management system that guarantees the quality of the service provided.
b) That the entity complies with the requirements of the Certification Practice Statement and other documentation linked to the issuance of the various digital certificates.
c) That the Certification Practice Statement and other linked legal documentation conform to what has been agreed by 3G and to what is established in the regulations in force.
d) That the entity adequately manages its information systems.

8.5. Actions to be taken as a result of a non-conformity

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

Once the management has received the report of the compliance audit carried out, the deficiencies found are analysed with the firm that performed the audit, and corrective measures that resolve those deficiencies are developed and implemented.

If 3G is unable to develop and/or implement the corrective measures, or if the deficiencies found pose an immediate threat to the security or integrity of the system, it shall notify the team responsible for security immediately, which may take the following actions:

- Temporarily cease operations.
- Revoke the key of the TSU Certificate and regenerate the infrastructure.
- Terminate the Time-Stamping Authority (TSA) service.
- Other complementary actions that may be necessary.

8.6. Handling of audit reports

The audit result reports are delivered to the team responsible for security within a maximum period of 15 days after the audit has been carried out.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

9. Commercial and legal requirements

9.1.Fees

9.1.1 Time-stamping service fee

3G may establish a fee for the time-stamping service, of which subscribers will be duly informed, where applicable.

9.1.2. Fee for access to time-stamp status information

3G has not established any fee for access to time-stamp status information.

9.1.3 Fees for other services

No stipulation.

9.1.4. Refund policy

No stipulation.

9.2. Financial capacity

3G has sufficient financial resources to maintain its operations and fulfil its obligations, as well as to face the risk of liability for damages, as established in ETSI EN 319 401-1 7.12 c), in relation to the management of service termination and the termination plan.

9.2.1. Insurance coverage

3G has a sufficient guarantee of coverage of its civil liability, by means of a professional civil liability insurance, which it maintains in accordance with the applicable regulations in force.

9.2.2. Other assets

No stipulation.

9.2.3. Insurance coverage for subscribers and relying parties on time-stamps

3G has a sufficient guarantee of coverage of its civil liability, by means of a professional civil liability insurance, for electronic trust services, with a minimum insured amount of 1,500,000 euros.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

9.3. Confidentiality

9.3.1. Confidential information

The following information is kept confidential by 3G:

- Service requests, as well as any other personal information obtained for the provision of the service, except for the information indicated in the following section.
- Transaction records, including complete records and audit records of transactions.
- Internal and external audit records.
- Business continuity and emergency plans.
- Security plans.
- Documentation on operations, archiving, monitoring and the like.
- Any other information identified as “Confidential”.

9.3.2. Legal disclosure of information

3G discloses confidential information only in the cases provided for by law.

9.4. Personal data protection

3G guarantees compliance with the regulations in force on personal data protection, reflected in Regulation (EU) 2016/679 (General Data Protection Regulation) and, in general, any national legislation that is applicable.

In compliance therewith, 3G has documented in this Time-Stamping Certification Practice Statement the security and organisational aspects and procedures, in order to ensure that all personal data to which it has access are protected against loss, destruction, damage, falsification and unlawful or unauthorised processing.

All the necessary information regarding the processing of personal data carried out by 3G is set out below:

Data controller

The personal data provided in connection with the SERVICE will be processed by 3G SOLUCIONES DE MOVILIDAD, S.L., which acts as Data Controller and whose details are set out below:

3G SOLUCIONES MOVILIDAD, S.L.,
B09444431
Pasaje Gutierrez 3, 1º

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

47002 – Valladolid
+34 983101932
soporte@3gmg.com

Purpose of the processing

3G processes the personal data provided in order to carry out the electronic services requested, specifically the issuance of electronic certificates, all in accordance with the provisions of the Certification Practice Statement (CPS) of 3G, which is available at the following link:

https://www.3gmg.com/cualificado/DPC/index.html

The purposes of the processing of data relating to the SERVICE are the following:

- Identification of the subscribers of the service.
- Communications relating to the service.
- Custody and maintenance of the archive relating to the service.
- Administrative, accounting and invoicing management arising from the contracting.

