Time Stamping Services Guidelines for Certifying Authorities (CA)

August 2016

Version 1.0

Office of the Controller of Certifying Authorities
Information and Communication Technology Division
Ministry of Posts, Telecommunications and Information Technology

Document Control

Document Name	Time Stamping Services Guidelines for CAs
Version	1.0
Date	20 August 2016
Status	Release
Document Owner	Office of the Controller of Certifying Authorities, Bangladesh.

Signature:

(Abul Masur Mohammad Sharf Uddin)
Controller
Office of the Controller of Certifying Authorities (CCA)

Table of Contents

1.0 Introduction

According to the RFC 3161 standard, a trusted timestamp is a timestamp issued by a trusted third party (TTP) acting as a **Time Stamping Authority** (**TSA**). It is used to prove the existence of certain data before a certain point (e.g. contracts, research data, medical records etc.) without the possibility that the owner can backdate the timestamps. Multiple TSAs can be used to increase reliability and reduce vulnerability.

This is a guideline for implementation of Time Stamping Services by the Certifying Authorities (CA). In support of the ICT Act, 2006 (amended in 2009 and 2013), the Government of People's Republic of Bangladesh established the Office of the Controller of Certifying Authorities (CCA). Licensed Certifying Authorities (CAs) are required to operate Time Stamping Services. The CA shall not issue a Time stamping certificate other than for its own time stamping service. The Time Stamping Service provided by CA should be logically & physically separate from the CA systems. However CA can use the same physical infrastructure and resources. The Audit of the Time Stamping Service shall be included in the audit of CA facilities.

The CCA Public Key Infrastructure (PKI) is a hierarchical one. The CCA PKI consists of the CCA component(s) to meet the assurance requirements.

2.0 Object Identifier (OID)

OID for time stamp token as listed below

id-CCA	::= {2.16.50.1}
id-tsp	::= (id-CCA 3}
This identifier (i.e., {2.16.50.1.3.0} shall be asserted in every time stamp token.	

3.0 Time Stamp Certificate

The Time Stamping Certificates shall be issued by a CA or an Intermediate CA.

The Time Stamping Certificates shall be issued by an Intermediate CA. An intermediate CA with sub-CA must necessarily issue time stamping certificates only through its intermediate CA. If intermediate CA is having no sub-CA, a time stamping CA shall be created to issue time stamping certificates.

4.0 Time Stamp Requirements

4.1 Time Stamp Token

Time stamp tokens shall be in compliance with RFC 3161.

Each time stamp token shall have a unique identifier.

The time included in the time-stamp token shall be synchronized with Standard Time Source within the accuracy defined in this policy and, if present, within the accuracy defined in the timestamp token itself. The accuracy is defined to be ± 1 second. In compliance with RFC 3161, the time-stamp token shall include a representation (e.g., hash value) of the datum being time-stamped as provided by the time stamp requestor/subscriber. The time-stamp token shall be signed using a key generated exclusively for this purpose. The relying parties shall be able to ascertain this by the presence of a critical extended key usage extension of id-kp-time stamping {1 3 6 1 5 5 7 3 8}.

4.2 Time Stamping Services Clock

The time values that the Time Stamping services uses in the time-stamp token shall be traceable to a Standard Time Source in Bangladesh. The Time Stamping services' clocks shall be protected against threats which could result in an undetected change to the clock that takes it outside its calibration.

Examples of threats include tampering by unauthorized personnel, radio or electrical shocks. The CA shall provide a capability to detect the Time Stamping services clock being out accuracy specified in this guideline. When the Time Stamping services clock is detected as being out of the accuracy specified in this guideline, the event shall be audited and time-stamp tokens shall not be issued. Furthermore, this non-issuance shall be audited. Note: The BSTI (Bangladesh Standards and Testing Institution) is responsible for maintenance and development of the Bangladesh Standard Time and the Bangladesh Computer Council (BCC) Servers time will be treated as the Time Stamping server.

5.0 Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the Time Stamping services. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with Section below.

5.1.1 Types of Events Recorded

All security auditing capabilities of the operating system and the applications required shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. At a minimum, each audit record shall include the following (either recorded automatically or
manually for each auditable event):

1. The type of event,
2. The date and time the event occurred,
3. Success or failure where appropriate, and
4. The identity of the entity and/or operator that caused the event.

