Time-Stamp Policy
and
Time-Stamp Practise Statement

Version 1.1

11 January 2019

MSC Trustgate.com Sdn. Bhd.(478231-X)
Suite 2-9, Level 2
Block 4801 CBD Perdana, Jalan Perdana, 63000 Cyberjaya
Selangor Darul Ehsan, Malaysia
Tel: +603 8318 1800
www.msctrustgate.com
security@msctrustgate.com

Revision date: 11 January 2019

Trademark Notices

9

MSC Trustgate and its associated logos are the registered trademarks of MSC Trustgate.com Sdn Bhd or its affiliates. Other names may be trademarks of their respective owners.

Without limiting the rights reserved above, and except as licensed below, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without prior written permission of MSC Trustgate.

Notwithstanding the above, permission is granted to reproduce and distribute this MSC Trustgate Time-Stamp Policy and Time-Stamp Practise Statement on a nonexclusive, royalty-free basis, provided that (i) the foregoing copyright notice and the beginning paragraphs are prominently displayed at the beginning of each copy, and (ii) this document is accurately reproduced in full, complete with attribution of the document to MSC Trustgate.

Requests for any other permission to reproduce this MSC Trustgate Time-Stamp Policy and Time-Stamp Practise Statement must be addressed to MSC Trustgate.com Sdn Bhd, Suite 2-9, Level 2, Block 4801 CBD Perdana, Jalan Perdana, 63000 Cyberjaya, Selangor Darul Ehsan, Malaysia or via email at security@msctrustgate.com.

ACKNOWLEDGMENTS

This Time-Stamp Policy (TP) derives from the Internet Engineering Task Force (IETF) RFC 3628: Policy Requirements for Time-Stamping Authorities. It conforms to current versions of the requirements of the following schemes:

- Malaysia Digital Signature Act 1997
- Malaysia Digital Signature Regulations 1998
- Version 2.1 of WebTrust for Certification Authorities
- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification and Practices Framework
- RFC 3161: Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)
- RFC 5816: ESSCertIDV2 update to RFC 3161
- ETSI TS 102.023: Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

1. Introduction

This Time-Stamp Policy and Time-Stamp Practise Statement (TP/TPS) document is the principal policy governing MSC Trustgate Time-Stamping Authority ("Trustgate TSA"). It addresses areas of policy, practices, procedures and technical used for the provision of qualified electronic time stamps. The time stamps can be used in support of digital signatures or for any application requiring to prove that a datum existed before a particular time .

This TP/TPS describes the obligations that the Trustgate TSA should respect while generating, handling or delivering time-stamps. It is also intended to inform subscribers and relying parties about their obligations towards the time-stamps usage.

The structure and contents of this TP/TPS are laid out in accordance with ETSI EN 319 421" Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps". In addition, it is aiming to meet the general requirements of the international community to provide trust and confidence in electronic transactions including, amongst others, applicable requirements from Regulation (EU) No 910/2014.

This TP/TPS can be found on the MSC Trustgate's repository at www.msctrustgate.com. It may be updated from time to time.

2. Overview

This TP/TPS defines the policies and practices used for the operation and management of the Time-Stamping Services ("TSS") of Trustgate TSA, so that subscribers and relying parties can assess the confidence level of the operation of this service. Trustgate TSA use public key cryptography, public key certificates and reliable time sources to provide reliable standard based time-stamps and in accordance with patterns globally accepted.

The Trustgate TSA aims to provide time-stamping services used in support for qualified electronic signatures, as well as under applicable Malaysia laws and regulation. In addition, the time-stamps can also be used for any other purpose that requires proof that certain data existed at a specific time.

Subscribers and relying parties should consult the Trustgate's TPS to obtain further details of precisely how this time-stamp policy is implemented (e.g., protocols used in providing this service)

3. Terms and Definitions

3.1 Definitions

For the purposes of the present document, the following terms and definitions the following apply:

Certification Authority (CA): means an entity who issues certificate

Certificate Practise Statement (CPS): statement of the practices that a CA employs in issuing, managing and distributing digital certificates

Coordinated Universal Time (UTC): time scale based on the second as defined in recommendation ITU-R TF.460-6

ETSI EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

ETSI EN 319 422: Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

Relying Party: recipient of a time-stamp who relies on that time-stamp

Subscriber: legal or natural person to whom a time-stamp is issued and who is bound to any subscriber obligations

