

# **Time-Stamping Service Practice Statement**

**Version 2.2**

**June 15, 2010**

## Revision History

Ver.	Date	Sections Affected	Descriptions
1.0	September 21, 2004		First Edition
2.0	November 30, 2005	All	Second edition (to reflect changes regarding the Service valid for 10 years). Changed some terms
		Allowable error (Time accuracy)	Changed the allowable error to +/- 1 second or less
		Conditions for revocation of Time stamp Token	Eliminated the revocation of Time stamp Token due to time accuracy by not issuing Time stamp in advance when time accuracy is in question
		1.2.2	Changed OID of the Service and thus changed Policy OID
		1.3.2 a)	Changed SHA-1 to SHA-512
		1.3.2 (3)	Changed the validity period of Time stamps from 5 to 10 years
		2.1.5 (1)	Changed the validity period of Public Key Certificate from 6 to 11 years
		4.7.1	Changed archival storage period from 10 to 15 years
		4.8	Changed Key update timing from 5 to 10 years
		6	Changed the chapter title
		6.1.5	Corrected the Public Key length (1024 -> 2048)
		6.2.1	Changed certified FIPS from FIPS 140-1 Level 3 to FIPS 140-2 Level 3_
		6.3	Changed the validity period of Public Key Certification from 6 to 11 years Changed the description about the active period of Private Key from "5 years before" to "10 years before"

Ver.	Date	Sections Affected	Descriptions
		8	<p>Changed the Document Hash algorithm from SHA-1 to SHA-512</p> <p>Changed the signature algorithm from SHA-1 with RSA Encryption to SHA-512 with RSA Encryption</p> <p>Changed TSA Policy OID from (0 2 440 200185 1 1 1) to (0 2 440 200185 1 2 1)</p>
2.1	September 21, 2006	<p>1.2.2</p> <p>2.3.2 (3)</p> <p>3.2</p> <p>4.1</p> <p>4.3</p> <p>4.5.1 (2)</p> <p>4.6.4</p> <p>4.6.5</p>	<p>Modified Public Key Certification (1.2.392.20075.2.7 -&gt;1.2.392.200075.2.7)</p> <p>Added a description "except for the case where the TSA is not notified of the contact address"</p> <p>Added a condition under which the authenticity of applicants is confirmed</p> <p>Added descriptions about cases where private information is not submitted upon applications</p> <p>Add a postscript about NDA</p> <p>Added a description, "except in cases where the TSA is not notified of the contact address"</p> <p>Changed the title and part of descriptions (backup -&gt; storage)</p> <p>Deleted a term "automatically"</p>
2.2	June 15, 2010	<p>1.2.1</p> <p>1.2.2</p> <p>1.3.1 (2)</p> <p>1.3.1 (3)</p> <p>2.1.4 (3)</p> <p>2.5.2</p> <p>4.5.1 (2)</p> <p>4.11 (1)</p> <p>4.11 (2)</p> <p>4.6.5</p> <p>6.5, 6.6, 6.7</p> <p>8</p>	<p>Changed the version number and modified date</p> <p>Changed the service and Policy OID</p> <p>Modified TA</p> <p>Modified CA</p> <p>Modified time error</p> <p>Added revocation information</p> <p>Modified the reason of suspension of the Service</p> <p>Modified TA</p> <p>Modified TA</p> <p>Modified the method for collecting the security inspection logs</p> <p>Modified the duplicated descriptions</p> <p>Added "parameters"</p> <p>Modified "GenTime", "TSApolicyId" and "Ordering"</p>

# Table of Contents

<b>Time-Stamping Service Practice Statement</b> .....	<b>i</b>
<b>Version 2.2</b> .....	<b>i</b>
<b>June, 2010</b> .....	<b>i</b>
<b>Revision History</b> .....	<b>i</b>
<b>Table of Contents</b> .....	<b>iii</b>
<b>1. Introduction</b> .....	<b>1</b>
<b>1.1 Overview</b> .....	<b>1</b>
<b>1.2 Identification</b> .....	<b>1</b>
1.2.1 <i>Document Name and Version</i> .....	1
1.2.2 <i>The Service and Object Identifiers (OIDs)</i> .....	1
<b>1.3 Definitions and Applicable Scope</b> .....	<b>2</b>
1.3.1 <i>Definitions</i> .....	2
1.3.2 <i>Contents of Time-Stamping Service</i> .....	3
1.3.3 <i>Applicability of Time Stamp Token</i> .....	4
<b>1.4 Contact Details</b> .....	<b>4</b>
<b>2. General Provisions</b> .....	<b>5</b>
<b>2.1 Obligations and Responsibilities</b> .....	<b>5</b>
2.1.1 <i>Obligations of Time-Stamping Authority</i> .....	5
2.1.2 <i>Obligations of Subscribers</i> .....	5
2.1.3 <i>Obligations of Relying Parties</i> .....	6
2.1.4 <i>Obligations of Time Authority</i> .....	6
2.1.5 <i>Obligations of Certification Authority</i> .....	7
2.1.6 <i>Repository-Related Obligations</i> .....	7
<b>2.2 Financial Responsibilities</b> .....	<b>7</b>
2.2.1 <i>Liability for Damage</i> .....	7
2.2.2 <i>Exception Clauses</i> .....	8
<b>2.3 Interpretation and Enforcement</b> .....	<b>8</b>
2.3.1 <i>Governing Law</i> .....	8
2.3.2 <i>Severability, Survival, and Notices</i> .....	8
2.3.3 <i>Dispute Resolution</i> .....	9
<b>2.4 Fees</b> .....	<b>9</b>
<b>2.5 Disclosure and Repository</b> .....	<b>9</b>
2.5.1 <i>Disclosure of TSA-Related Information</i> .....	9