The following events shall be audited:

Auditable Event	CA
SECURITY AUDIT	
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X
Any attempt to delete or modify the Audit logs	X
LOGICAL ACCESS	
Successful and unsuccessful attempts to assume a role	X
The value of *maximum number of authentication attempts* is changed	X
The number of unsuccessful authentication attempts exceeds the *maximum authentication attempts* during user login	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X
An Administrator changes the type of authenticator, e.g., from a password to a biometric	X
KEY GENERATION	
Whenever the CA generates Time Stamping Services Signing Key Pair	X
KEY BACKUP AND RESTORE	
Backing up Time Stamping Services private key	X
Restoration of Time Stamping Services private key from backup	X

TIME STAMPING SERVICES CERTIFICATE REGISTRATION	
All Time Stamping Services certificate requests	X
CERTIFICATE REVOCATION	
All Time Stamping Services certificate revocation requests	X
CONFIGURATION	
Any security-relevant changes to the Time Stamping Services configuration	X

ACCOUNT ADMINISTRATION	
Roles and users are added or deleted	X
The access control privileges of a user account or a role are modified	X
TIME STAMP TOKEN MANAGEMENT	
All changes to the time stamp token profile	X
TIME CLOCK	
All changes to the Time Stamping Services time clock	X
All changes to the Time Stamping Services time source	X
MISCELLANEOUS	
Appointment of an individual to a Trusted Role	X
Designation of personnel for multiparty control	X
Installation of the Operating System	X
Installation of the Time Stamping Services Application	X
Installation of hardware cryptographic modules	X
Removal of hardware cryptographic modules	X
Destruction of cryptographic modules	X
Zeroization of cryptographic modules	X
System Startup	X
Logon attempts to Time Stamping Services	X
Application	X
Receipt of hardware / software	X
Attempts to set passwords	X
Attempts to modify passwords	X
Back up of the internal Time Stamping Services database	X
Restoration from back up of the internal Time Stamping Services database	X
File manipulation (e.g., creation, renaming, moving)	X
Access to the internal Time Stamping Services database	X
Re-key of the Time Stamping Services certificate	X
CONFIGURATION CHANGES	
Hardware	X

Software	X
Operating System	X
Patches	X
Security Profiles	X
PHYSICAL ACCESS / SITE SECURITY	
Personnel Access to room housing Time Stamping Services	X
Access to the Time Stamping Services	X
Known or suspected violations of physical security	X
ANOMALIES	
Software error conditions	X
Software check integrity failures	X
Receipt of improper messages	X
Misrouted messages	X
Network attacks (suspected or confirmed)	X
Equipment failure	X
Electrical power outages	X
Uninterruptible Power Supply (UPS) failure	X
Obvious and significant network service or access failures	X
Violations of Time Stamping Services	X
Resetting Operating System clock	X

5.1.2 Frequency of Processing Audit Logs

Frequency of Time Stamping Services audit log processing shall be in accordance with the requirements set for the CAs in Section 5.4.2 of the Bangladesh Root CA CPS.

5.1.3 Retention Period for Audit Logs

See Section 5.2.1.

5.1.4 Protection of Audit Logs

Protection of Time Stamping Services audit log shall be in accordance with the requirements set for the CAs.

5.1.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be archived per Section 5.2.1.

5.1.6 Audit Collection System (internal vs. external)

Time Stamping Services audit collection requirements shall be in accordance with the requirements set for the CAs.

5.2 Records Archival

5.2.1 Types of Records Archived

CA archive records shall be sufficiently detailed to establish the proper operation of the Time Stamping Services or the validity of any time stamp issued by the Time Stamping Services.

Data To Be Archived	**CA**
Contractual obligations	X
System and equipment configuration	X
Modifications and updates to system or configuration	X
Time stamp requests	X
Time stamp tokens	X
Record of Time Stamping Services Re-key	X
All Audit Logs	X
All Audit Log Summaries	X
Other data or applications to verify archive contents	X
Compliance audit reports	X

5.2.2 Retention Period for Archive

The archive retention period for Time Stamping Services shall be the same as those listed for Class 3 CA in Section 5.5.2 of the Bangladesh Root CA CPS.

5.2.3 Protection of Archive

Protection of Time Stamping Services archives shall be the same as those listed for CA in Section 5.5.3 of the Bangladesh Root CA CPS.

5.2.4 Archive Backup Procedures

No Stipulation.

5.2.5 Requirements for Time-Stamping of Records

Archived records shall be time stamped such that order of events can be determined.

5.2.6 Archive Collection System (Internal or External)

No stipulation.

5.2.7 Business Continuity Capabilities after a Disaster

In the case of a disaster whereby a Time Stamping Services installation is physically damaged and all copies of the Time Stamping Services Signing Key are destroyed as a result, the Time Stamping Services shall reestablish services as soon as practical

6.0 Time Stamping Services Certificate and Time Stamp Token Profiles

6.1 Time Stamping Services Certificate Profile

Time Stamping Services Certificate profile is detailed in the CCA's Digital Signature Interoperability Guidelines document.