Time-Stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time

Time-Stamp Policy (TP): named set of rules that indicates the applicability of a time-stamp to a particular community and/or class of application with common security requirements

Time-Stamp Authority (TSA): an entity which issues time-stamps using one or more time-stamping units Time-Stamping Unit (TSU): set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time

Trust Service: electronic service that enhances trust and confidence in electronic transactions

TSA Disclosure statement: set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements

TSA Practice Statement (TPS): statement of the practices that a TSA employs in issuing time-stamp TSA system: composition of IT products and components organized to support the provision of time-stamping services

3.2 Abbreviations

For the purposes of the present document, the following abbreviation apply:

BIPM	Bureau International des Poids et Mesures
CA	Certification Authority
GMT	Greenwich Mean Time
IT	Information Technology
MCMC	Malaysian Communications and Multimedia Commission
MST	Malaysia Standard Time
NMIM	National Metrology Institute of Malaysia
TAI	International Atomic Time
TSA	Time-Stamping Authority
TSS	Time Stamp Services
TSU	Time-Stamping Unit
Trustgate	MSC Trustgate.com Sdn Bhd
UTC	Universal Time Coordinated

3.3 Modal Verbs Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described below:.

1. MUST This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

2. MUST NOT This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

3. SHOULD This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

4. SHOULD NOT This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

5. MAY This word, or the adjective "OPTIONAL", mean that an item is truly optional.

4. General Concepts

4.1 Time-Stamping Services

The provision of time-stamping services can be broken down into the following components:

- Time-stamping provision: technical components that issue timestamps;

- Time-stamping management: management, control and monitoring components of time-stamping services, including synchronization with reliable UTC time sources, to ensure that the services provided is as specified by the TSA.

4.2 Time-Stamp Authority

The main task of Trustgate TSA is to provision time-stamping services identified in clause 4.1. Trustgate TSA can operate one or more TSU's which creates and signs on behalf of Trustgate TSA. Trustgate TSA is to be trusted by subscribers and relying parties for the issuance of time-stamp tokens.

Trustgate TSA may use other parties to provide parts of the TSS. However, it always maintains overall responsibility and ensures that the policy requirements identified in the present document are met.

4.3 Subscribers

The subscriber can either be an organization comprising several end-users or an individual end-user that have agreed to Trustgate Subscriber Agreement.

4.4 Time-Stamp Policy and TSA Practice Statement

This section explains the relative roles of TP and TPS. It places no restriction on the form of a TP or TPS specification.

4.4.1 Purpose

In general, Trustgate TP ('what is adhered to") and Trustgate TPS ("how it is adhered to") have been merged into one document, the Trustgate TP/TPS. The relationship between the TP and TPS is similar in nature to the relationship of other business policies which state the requirements of the business, while operational units define the practices and procedures of how these policies are to be carried out.

4.4.2 Level of Specificity

Trustgate TP/TPS extends the CP/CPS which regulates the operation of the Trustgate CA and associated non-repudiation services. This TP/TPS provides detailed description of the terms and conditions as well as business and operational practices of Trustgate TSA in issuing and otherwise managing time-stamping services. In addition, it enforces the rules established by Trustgate TSA. The rules cover the technical, organizational and procedural requirements.

4.4.3 Approach

The Trustgate TP/TPS establishes the general rules concerning the operation of the Trustgate TSA. Additional internal documents define how Trustgate meets the technical, organizational, and procedural requirements identified in the Trustgate TP/TPS. These documents may be provided only under strictly controlled conditions.

5. Time-Stamp Policies

5.1 Overview

Trustgate TP/TPS is set of rules that indicates the applicability of a TST to a particular community or class of application with common security requirements, which include:

- The TSU, private keys, and profiles of public key certificates are in compliance with technical specifications of the RFC 3161 and RFC 3628
- Trustgate TSA holds private keys used in signing time-stamps
- TSTs are issued with the accuracy of ± 1 second, as indicated in Section 4.3 (Timestamp Authority Obligations)
- Means used in requesting for time-stamps include the Transfer Control Protocol (TCP) and Hypertext Transfer Protocol (HTTP).

5.2 Identification

The object identifier (OID) for the Trustgate TP/TPS is: 1.3.6.1.4.1.49530.1.3.1

By including this object identifier in a time-stamp, Trustgate TSA claims conformance to the identified TP and also the ETSI time-stamping identifier is being supported.

5.3 User Community and Applicability

The Trustgate TSA's User Community is composed of subscribers and relying parties. Accordingly, subscribers are also regarded as relying parties.