	2.5.2 Revision of Public Information.....	9
	2.5.3 Access Controls .....	10
	2.5.4 Repository.....	10
<b>2.6</b>	<b>Compliance Audit .....</b>	<b>10</b>
	2.6.1 Frequency of Compliance Audit .....	10
	2.6.2 Identity / Qualification of Auditor .....	10
	2.6.3 Relationship between Auditor and Auditee .....	10
	2.6.4 Purpose of Audit .....	10
	2.6.5 Actions against Incompliance.....	10
	2.6.6 Report on Result of Audit.....	11
<b>2.7</b>	<b>Confidentiality.....</b>	<b>11</b>
	2.7.1 Information Considered Confidential.....	11
	2.7.2 Information Not Considered Confidential .....	11
	2.7.3 Disclosure of Revocation Information of Public Key Certificates... ..	12
	2.7.4 Disclosure to Law Enforcement Officials.....	12
	2.7.5 Information Disclosure by Other Reasons.....	12
<b>2.8</b>	<b>Intellectual Property Rights .....</b>	<b>12</b>
<b>2.9</b>	<b>Handling of Private Information .....</b>	<b>12</b>
<b>3.</b>	<b>Identification and Authentication .....</b>	<b>14</b>
<b>3.1</b>	<b>Initial Registration .....</b>	<b>14</b>
	3.1.1 Type of Names.....	14
	3.1.2 Meaning of Names .....	14
	3.1.3 Uniqueness of Names.....	14
<b>3.2</b>	<b>Applicant Authentication for Service.....</b>	<b>14</b>
<b>3.3</b>	<b>Renewal of the Service Contract .....</b>	<b>14</b>
<b>3.4</b>	<b>Termination of the Service Contract .....</b>	<b>14</b>
<b>4.</b>	<b>Operational Requirements .....</b>	<b>15</b>
<b>4.1</b>	<b>Application for Use of the Service .....</b>	<b>15</b>
<b>4.2</b>	<b>Time Stamp Request .....</b>	<b>15</b>
<b>4.3</b>	<b>Issuance of Time Stamp Token .....</b>	<b>15</b>
<b>4.4</b>	<b>Verification of Time Stamp Token .....</b>	<b>15</b>
<b>4.5</b>	<b>The Service Suspension and Termination.....</b>	<b>16</b>
	4.5.1 Suspension of the Service .....	16
	4.5.2 Cancellation of Suspension of the Service.....	16
	4.5.3 Suspension of the Service to Subscribers.....	16

	4.5.4 Cancellation of Suspension of the Service to Subscribers.....	17
	4.5.5 Revocation of the Service .....	17
<b>4.6</b>	<b>Security Inspection Procedure .....</b>	<b>17</b>
	4.6.1 Information to be Recorded in Security Inspection Log.....	17
	4.6.2 Inspection Frequency of Security Inspection Log.....	18
	4.6.3 Protection of Security Inspection Log.....	18
	4.6.4 Procedure for Storage of Security Inspection Log.....	18
	4.6.5 Collection of the Security Inspection Log .....	18
	4.6.6 Assessment of Vulnerability .....	18
<b>4.7</b>	<b>Archive .....</b>	<b>18</b>
	4.7.1 Type of Archive .....	18
	4.7.2 Protection of Archived Data .....	19
	4.7.3 Archive Retention.....	19
<b>4.8</b>	<b>Key Renewal.....</b>	<b>19</b>
<b>4.9</b>	<b>Recovery from Compromise and Disaster .....</b>	<b>19</b>
	4.9.1 Actions for Destruction of Hardware, Software, or Data.....	19
	4.9.2 Requirements of Revocation of Time Stamp Token.....	19
	4.9.3 Conditions for Free Issuance of Time Stamp Token .....	20
	4.9.4 Private Key Compromise Control.....	20
	4.9.5 Restoration of Facilities at Disasters.....	20
<b>4.10</b>	<b>Termination of the Service.....</b>	<b>20</b>
<b>4.11</b>	<b>Time Synchronization with UTC .....</b>	<b>21</b>
<b>4.12</b>	<b>Time Traceability .....</b>	<b>21</b>
<b>5.</b>	<b>Physical, Procedural, and Personnel Security Management.....</b>	<b>22</b>
<b>5.1</b>	<b>Physical Management .....</b>	<b>22</b>
	5.1.1 Location and Structure .....	22
	5.1.2 Physical Access .....	22
	5.1.3 Power and Air Conditioning.....	22
	5.1.4 Flood-Control Measures.....	22
	5.1.5 Anti-earthquake Measures .....	22
	5.1.6 Anti-Fire Measures.....	22
	5.1.7 Media Storage.....	23
	5.1.8 Material Disposal.....	23
	5.1.9 Off-Site Backup.....	23
<b>5.2</b>	<b>Procedure Management .....</b>	<b>23</b>
<b>5.3</b>	<b>Personnel Management .....</b>	<b>23</b>