6.2 Time Stamp Token Profile

6.2.1 Time Request Format

Time stamp requests sent to the CAs are not required to be signed, but may be at the discretion of the Issuer PKI. See RFC 3161 for detailed syntax. The

following table lists the fields that are expected by the Time Stamping Services.

*no extension is required to be supported

Field	Value
Version	V1 (1)
Message Imprint	Hash algorithm identifier, hashed message
Time Stamping Services Policy ID	Absent or id-tsp business {2.16.50.1.3.0}
Nonce	Optional
Certificate Request	Optional
Request Extension	**Value ***
None	None

6.2.2 Time Stamp Response Format

See RFC 3161 for detailed syntax. The following table lists which fields are populated by the Time Stamping Services.

Field	**Value**
Status As specified in RFC 3161	
Time Stamp Token	CMS signed Data content type with encapsulated content type of id-ct-TST Info {1.2.840.113549..1.9.16.1.4} – always contains Time Stamping Services certificate in Signing Certificate attribute which is part of the Signer Info

	Version: V1 (1)
	Time Stamping Services Policy ID: id-tsp business {2.16.50.1.3.0}
	Message Imprint (same as in the request)
	Serial Number (unique, up to 160 bits)
	Time Stamp: Generalized Time in UTC
	Accuracy: Optional
	Ordering: Optional
	Nonce: Same as in request; present if and only if in the request
	TSA: Time Stamping Services DN
Response Extension	**Value ***
None	None

*no extension is required to be generated, no extension shall be critical

7.0 Compliance Audit and Other Assessments

The Time Stamping Services compliance audit requirements shall be the same as those listed for CA in Section 8 and subsections thereof in Bangladesh Root CA CPS.

8.0 Other Business and Legal Matters

8.1 Confidentiality of Business Information

Each CA shall maintain the confidentiality of confidential business information that is clearly marked or labeled as confidential or by its

nature should reasonably be understood to be confidential, and shall treat such information with the same degree of care and security as the licensed CA treats its own most confidential information.

8.2 Privacy of Personal Information

CAs may store, process, and disclose personally identifiable information in accordance with the privacy policy of that Time Stamping Services

8.3 Intellectual Property Rights

CAs shall not knowingly violate any intellectual property rights held by others.

8.3.1 Property Rights in Certificates and Revocation Information

CAs may claim all Intellectual Property Rights in and to the time stamps they issue. However, they must grants permission to reproduce and distribute time stamp information on a non-exclusive royalty-free basis, provided that the recipient agrees to distribute them at no cost.

8.3.2 Property Rights in Keys

CAs may claim property rights to the keys they use (i.e., time stamp authority key pair).

8.3.3 Property Rights in Time Stamp Data

Time stamp applicants may claim property rights to the data they request to be time stamped.

8.4 Representations and Warranties

8.4.1 CA Representations and Warranties

8.4.1.1 CA

CAs represents and warrants that:
1. Time Stamping Services signing private key is protected and that no unauthorized person has ever had access to that private key; and
2. All representations made by the CA in any applicable agreements are true and accurate, to the best knowledge of the applicable CA

8.4.2 Relying Party

Parties who rely upon the time stamps issued under this Time Stamping Services shall:

1. Validate the certification path for the Time Stamping Services certificate using procedures described in RFC 5280;
2. Verify that the Time Stamping Services certificate contains extended key usage extension with id-kp-time stamping {1 3 6 1 5 5 7 3 8} OID; and
3. Signature on the time stamp verifies using the Time Stamping Services public key in the Time Stamping Services public key certificate.

8.5 Dispute Resolution Provisions

8.5.1 Disputes among CAs and Customers

Provisions for resolving disputes between a CA and its Customers shall be set forth in the applicable agreements between the parties.

Dispute resolution procedures shall be consistent with Information & Communication Technology Act, 2006.

8.5.2 Alternate Dispute Resolution Provisions

No stipulations.

8.6 Governing Law

The laws of Bangladesh and more particularly the Information & Communication Technology Act, 2006, The Information Technology (Certifying Authorities) Rules, 2009 and Bangladesh Root CA Certification Practice Statement,2013 and the guidelines issued and clarifications made from time to time by the Controller of Certifying Authorities, Ministry of Posts, Telecommunications and Information Technology shall govern the construction, validity, enforceability and performance of actions per this Time Stamping Service guidelines

8.7 Miscellaneous Provisions

8.7.1 Force Majeure

CAs shall not be liable for any failure or delay in its performance under this Time Stamping Services due to causes that are beyond their reasonable control, including, but not limited to, an act of God, act of civil or military authority, fire, epidemic, flood, earthquake, riot, war, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and Governmental action.