Trustgate TP/TPS is aimed at meeting the requirements of time-stamping qualified digital signatures for long term validity, but is generally applicable to any requirement for an equivalent quality.

This policy does not define restrictions on the applicability of the time-stamps issued.

5.4 Conformance

To show conformance with this document, the Trustgate TSA uses the identifier for the time- stamp policy established in Section 5.2 (Document Name and Identification) of this document in its issued TSTs.

The Trustgate TSA is subject to periodic independent internal and external audits. Trustgate TSA guarantees conformance of its implemented controls and ensures that it meets its obligations specified in Section 6.3 (TimeStamp Authority Obligations) of this document.

6. Trustgate TSA

6.1 Practise Statement

This TP/TSP establishes the general rules concerning the operation of the Trustgate TSA. The Trustgate CPS and additional internal documents define how Trustgate TSA meets the technical, organizational, and procedural requirements identified in TP/TPS.

This TP/TPS and other public documents may be found at http://www.msctrustgate.com/repository. Internal documents may be provided only under strictly controlled conditions.

Trustgate TSA conducts risk assessments to evaluate threats and to determine the necessary security controls and operational procedures.

6.2 Disclosure Statement

The TP/TPS disclosure statement can be found at http://www.msctrustgate.com/respository. This document discloses to all Subscribers and potential Relying Parties the terms and conditions regarding use of Trustgate TSS:

- The Trustgate TSA is a service of MSC Trustgate, which is licensed by MCMC as an authorised Certification Authority and TimeStamp Authority

- Each time-stamp token issued by the Trustgate TSA contains the policy object-identifier contained in section 5.2 Identification of this document.

- The cryptographic algorithms and key lengths used by the Trustgate TSA comply with ETSI TS 101.861 are as follows:
    - Hash: SHA2
    - Signature: SHA2WithRSAEncryption, 2048 bit key and SHA2WithECDSAEncryption, 256 bit key

- Trustgate TSA does not set reliance limits for time-stamp services beyond those outlined in section 6.5 Relying Party Obligations of this document. Trustgate TSA will post public notice on its website if the cryptographic algorithms and key lengths have been changed.

- The Trustgate TSA assures time with ±1 second of a trusted UTC time source and will not issue time-stamps outside this declared accuracy.

- Subscriber obligations are described in section 6.4 Subscriber Obligations of this document.

- Relying Party obligations are described in section 6.5 Relying Party Obligations of this document.

- Trustgate TSA maintains secure records concerning the operation of the Trustgate TSA according to section 5.5 Records Archival of the Trustgate CPS.

- Trustgate makes no express or implied representations or warranties relating to the availability or accuracy of the Trustgate TSA. Trustgate bears specific liability for damage to Subscribers and Relying Parties in relationship to valid qualified digital certificates relied upon in accordance with specific laws and regulations of Malaysia. These liabilities are described in section 6.8 Limitation of Liability of the Trustgate CPS.

- The applicable legal system and dispute resolution procedures relating to the Trustgate TSA are dealt with in the underlying Subscriber agreement.

- Trustgate TSA conformance with the applicable TP is confirmed by an independent certification body.

6.3 Obligations

The obligations of Trustgate TSA is as follows:

- Compliant with its TP/TPS
- Provide trustworthy time-stamp
- Provide UTC time accuracy of ± 1 second
- Deliver time-stamping services based on minimum 99,9% availability
- Perform internal and external audits to assure compliance to this policy
- Ensure that all requirements and procedures detailed in this TPS are implemented
- Authenticate requests for time countermarks using digital certificates.

6.4 Subscriber Obligations

The Subscriber's obligations are as follows:

- When the subscriber is an organization, some of the obligations that apply to that organization will have to apply to the end-users. In any case the organization will be held responsible if the obligations from its end-users are not correctly fulfilled and therefore the organization is expected to suitably inform its end users.

- When the subscriber is an end-user, the end-user will be held directly responsible if its obligations are not correctly fulfilled.

6.5 Relying Party Obligations

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

a. verify that the time-stamp token has been correctly signed and that the private key used to sign the timestamp has not been compromised until the time of the verification;

b. take into account any limitations on the usage of the time-stamp indicated by the timestamp policy;

c. take into account any other precautions prescribed in agreements or elsewhere. After expiry of the time-stamp certificate, the relying party should:
   - verify that the TSU private key is not revoked, and
   - verify that the cryptographic hash function and the signing algorithm used in the timestamp token are still considered secure.