5.3.1	<i>Background, Qualification, Experience, and Prerequisite Conditions</i> .....	23
5.3.2	<i>Training Requirements</i> .....	23
5.3.3	<i>Retraining Frequency and Requirements</i> .....	24
5.3.4	<i>Sanctions for Unauthorized Actions</i> .....	24
5.3.5	<i>Documentation Supplied to Personnel</i> .....	24
<b>6.</b>	<b>Technical Security Management</b> .....	<b>25</b>
<b>6.1</b>	<b>Key Pair Generation and Installation</b> .....	<b>25</b>
6.1.1	<i>Key Pair Generation</i> .....	25
6.1.2	<i>Time Stamp Unit Public Key Registration with Certification Authority</i> .....	25
6.1.3	<i>Receipt of Route Certificate from Certification Authority</i> .....	25
6.1.4	<i>Receipt of Route Certificate for Public Key Certificate of Time Authority</i> .....	25
6.1.5	<i>Key Size</i> .....	25
6.1.6	<i>Hardware / Software for Key Generation</i> .....	25
6.1.7	<i>Purpose of Use of Key</i> .....	25
<b>6.2</b>	<b>Private Key Protection</b> .....	<b>25</b>
6.2.1	<i>Standards for Cryptographic Modules</i> .....	25
6.2.2	<i>Private Key Multi-Personnel Management</i> .....	26
6.2.3	<i>Private Key Escrow</i> .....	26
6.2.4	<i>Private Key Backup</i> .....	26
6.2.5	<i>Private Key Archival</i> .....	26
6.2.6	<i>Private Key Entry into Cryptographic Module</i> .....	26
6.2.7	<i>Method of Activating Private Key</i> .....	26
6.2.8	<i>Method of Deactivating Private Key</i> .....	26
6.2.9	<i>Method of Destroying Private Key</i> .....	26
<b>6.3</b>	<b>Validity Period of Public Key and Private Key</b> .....	<b>26</b>
<b>6.4</b>	<b>Activation Data</b> .....	<b>27</b>
6.4.1	<i>Activation Data Generation and Installation</i> .....	27
6.4.2	<i>Activation Data Protection</i> .....	27
<b>6.5</b>	<b>Computer Security</b> .....	<b>27</b>
<b>6.6</b>	<b>Network Security</b> .....	<b>27</b>
<b>6.7</b>	<b>Cryptographic Module Engineering Management</b> .....	<b>27</b>
<b>7.</b>	<b>Management of Time-Stamping Service Practice Statement</b> .....	<b>28</b>

7.1	Modification of TPS .....	28
7.2	Publication and Notification Policies of TPS.....	28
8.	Time Stamp Token Profile.....	29
	Appendix: Abbreviations and Definitions .....	34

# 1. Introduction

This document, or Time-Stamping Service Practice Statement (hereinafter referred to as the "TPS"), states the basic operations of Time-Stamping Service (hereinafter referred to as the "Service") provided by a Time-Stamping Authority operated by PFU LIMITED (hereinafter referred to as "PFU"). The Time Stamp discussed in this TPS shall be issued in accordance with "Public Key Infrastructure: Time Stamp Protocol (TSP)" of IETF RFC 3161. We drew upon "Time-Stamping Service Practical Guideline" made public by the Electronic Commerce Promotion Council of Japan (ECOM) for determining the organization and descriptions of this TPS.

## 1.1 Overview

This statement gives you information about the operational policy and business procedures of the Service that the PFU-operated Time-Stamping Authority (hereinafter referred to as the "TSA") provides.

This statement is applicable to all applicants, Subscribers, and relying parties, as well as all individuals, corporations, and organizations relating to the Service, and it expresses the rights and obligations of the TSA and all of those mentioned above.

The TSA does not define the Time Stamp Policy and Time-Stamping Practice Statement separately; it positions this Statement as the operational policy of the Service of the PFU TSA.