Legal basis for the processing

In accordance with the processing purposes indicated, the legal basis for the processing of users' personal data is:

- The legal basis for the processing for the Provision of Electronic Trust Services is the performance of the contract for the services requested, to which the user is a party.

Data processed and retention

The categories of personal data processed by UANATACA include, by way of example but not limitation:

- Identification data: name, surnames and official identity number.
- Professional data: organisation, department and/or position.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

- Contact data: postal address, email address and telephone number.

Personal data will be retained until the end of the contractual relationship and thereafter for the periods legally required in each case. As a general rule, personal data relating to the service will be retained for 15 years from the end of the contract signed or of the provision of the trust service.

Data transfers

Data may be made available to third parties, within the territory of the European Union, in connection with the provision of services contracted by the user (for example data hosting providers (CPD), identification support services, group companies, etc.), all under the corresponding personal data processing agreement, guaranteeing at all times suitable security measures that ensure the due protection of users' personal data.

Without prejudice to the foregoing, as a general rule personal data will only be disclosed to third parties under a legal obligation.

As a general rule, no international transfers will be made.

User rights

Users may exercise their rights of confirmation, access, rectification, erasure, cancellation, restriction, objection and portability.

- Confirmation. All users have the right to obtain confirmation as to whether 3G is processing personal data concerning them.
- Access and rectification. Users have the right to access all their personal data, as well as to request the rectification of any data that is inaccurate or erroneous.
- Erasure and cancellation. Users may request the erasure/cancellation of data when, among other reasons, the data are no longer necessary for the purposes for which they were collected.
- Restriction and objection. The user may request the restriction of processing so that their personal data are not applied in the corresponding operations. In certain circumstances and on grounds relating to their particular situation, the user may object to the processing of data, in which case 3G is obliged to cease processing them, except for compelling legitimate grounds, or for the establishment, exercise or defence of possible claims.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

- Portability. Data subjects may request that their personal data be sent to them or transmitted to another controller, in a structured, commonly used electronic format.

To exercise their rights, users may send a request to the email address dpo@3gmg.com or send a written request to the address: Pasaje Gutiérrez 3,1 47002, Valladolid.

In that request, they must attach a copy of their identity document and clearly state which right they wish to exercise.

9.4.1. Notification to the Supervisory Body

In accordance with European Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS), 3G shall notify any breach of security or loss of integrity that has a significant impact on the provision of trust services within 24 hours after having become aware of it, to the competent supervisory body, regardless of the name it may bear at any given time.

In addition to the above, the same time limits shall be observed in respect of any breach of security or loss of integrity that has an impact on the Video Identification service, as well as in respect of the content of the notification, both initial and subsequent.

1.3.2.6 9.4.1.1 What to notify

Within a maximum of 24 hours after becoming aware of the incident, a first electronic notification with a brief description of its details must be sent to the Supervisory Body, which must contain, at least, the following information:

- Date and time at which the incident became known;
- Date and time of the end of the incident, where applicable, or of the expected date of its resolution;
- Contact details of the person responsible for managing the incident;
- Identification details of the trust service provider involved;
- Description of the service affected;
- Description, where applicable, of the personal data affected;
- Brief description of the security incident;
- Summary of the measures adopted or planned to be adopted to counter the incident;
- Where applicable, cross-border consequences of the incident.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

Subsequently, within a maximum of 1 month from its occurrence, and once the security incident, its causes, consequences and the measures taken have been thoroughly analysed, all the related information shall be notified to the Supervisory Body.

1.3.2.7 9.4.1.2. Whom to notify

The notification must be sent to the ministerial supervisory body that has the necessary powers in respect of receiving the notification, hereinafter the Ministry.

1.3.2.8 9.4.1.3. How to notify

The communication must be made through the procedure relating to electronic trust services on its Electronic Office (Sede).

Notifications under Articles 19.2, 21.1 and 24.2 of Regulation (EU) No 910/2014 on electronic identification and trust services, communications under Article 12 of Law 6/2020 of 11 November, and notifications under Article 5.4 of Order ETD/465/2021 of 6 May, as well as any other submission.