6.6 Liability

Trustgate undertakes to operate the Trustgate TSA in accordance with this TP/TPS, Trustgate CPS, and the terms of service level agreements with the Subscriber. Trustgate makes no express or implied representations or warranties relating to the availability or accuracy of the time-stamping service.

Trustgate bears specific liability for damage to Subscribers and Relying Parties in relationship to valid qualified digital certificates relied upon in accordance with specific national laws and regulations. These liabilities are described in section 9.8 Limitation of Liabilities of the Trustgate CPS.

7. Trustgate TSA Management and Operation

7.1 TSU Key Management Life Cycle

7.1.1 TSU Key Generation

Trustgate generates the cryptographic keys used in its TSA services under the control of authorised personnel in a secure physical environment. Additional information is provided in Section 6.1 Key Generation and Installation of the Trustgate CPS. The keys are generated within TSU hardware security modules that are certified to FIPS 140-2 Level 3. Algorithms and key size are described in section 6.2 Disclosure Statement of this document.

7.1.2 TSU Private Key Protection

Trustgate takes specific steps to ensure that TSU private keys remain confidential and maintain their integrity. These include use of HSMs certified to FIPS 140-2 Level 3 to hold and sign with the keys.

7.1.3 TSU Public Key Distribution

Digital certificates used in the Trustgate TSA are issued by Trustgate CA according to certificate policies which provide a level of security equivalent to this time-stamping policy. Additional information is provided in section 6.1 Key Generation and Installation of the Trustgate CPS.

7.1.4 Rekeying TSU's Key

TSU private signing keys are replaced before the end of their validity period, (i.e., when their algorithm or key size are determined to be vulnerable). Additional information is provided in section 4.6 Certificate Renewal and section 4.7 Certificate ReKey of the Trustgate CPS.

7.1.5 End of TSU Key Life Cycle

TSU private signing keys are replaced upon their expiration. The TSU rejects any attempt to issue time-stamps once a private key has expired. After expiry, private keys are destroyed.

7.2 Time-Stamp Issuance

Trustgate has technical prescriptions in place to ensure that TSTs are issued securely and include the correct time. In line with the protocols referenced in Section 2 of this document, each TST includes:

- a representation (e.g., hash value) of the datum being time-stamped as provided by the requestor
- a unique serial number that can be used to both order TSTs and to identify specific TSTs
- an identifier for the time stamp policy
- the time calibrated to within 1 second of UTC, traceable to a UTC(k) source
- an electronic signature generated using a key used exclusively for time-stamping
- an identifier for the TSA and the TSU
  Trustgate maintains audit logs for all calibrations against the UTC(k) references, and will not issue TSTs when the time is out of the stated accuracy.

7.3 Clock Synchronization with MST

Trustgate TSA provides time with ±1 second of a trusted UTC time source. The TSUs have technical measures in place to ensure that the clocks do not drift outside the declared accuracy. The TSUs use DS/NTP, a mutually authenticated extension of the Network Time Protocol (NTP), to secure synchronizations with NMIM time source and to provide audit records that the time in a given TST is accurate.

TSU clocks are protected within the HSMs and are periodically recalibrated against NMIM time source. TSU clocks are also able to detect time-stamp drifts outside preset boundaries and request additional recalibrations as needed. If the TSU clock drifts or jumps out of synchronization with MST, and recalibration fails, the TSA will not issue time-stamps until correct time is restored. Manual administration of the TSU clock requires an authorized personnel.

Trustgate shall obtain written confirmation on annual basis from NMIM to verify that the TSU clocks are in synced with MST within the declared accuracy

7.4 Termination and Termination Plans

Trustgate TSA shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of its time-stamping services, and in particular ensure continued maintenance of information required to verify the correctness of time-stamp tokens.