## 1.2 Identification

### 1.2.1 Document Name and Version

Document Name: Time-Stamping Service Practice Statement

Version: 2.2

Date modified: June 15, 2010

Prepared by: PFU LIMITED

Date on which the revision becomes effective: July 20, 2010

### 1.2.2 The Service and Object Identifiers (OIDs)

This section describes the following object identifiers (OIDs) to which this TPS is applicable:

- PFU LIMITED: 0.2.440.200185
- Time-Stamping Service: 0.2.440.200185.1.2
- Time Stamp Policy: 0.2.440.200185.1.2.2
- Time Source used by the TSA
  - SecureNTP Time Authentication Service: 0.2.440.200125.1.6
  - Time Attribute Certificate Policy: 0.2.440.200125.1.6.1

- Certification Authority policy used by the TSA  
Public Key Certificate Policy for SecureSignAD Time Stamp: 1.2.392.200075.4.2

## 1.3 Definitions and Applicable Scope

### 1.3.1 Definitions

- (1) Time-Stamping Authority (TSA)  
“Time-Stamping Authority” in this TPS shall mean any entity that issues Time Stamp Tokens that conform to the RFC3161-based Time-Stamp protocol upon reception of time information from a Time Source. The TSA described in this TPS means the TSA of PFU.
- (2) Time Authority (TA)  
“Time Authority” in this TPS shall mean any entity that provides time synchronized with the coordinated universal time (hereinafter referred to as the “UTC”) for Time Stamp Unit managed by the TSA, as a time source that possesses the traceability to the UTC according to 4.12 and that performs time audits on the clock of the Time Stamp Unit. The TSA designates the SecureNTP Time Authority operated by Seiko Instruments Inc. as a Time Authority (hereinafter referred to as the “TA”) and uses the SecureNTP Time Authentication Service of the company.
- (3) Certification Authority (CA)  
“Certification Authority” in this TPS shall mean a Certification Authority for Public Key Infrastructure (hereinafter referred to as PKI), which is an entity that authenticates the Public Key Certificate of the PKI used by the TA server of the TSA-managed Time Stamp Unit or that of the TA. The TSA designates Japan Certification Service, Inc. as the Certification Authority (hereinafter referred to as the “CA”) and uses the SecureSignAD Service of the company. For details of the CA for the TA, refer to the Time Authority Practice Statement.
- (4) Subscriber(s)  
“Subscriber(s)” in this TPS shall mean any person or entity that applies for and, if accepted, receives the Service (use of the Service) provided by the TSA.
- (5) Relying Party  
“Relying Party” in this TPS shall mean any person or party who uses or verifies Time Stamp Tokens issued by the TSA. Subscribers defined in the previous Section will be considered relying parties when they use or verify Time Stamp Tokens.
- (6) Time Stamp Token (TST)  
“Time Stamp Token” in this TPS shall mean a digital certificate issued for hash values sent by a Subscriber for the purpose of descriptions in Section 1.3.3 (1). A Time Stamp Token contains the time at which the Time Stamp Token is issued by the Time Stamp Unit, which issued the Time Stamp Token; it also contains the identification information of the Time Stamp Unit.  
The profile of the Time Stamp Token is described in Section 8.
- (7) Time Attribute Certificate

“Time Attribute Certificate” in this TPS shall mean a digital certificate that contains the time and date on which the time source of the Time Stamp Unit that issued Time Stamp Tokens and the Time Stamp Unit itself undergo a time audit, as well as the time error at the time of the audit. A Time Attribute Certificate is issued to the TSA by the TA. The Time Stamp Unit is allowed to issue Time Stamp Tokens when the time error between the Time Stamp Unit and UTC is within +/- 500 milliseconds at the point of the time audit conducted by the TA, only in the validity period of the Time Attribute Certificate.

The TSA can include Time Attribute Certificates in its Time Stamp Tokens at own discretion.

(8) Repository

“Repository” in this TPS shall mean any system to store the related information necessary for verification of Time Stamp Token.

### 1.3.2 Contents of Time-Stamping Service

The Time-Stamping Service includes the following:

- (1) Upon a request from a Subscriber, the TSA shall generate an RFC3161-compliant Time Stamp Token for the hash value sent by the Subscriber and shall send it to the Subscriber.
  - a) The hash algorithm to be applied shall be SHA-512.
  - b) Time Stamp Tokens shall be generated using any Time Stamp Unit managed by the TSA and digitally signed using a Private Key that is unique to each Time Stamp Unit.
  - c) The TSA shall have no concern with the content of Time Stamp targets (content of original data for which hash values calculated).
  - d) No Time Stamp Token shall include information that can be used to identify Subscribers.
  - e) Data exchanges between the TSA and a Subscriber shall be conducted in a way in which security can be implemented. The details of the communication procedure are defined separately.
- (2) Time to be provided in Time Stamp Tokens shall be given in accordance with the provisions of this TPS so that the following conditions are met:
  - a) A time provided in a Time Stamp Token shall be the time of the clock of the Time Stamp Unit.
  - b) In an audit conducted according to Section 2.1.4 (1) by the TA, if it is confirmed that there is a time error of more than +/- 500 milliseconds between the time of the Time Stamp Unit clock and UTC, the Time Stamp Unit's function of issuing Time Stamp Tokens is disabled according to Section 2.1.4 (2).
  - c) Every time a Time Stamp Token is issued, an issue time provided with the Time Stamp Token generated by the Time Stamp Unit is compared with that of a Time Source synchronized with UTC other than the TA. If the TA finds a time error of more than +/- 1 second between those above, Time Stamp Tokens that contain a wrong time shall be discarded within the TA and not

issued for users.