Electronic Office of the Ministerio para la Transformación Digital y de la Función Pública (Ministry for Digital Transformation and the Civil Service) - Details of Electronic Procedures (mineco.gob.es):
https://sedediatid.mineco.gob.es/es-es/procedimientoselectronicos/Paginas/detalle-procedimientos.aspx?IdProcedimiento=120

1.3.2.9 9.4.1.4. Responsibility

It is the responsibility of the Security Officer to make this communication. However, when deemed appropriate, communications may be channelled through Management.

9.4.2. Notification to the national data protection authority

In compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), where personal data may be compromised by a security breach, 3G, as controller, shall notify the security breach to the Agencia Española de Protección de Datos (AEPD, Spanish Data Protection Agency)

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

within 72 hours after having become aware of it. In addition to the preceding section on Notification to those affected, 3G shall notify the data subject if the breach entails a high risk to their rights and freedoms.

In addition to the above, the same time limits shall be observed in respect of any breach of security or loss of integrity that has an impact on the Video Identification service, as well as in respect of the content of the notification.

1.3.2.10 9.4.2.1 What to notify

Within a maximum of 72 hours after becoming aware of the incident, a brief description of its details must be notified, together with the scope of the personal data affected. The communication shall follow the communication template provided by the Agencia Española de Protección de Datos (AEPD), which must contain the following information:

Identification and contact details of:

- Entity/Controller
- Data Protection Officer (if designated) or contact person.
- Indication of whether it is a complete or partial notification. In the case of a partial notification, indicate whether it is a first notification or a supplementary notification.

Information on the personal data security breach:

- Date and time of detection.
- Date and time at which the incident occurs and its duration.
- Circumstances in which the personal data security breach occurred (for example, loss, theft, copying, etc.)
- Nature and content of the personal data concerned.
- Summary of the incident that caused the personal data security breach (indicating the physical location and the storage medium).
- Possible consequences and adverse effects on those affected.
- Technical and organisational measures adopted by the controller in accordance with Article 33.2.d) of the GDPR.
- Category of the data affected and number of records affected.
- Category and number of individuals affected.
- Possible cross-border issues, indicating the possible need to notify other supervisory authorities.

If, at the time of notification, it is not possible to provide all the information, it may be provided subsequently, gradually in different phases. The first notification shall be made

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

within the first 72h, and at least one final or closing communication shall be made when all the information relating to the incident is available.

Where the initial notification is not possible within 72 hours, the notification must nevertheless be made, and it must state and justify the reasons for the delay.

1.3.2.11 9.4.2.2. Whom to notify

The notification must be sent to the national data protection authority, currently the Agencia Española de Protección de Datos (AEPD).

1.3.2.12 9.4.2.3. How to notify

The notification to the AEPD shall be made through the form provided for that purpose and published on the agency's electronic office, at: https://sedeagpd.gob.es/sede-electronicaweb/vistas/infoSede/nbs/guiadoBrechasInicio.jsf

1.3.2.13 9.4.2.4. Responsibility

Responsibility for this communication lies with the Data Protection Officer of 3G or, failing that, the Security Officer. However, when deemed appropriate, communications may be channelled through Management.

9.5. Intellectual property rights

3G holds intellectual property rights over this Time-Stamping Certification Practice Statement.

9.6. Obligations and civil liability

9.6.1. Obligations of 3G

3G warrants, under its full responsibility, that it complies with all the requirements established in the Time-Stamping Certification Practice Statement, and is responsible for compliance with the procedures described, in accordance with the indications contained in this document.

3G provides electronic certification services in accordance with this Time-Stamping Certification Practice Statement.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

3G informs the subscriber of the terms and conditions relating to the provision of the time-stamping service, its price and its limitations of use, by means of a subscriber agreement that incorporates by reference the Disclosure Statements (PDS) of the service.

The Disclosure Statement document, also called PDS, meets the content of Annex A of ETSI EN 319 421; this document may be transmitted by electronic means, using a durable means of communication, and in understandable language.