Trustgate TSA shall:

a. make available to all subscribers and relying parties information concerning its termination;
b. terminate authorization of all subcontractors to act on behalf of Trustgate TSA in carrying out any functions relating to the process of issuing time-stamp tokens;
c. transfer obligations to a reliable party for maintaining event log, audit archives and to demonstrate the correct operation of the TSA for a reasonable period;
d. maintain or transfer to a reliable party its obligations to make available its public key or its certificates to relying parties for a reasonable period;
e. TSU private keys, including backup copies, shall be destroyed in a manner such that the private keys cannot be retrieved;
f. arrange to cover the costs to fulfil these minimum requirements in case Trustgate becomes bankrupt or for other reasons is unable to cover the costs by itself

8. General Security and Controls

8.1 Security Management

The configuration of the Trustgate TSA system as well as any modifications and upgrades are documented and controlled by the Trustgate TSA management. There is a mechanism for detecting unauthorised modification to the Trustgate TSA software or configuration. A formal configuration management methodology is used for installation and on-going maintenance of the Trustgate TSA system. The Trustgate TSA software, when first loaded, is checked as being that supplied from the vendor, with no modifications and is the version intended for use.

8.2 Asset Classification and Management

Trustgate TSA has ensured an appropriate level of protection of its assets including information assets. All information assets and has assigned a classification consistent with the risk assessment. All media are handled securely in accordance with requirements of the information classification scheme. Media containing sensitive data is securely disposed of when no longer required.

8.3 Human Resource Security

Please refer to Trustgate CPS Section 5.3 Personnel Control.

8.4 Physical and Environment Security

Trustgate TSA maintains physical and environmental security policies for systems used for time-stamps issuance and management which cover physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking & entering and disaster recovery. Controls should be implemented to avoid loss, damage or compromise of assets and interruption to business activities and theft of information and information processing facilities.

8.5 Operation Security

Please refer to Trustgate CPS Section 5.

8.6 Incident Management

Trustgate TSA handles incident and compromise according to incident and compromise handling procedures in order to minimise the impact of such events.

If any equipment is damaged or rendered inoperative but the Private Keys are not destroyed, the operation should be re-established as quickly as possible, giving priority to the ability to generate Certificate status information according to Trustgate CA's disaster recovery plan.

In the event a Trustgate TSA Private Key is Compromised, lost, destroyed or suspected to be Compromised: Trustgate TSA, after investigation of the problem, shall decide if the Trustgate TSA Certificate should be revoked. If so, then all the Subscribers who have been issued a Certificate will be notified at the earliest feasible opportunity. A new Trustgate TAA Key Pair shall be generated or an alternative existing TSA hierarchy shall be used to create new Subscriber Certificates.

8.7 Access Control

Please refer to Trustgate CPS Section 5.2 Procedural Control.

8.8 System Development and Maintenance

The system development controls for Trustgate TSA are as follows:

- Use software that has been designed and developed under a formal, documented development methodology;

- All hardware will be inspected during commissioning process to ensure conformity to supply and no evidence of tampering found. Hardware and software procured are purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase);

- Hardware and software are developed in a controlled environment and the development processes are defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software;

- The hardware and software are dedicated to performing CA/TSA activities. There are no other applications, hardware devices, network connections or component software installed which are not part of the CA/TSA operation;

- Proper care is taken to prevent malicious software from being loaded onto the equipment. Only applications required to perform the CA/TSA operations are installed on the equipment and are obtained from sources authorised by local policy. Trustgate TSA hardware and software are scanned for malicious code on first use and periodically thereafter; and

- Hardware and software updates are purchased or developed in the same manner as original equipment and are installed by trusted and approved personnel in a defined manner.

8.9 Business Continuity Management

The disaster recovery plan deals with the business continuity as described in Trustgate CPS Section 5.7. Certificate status information systems should be deployed so as to provide 24 hours per day, 365 days per year availability.

8.10 Compliance

Trustgate TSA offers its services in strict compliance with Digital Signature Act 1997 and Digital Signature Regulations 1998. Verification is performed through internal and external audits.

8.11 Collection of Evidence

The archive collection system complies with the security requirements described in Trustgate CPS Section 5.4 Audit Logging Procedure and 5.5 Records Archival.

Annex A (Normative) – Time-stamping protocol and time-stamp token profiles

A.1 Requirements for a time-stamping client

1.1 Profile for the format of the request

1.1.1 Core requirement

A time-stamping client shall support the time-stamping request as defined in IETF RFC 3161, clause 2.4.1 with the amendments defined in the following clauses.

1.1.2 Fields to be supported

The use of the following fields in the time-stamping request should be supported:

- the reqPolicy;
- the nonce; and
- the certReq.

1.1.3 Hash algorithms to be used

Hash algorithms used to hash the information to be time-stamped should be as specified in Annex A.4

1.2 Profile for the format of the response

1.2.1 Core requirement

A time-stamping client shall support the time-stamping response as defined in IETF RFC 3161, clause 2.4.2 with the amendments defined in the following clauses.