- d) Within the allowable error range of +/- 1 second, the order of times provided in Time Stamp Tokens shall not have any significance. In addition, the serial numbers of Time Stamp Tokens shall not have any significance because those numbers are issued by multiple Time Stamp Units.
  - e) A time value provided in a Time Stamp Token shall not indicate the time at which a request for issuance of a Time Stamp is accepted but shall be the actual time at which the Time-Stamping process is conducted.
  - f) It is not guaranteed that the order in which Time Stamp requests are accepted is equal to the order in which the Time Stamp Tokens are generated (time order).
- (3) The validity period of a Time Stamp Token shall be the validity period of a Public Key certificate corresponding to the Private Key that is described in Section 6.3, and that is used for digital signature in the Time Stamp Token. In accordance with Section 6.3, the TSA shall secure 10 years of validity period for the Time Stamp Token issued to a Subscriber except for the case referred to in Section 4.9.2.

### **1.3.3 Applicability of Time Stamp Token**

(1) Suitable Applications

The purpose of Time Stamp Tokens is to verify that digital data corresponding to the relevant hash value of digital data owned by a Subscriber of the TSA remains in the same state as it was at the time provided in the Time Stamp Token, and that such digital data existed on and before that time. Subscribers and Relying Parties may use Time Stamp Tokens only for the purpose described above. In addition, it is possible for Subscribers to copy and distribute Time Stamps.

(2) Prohibited Applications

Subscribers and Relying Parties shall use Time Stamp Tokens only for the purpose described in the previous Section and shall not use in high safety applications, which directly involve danger to life and health, if the safety is not guaranteed.

## **1.4 Contact Details**

When you have any questions about this TPS, please feel free to contact us.

For the information about contacts, visit: <http://www.pfutsa.net/en/faq>

## **2. General Provisions**

### **2.1 Obligations and Responsibilities**

#### **2.1.1 Obligations of Time-Stamping Authority**

In providing the Service, the TSA shall fulfill obligations to Subscribers to perform the following operations according to this TPS and have financial responsibilities as set forth in Section 2.2. However, when Subscribers or Relying Parties use Time Stamp Tokens issued by the TSA according to this TPS, the TSA shall not be responsible or liable for the result of using digital data to which Time Stamps are applied and/or Time Stamp Tokens applied to the digital data.

(1) Generation/Issuance of Time Stamp Token

The TSA shall generate Time Stamp Tokens and issue them to Subscribers.

(2) Time control

The TSA shall control its system time so that a Time Stamp Token issue-time error does not exceed the value specified in Section 1.3.2 (2) c).

(3) Security management

The TSA shall manage the time, the Private Key, other equipment, systems, and data of the Time Stamp Unit in order to provide the Service.

(4) Revocation request for Private Key and Notification of revocation

When the Private Key of the Time Stamp Unit is compromised, the TSA shall request the revocation of the relevant Private Key to the CA, and then notify Subscribers of it. In addition, when the revocation of the Private Key is requested on accounts other than the compromise of the Private Key, the TSA shall notify Subscribers of it in advance.

Subscribers shall be notified of revocation as described in Section 2.3.2 (3).

#### **2.1.2 Obligations of Subscribers**

When applying for the Service, Subscribers shall have the following obligations with their agree to the contents described in this TPS. When using Time Stamp Tokens issued by the TSA under this TPS, Subscribers shall be responsible for digital data that is Time-Stamped and the result of using the Time Stamp Tokens provided for that digital data.

(1) Compliance with restrictions on the use of Time Stamp Tokens

Time Stamp Tokens are issued under this TPS, which describes the purposes and applicable scope of Time Stamp Tokens. Subscribers shall read this TPS thoroughly before using Time Stamp Tokens.

(2) Compliance with this TPS

Subscribers shall comply with this TPS, and, when copying and distributing the Time Stamp Tokens to Relying Parties, Subscribers shall obligate those parties to comply with this TPS.

- (3) Verification of Repository and notifications

Subscribers shall collect data in the Repository or information on notifications from the TSA, on a regular basis.

### **2.1.3 Obligations of Relying Parties**

When using the Time Stamp Tokens, Relying Parties shall have the following obligations with their agree to the contents described in this TPS. When using the Time Stamp Token issued by the TSA under this TPS, Relying Parties shall be responsible for the result of using digital data that is Time-Stamped and Time Stamp Tokens provided for the digital data.