3G binds subscribers and relying parties by means of that Disclosure Statement or PDS, in written and understandable language, with the following minimum contents:

- Requirements for compliance with the provisions of this document.
- Limits on the use of time-stamps.
- Information on how to validate a time-stamp, including the requirement to check its status, and the conditions under which it can reasonably be relied upon, which applies when the subscriber acts as a relying party.
- The way in which the financial liability of the Certification Service Provider is guaranteed.
- Applicable limitations of liability, including the uses for which the Certification Service Provider accepts or excludes its liability.
- Retention period for audit logs.
- Applicable dispute resolution procedures.
- Governing law and competent jurisdiction.

9.6.2. Warranties offered to subscribers and relying parties

In the documentation that binds it with subscribers and relying parties, 3G establishes and disclaims warranties, and applicable limitations of liability.

3G warrants to the subscriber that the time-stamps comply with all the material requirements established in this Certification Practice Statement, as well as the reference standards.

3G warrants to the relying party that relies on the time-stamp that the information contained in or incorporated by reference into the time-stamp is correct, except where otherwise indicated.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

9.6.3. Disclaimer of other warranties

3G disclaims any other warranty that is not legally enforceable, except those provided for in this document.

9.6.4. Limitation of liability

3G limits its liability to the provision of the time-stamp issuance service, which shall be governed by the relevant agreement.

3G does not carry out any verification of the document for which the time-stamp is requested, since it is sent directly by the Subscriber under its own and exclusive responsibility.

3G assumes no obligation with respect to monitoring the content, type and/or format of the documents and of the hash sent through the time-stamping process.

3G shall not be liable for any direct damage and/or damage caused by third parties as a result of the misuse of time-stamps duly issued in accordance with this document.

9.6.5. Fortuitous event and force majeure

3G includes in its certification policies clauses that limit its liability in the event of a fortuitous event and in the event of force majeure.

9.6.6. Governing law

3G establishes, in the subscriber agreement and in the Disclosure Statement or PDS, that the law governing the provision of the services, including the certification policy and practices, is Spanish law.

9.6.7. Severability, survival, entire agreement and notice clauses

3G establishes, in the subscriber agreement and in the Disclosure Statement or PDS, severability, survival, entire agreement and notice clauses:

- By virtue of the severability clause, the invalidity of a clause shall not affect the remainder of the agreement.

By virtue of the survival clause, certain rules shall remain in force after the end of the legal relationship governing the service between the parties. To this end, 3G ensures that, at least, the requirements contained in sections 1.12.1.12

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

9.6.8. Competent jurisdiction clause

3G establishes, in the subscriber agreement and in the Disclosure Statement or PDS, a competent jurisdiction clause, stating that international jurisdiction lies with the Spanish courts.

Territorial and functional jurisdiction shall be determined by virtue of the applicable rules of private international law and rules of procedural law.

9.6.9. Dispute resolution

3G establishes, in the subscriber agreement and in the Disclosure Statement or PDS, the applicable mediation and dispute resolution procedures.

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00

10. Annex I – Acronyms and glossary

AC	Certification Authority (Autoridad de Certificación)
CA	Certification Authority
RA	Registration Authority (Autoridad de Registro)
CN	Common Name
CP	Certificate Policy
CPD	Data Processing Centre (Centro de Procesamiento de Datos)
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DES	Data Encryption Standard
DN	Distinguished Name. Distinguished name within the digital certificate
DPC	Certification Practice Statement (Declaración de Prácticas de Certificación; CPS)
DSA	Digital Signature Algorithm. Signature algorithm standard
DSCF	Secure Signature Creation Device (Dispositivo Seguro de Creación de Firma; SSCD)
FIPS	Federal Information Processing Standard Publication
ISO	International Organization for Standardization
LRC	Certificate Revocation Lists (Listas de Revocación de Certificados; CRL)
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PC	Certificate Policy (Política de Certificación; CP)
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PSC	Certification Service Provider (Prestador de Servicios Electrónicos de Certificación; CSP)
RSA	Rivest-Shamir-Adleman. Type of encryption algorithm
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TSA	Time-Stamping Authority
TSU	Time-Stamping Unit

Sellado electrónicamente por
3G SOLUCIONES MOVILIDAD S.L.
B09444431
a las 25/11/2026 11:04:58 +01:00