1.2.2 Fields to be supported

The following requirements apply:

- the accuracy field shall be supported; and
- the nonce field should be supported.

A TSU needs not support ordering hence clients should not depend on the ordering of time-stamps. If the nonce field is present in the request, the nonce field shall be present in the response with the same value.

1.2.3 Algorithms to be supported

Time-stamp token signature algorithms to be supported should be as specified in Annex A.4

1.2.4 Key lengths to be supported

Signature algorithm key lengths for the selected signature algorithm should be supported as recommended in Annex A.4

A.2 Requirements for a time-stamping server

2.1 Profile for the format of the request

2.1.1 Core requirement

A time-stamping server shall support the time-stamping request as defined in IETF RFC 3161, clause 2.4.1 with the amendments defined in the following clauses.

2.1.2 Fields to be supported

The following requirements apply:

- reqPolicy field shall be supported;
- the nonce field shall be supported; and
- certReq field shall be supported.

2.1.3 Algorithms to be supported

Hash algorithms for the time-stamp data to be supported should be as specified in Annex A.4

2.2 Profile for the format of the response

2.2.1 Core requirement

A time-stamping server shall support the time-stamping response as defined in IETF RFC 3161, clause 2.4.2 with the amendments defined in the following clauses.

2.2.2 Fields to be supported

The requirements from IETF RFC 3161, clause 2.4.2 shall apply and the following requirements apply:

- the policy field shall be present as an identifier for the time-stamp policy and shall conform to annex A;
- a genTime field shall have a value representing time with a precision necessary to support the declared accuracy shall be supported;
- the accuracy field shall be present and a minimum accuracy of one second shall be supported;
- the ordering field shall not be present or shall be set to false; and
- no extension shall be marked as critical.

The following requirement applies to the content of the SignedData structure in which the TSTInfo structure is encapsulated:

- the certificate identifier of the TSU certificate (ESSCertID as in IETF RFC 3161 or ESSCertIDv2 as in IETF RFC 5816) shall be included as a signerInfo attribute inside a SigningCertificate or a SigningCertificateV2 attribute as specified in IETF RFC 5816, clause 2.2.1.

2.2.3 Algorithms to be used

Hash algorithms used to hash the information to be time-stamped and time-stamp token signature algorithms should be as specified in Annex A (1).

A.3 TSU certificate profile

The TSU certificate shall meet the following requirements

3.1 Subject name requirements

The countryName attribute shall specify the country in which the TSA is established (which is not necessarily the name of the country where the TSU is located).

For a TSA being a legal person or a natural person associated with a legal person the organizationName shall contain the full registered name of the TSA responsible for managing the TSU. That name should be an officially registered name of the TSA.

The commonName specifies an identifier for the TSU. Within the TSA, the attribute commonName uniquely identifies the TSU used.

For a TSA being a natural person, one instance of the attribute serialNumber should be included in the subject field.

3.2 Key lengths requirements

The key length for the selected signature algorithm of the TSU certificate should be as recommended in Annex A.4

3.3 Key usage requirements

The TSU certificate extended key usage setting shall be as defined in IETF RFC 3161, clause 2.3

The TSU certificate private key usage period extension should be used in order to limit the validity of the TSU's signing key.

3.4 Algorithm requirements

The TSU public key and the TSU certificate signature should use the algorithms as specified in Annex A.4

A.4 Algorithms for Time Stamping

4.1 Time Stamping Token (TST)

The following requirements apply to hash functions and TST signature algorithms.

Time Stamping Token	TST Requesters	TST Issuers	TST Verifiers
Hash Function	shall support SHA-256	shall support SHA-256	shall support SHA-256
TST Signature Algorithms	shall support RSA with SHA-256 or SHA-512	shall support RSA with SHA-256 or SHA-512 should support EC-DSA with SHA-256	shall support RSA with SHA-256 or SHA-512 should support EC-DSA with SHA-256

4.2 TSU Certificate

TSU Certificates	Issuers of TSU Certificates	Users of TSU Certificates
TSU Public Key	should support RSA with SHA256 or SHA-512 should support EC-DSA with SHA-256	shall support RSA with SHA-256 or SHA512 should support EC-DSA with SHA-256
Issuer CA Public Key	shall support RSA with SHA-256 or SHA-512 should support EC-DSA with SHA-256	shall support RSA with SHA-256 or SHA512 should support EC-DSA with SHA-256