- (1) Obligation to verify Time Stamp Token

When using a Time Stamp Token, Relying Parties shall verify the Time Stamp Token. The Time Stamp Token shall be verified that hash values in the Time Stamp Token are equal to those in digital data to be time-stamped, that signatures on the Time Stamp Token itself are correct, that whether a Public Key Certificate corresponding to a Private Key that provides a signature to the Time Stamp Token is revoked, and that whether the Time Stamp Token is revoked.

- (2) Compliance with restrictions on the use of Time Stamp Tokens

Time Stamp Tokens are issued under this TPS, which describes the purposes and applicable scope of Time Stamp Tokens. Relying Parties shall read this TPS thoroughly before using Time Stamp Tokens.

### **2.1.4 Obligations of Time Authority**

The TA shall have the following obligations to the TSA:

- (1) The TA shall distribute a time to the Time Stamp Unit of the TSA and conduct an audit on it at least once a day.
- (2) When the time audit on the Time Stamp Unit finds that a measured time error is within +/- 500 milliseconds against UTC, the TSA shall issue a Time Attribute Certificate valid for 25 hours to the relevant Time Stamp Unit and permit the Time Stamp Unit to issue Time Stamp Tokens during the validity period of the Time Attribute Certificate. When a measured value of the time error exceeds +/- 500 milliseconds, the TA shall take action to suspend the Time Stamp Unit's function of issuing Time Stamp Tokens.
- (3) Time synchronization accuracy of the clock used by the TA shall be maintained so that a time error against UTC does not exceed +/- 30 milliseconds. In addition, leap seconds shall be set based on notifications from the National Time Authority (NTA) and time traceability to UTC shall be maintained.
- (4) The security of the Private Key of the Time Authentication server shall be maintained; if the Private Key is compromised, the TA shall immediately file a request for revocation of the key with

the CA and notify the TSA of it.

- (5) The TA shall keep the following data in storage securely for 10 years: Time Attribute Certificates issued to the TSA; time audit logs related to the relevant time audit and issuance of Time Attribute Certificates; data to certify time traceability to UTC, including Time Attribute Certificates issued for the equipment in the TA and data generated by the TA to compare its time and UTC.

The TA shall provide the relevant data upon the TSA's request.

### **2.1.5 Obligations of Certification Authority**

In the certifying service (the service of issuing Certificates) for the TSA, the CA of the TSA shall have the following obligations to the TSA:

- (1) The CA shall issue Public Key Certificates to the TSA for issuing Time Stamp Tokens intended for the long-period storage. The validity period of the relevant certificates shall be 11 years.
- (2) The CA shall keep the Private Key of the CA in security. When the Private Key is compromised, the CA shall notify the TSA of it immediately.
- (3) The CA shall notify the TSA of the Revocation List of Public Key Certificates and other information related to issuance of Public Key Certificates. Upon a request from the TSA for the Public Key Certificate revocation, the CA shall revoke the Public Key Certificate immediately.

### **2.1.6 Repository-Related Obligations**

The TSA shall make public some of the service-related information in the repository in a method provided in Section 2.5.

## **2.2 Financial Responsibilities**

### **2.2.1 Liability for Damage**

If the acts of the TSA, intentionally or accidentally, results in damage to Subscribers, the TSA shall compensate the Subscribers for damages with the Time Stamp Tokens free of charge (upon a Subscriber's request) up to the amount of the relevant Time Stamp Tokens issued by the TSA. The TSA shall compensate for damages above only with the free-of-charge issuance of the Time Stamp Token as set forth in Section 4.9.3 and shall not indemnify the Relying Parties for the damages. However, if enforced by law, the TSA shall indemnify the Subscribers or the Relying Parties for damages caused through the negligence of the TSA, up to a ceiling of 100,000 yen, when the damages are resulted from the same cause. UNDER NO CIRCUMSTANCES SHALL TSA SHALL BE LIABLE TO SUBSCRIBERS OR TO ANY OTHER PERSON UNDER TORT, CONTRACT, OR ANY OTHER LEGAL THEORY, FOR ANY, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER ARISING FROM THE USE, PERFORMANCE OR NON-PERFORMANCE OF THE TIMESTAMP SERVICE, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF

PROFITS, LOSS OF GOODWILL, LOSS OF DATA, DEATH, OR PERSONAL INJURY, EVEN IF PFU HAS BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THESE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU.

## **2.2.2 Exception Clauses**

Notwithstanding the provisions in Section 2.2.1, the TSA shall not be liable for damages in the following cases:

- (1) The TSA has performed the Service properly in compliance with this TPS and the individual agreements for the Service.
- (2) Damage arises from negligence, whether intentionally or unintentionally; or any illegal activities of Subscribers or Relaying Parties.
- (3) Damage is attributable to Subscribers or Relaying Parties in breach of this TPS or individual service agreements.
- (4) Damage is resulted from the use of the systems of Subscribers or Relaying Parties.
- (5) Damage arises from the following causes, which are beyond the control of the TSA:
  - a) Acts of God including fires, earthquakes, eruptions, tsunamis, typhoons, and other natural disasters
  - b) Wars, riots, insurrection, rebellion, strike, civil commotions, and labor disputes
  - c) Radioactive materials, explosive substances, and environmental pollutants
  - d) Communication network failure
  - e) Other reasons beyond the control of the TSA
- (6) The suspension or termination of the Service arises from causes set forth in Section 4.5.1, 4.5.3, and 4.5.5, and Section 4.10, in this TPS.
- (7) Codes are decoded and security is broken even though the TSA has used codes/security that is indecipherable/sufficient, in view of expertise and technical standards within general entities issuing certificates.
- (8) Damage arises from the revocation of Time Stamp Tokens described in Section 4.9.2.

## **2.3 Interpretation and Enforcement**

### **2.3.1 Governing Law**

This TPS and the validity is governed by and interpreted in accordance with the laws of Japan,

### **2.3.2 Severability, Survival, and Notices**

- (1) Severability

Each provision or the application of this TPS thereof is several and if one or more provisions are declared in invalid or unenforceable for any reason and to any extent, the remaining portions of

this TPS will remain in full force and effect.

(2) Survival

Even if the Service of the TSA is terminated and this Statement is repealed, Section 2.2, 2.3, 2.7 and 2.8 of this TPS shall survive effectively.

(3) Notices

The notice from Subscribers to the TSA shall be given in writing or by e-mail, and shall be addressed to the specified address destination designated in Section 1.4. The written notice shall become effective on the date of receipt.

Under the service contract, the notice from the TSA shall be deemed to have been received by a Subscriber on the date of dispatch to the registered contact address of the Subscriber. The Subscriber shall notify the TSA of any changes made to the contact address without delay. If the TSA is not notified of such changes, the notification obligation shall be deemed to have been fulfilled upon dispatch to the registered contact address, except in cases where the TSA is not notified of any contact address.

### **2.3.3 Dispute Resolution**

The parties hereto agree that any dispute arising under or relating to this TPS shall be resolved by binding arbitration of the Tokyo District Court. If need to discuss provisions hereof or matters not described herein should arise, parties concerned shall discuss those in good faith.

## **2.4 Fees**

Fees shall be specified in the Service price list separately.

## **2.5 Disclosure and Repository**

### **2.5.1 Disclosure of TSA-Related Information**

The TSA shall make public the following information in the Repository specified in Section 2.5.4.

- (1) Time-Stamping Practical Statement (This TPS)
- (2) Information of Public Key Certificates
- (3) Notification (including revocation information of Public Key Certificates)

### **2.5.2 Revision of Public Information**

The frequency of updates of information to be made public is as follows:

- (1) Every time the Time-Stamping Practice Statement is amended
- (2) When revocation information of Public Key Certificates is obtained from the CA
- (3) When considered necessary by the person responsible for the TSA

### **2.5.3 Access Controls**

The TSA shall provide information made public in the Repository via the Internet. Particular access control shall not be used for providing such information.

### **2.5.4 Repository**

Information stipulated in Section 2.5.1 shall be made public in the Repository.

URL: <https://www.pfutsa.net/en/repository/>

## **2.6 Compliance Audit**

### **2.6.1 Frequency of Compliance Audit**

The TSA shall conduct an audit, by using an auditor, once a year on a regular basis. In addition to those regular audits, the TSA shall conduct organizational audits as necessary.

### **2.6.2 Identity / Qualification of Auditor**

The TSA shall appoint an employee of PFU, who is conversant with the operations of the audit and certification, as an auditor. The TSA shall outsource audits to an agency as necessary. The person responsible for the TSA shall appoint an auditor.

### **2.6.3 Relationship between Auditor and Auditee**

The TSA shall appoint a person who is not directly involved in operations of the TSA as an auditor to conduct a compliance audit on the TSA.

### **2.6.4 Purpose of Audit**

Audits shall be conducted mainly to confirm that the Service is practiced in compliance with this TPS, and that appropriate measures are taken against misconduct toward the TSA, inside and outside of the TSA.

### **2.6.5 Actions against Incompliance**

The TSA shall, based on the decision made by the person responsible, take corrective actions promptly for serious or urgent issues pointed out by the auditor, such as noncompliance. If the auditor points out that the clock managed by the TSA is not synchronized with that of UTC and/or the Public Key of the Time Stamp Unit is compromised, emergency measures shall be taken, the situations above being considered emergencies. The person responsible shall determine whether the operation of the Time Stamp Unit of the TSA is suspended until compliance is secured. In addition, the person responsible shall confirm that the TSA has implemented the countermeasures against the problems pointed out by

the auditor.

### **2.6.6 Report on Result of Audit**

A report on the audit results shall be submitted to the person responsible for the TSA.

## **2.7 Confidentiality**

### **2.7.1 Information Considered Confidential**

The TSA shall keep secret and confidential information, leakage of which may damage the reliability of the TSA, Subscribers, the TA, or the certification operation of the CA. The TSA shall appoint a person in charge of managing documents and media including confidential information and keep them in a safe place.

In principle, the confidential information shall not be disclosed, leaked, or used beyond the scope of the Service, unless otherwise set forth in this TPS or the Service agreement.

The confidential information shall include:

- (1) Records related to applications for the Service (regardless of whether approved or not)
- (2) Security check logs kept in storage by the TSA
- (3) Contingency plans and disaster recovery plans
- (4) Security measures for the operation of hardware and software, and for the administration of the TSA
- (5) Information for the identification of Subscribers, with which the TSA provides the Subscribers

Upon the receipt of information used for identifying Subscribers, the Subscribers shall not disclose or leak the information provided by the TSA.

### **2.7.2 Information Not Considered Confidential**

Notwithstanding the provision of Section 2.7.1, the following information shall not be considered confidential:

- (1) Information explicitly made public such as the Public Key Certificate, revocation information, and this TPS
- (2) Information already known at the time of disclosure other than through an act or mission attributable to the non-disclosing party
- (3) Information publicly known after the disclosure other than through an act or mission attributable to the non-disclosing party
- (4) Information disclosed legally to the recipient from a third party without confidentiality obligations
- (5) Information developed independently by the recipient, without using the information disclosed
- (6) Information disclosed to a third party from a disclosing party without confidentiality obligations

### **2.7.3 Disclosure of Revocation Information of Public Key Certificates**

The revocation information of Public Key Certificates of the TSA shall be made public in the Public Key Certificate Revocation list of the relevant CA that issues the Public Key Certificates.

### **2.7.4 Disclosure to Law Enforcement Officials**

When Law Enforcement Officials request the disclosure of information managed by the TSA (including the confidential information) based on legal grounds, the TSA shall disclose the relevant information to the Officials under the provision of the Law.

### **2.7.5 Information Disclosure by Other Reasons**

When part of the Service is entrusted to a third party, some confidential Information may be disclosed to the third party. If this is the case, the TSA shall make it obligatory for the third party to observe the confidentiality in the consignment contract.

## **2.8 Intellectual Property Rights**

The patents, model utility rights (including the rights to receive the registration), trademarks, copyrights, proprietary and intellectual property right (hereafter collectively referred to as "Intellectual Property Rights") relating to documentation, data, and programs created by the TSA, including those defined in the following, belong to the Licensor and shall not be transferred to Subscribers or others.

- (1) Time Stamp Tokens issued by the TSA
- (2) Time Stamp Token verification software provided by the TSA
- (3) This TPS

The Intellectual Property Rights of Time Attribute Certificates attached to Time Stamp Tokens shall belong to the TA, and those rights shall not be transferred to Subscribers or others.

## **2.9 Handling of Private Information**

The TSA shall not use private information provided by Subscribers at the time of the service contract beyond the scope defined in the following. In addition, the TSA shall protect private Information as described below unless otherwise stipulated in the Law.

- (1) Handling of private information in hand

The TSA shall handle information that can be used to identify individuals, such as the personal name, telephone number, and place of work, which is provided by Subscribers as private information.

- (2) Purpose of use of private information

The TSA shall use private information to provide Subscribers with the Service. In addition, the TSA may use private information to inform Subscribers of the Service-related commercial products of its own or the

subsidiaries', if otherwise agreed.

(3) Restrictions on the use of private information

The TSA shall use private information only for purposes stipulated in Section 2.9 (2).

(4) Provision providing for the purpose of use of private information

The TSA shall describe the purpose of use of private information in this TPS to make it public.

(5) Security of integrity of private information

Based on requests from Subscribers, the TSA shall manage private information so that the integrity of information is secured.

(6) Security Management Measures

The TSA shall take reasonable security measures to protect private information from unauthorized access, loss, destruction, tampering, and leakage. When the TSA entrusts the management of private information to a third party, the TSA shall exercise supervision and control over the third party as appropriate so that the third party manages the relevant private information securely.

(7) Disclosure and Correction

When a Subscriber requests the disclosure, correction, or deletion of private information of the Subscriber, the TSA shall perform those above to the extent reasonable.

## **3. Identification and Authentication**

### **3.1 Initial Registration**

#### **3.1.1 Type of Names**

The name of the subject of a Public Key Certificate for the Time Stamp Unit shall be provided in the format of X.500 Distinguished Name (DN) by the CA.

#### **3.1.2 Meaning of Names**

The unique name of the Time Stamp Unit described in the Time Stamp Token, which is issued by the TSA, shall be the name described in the Public Key Certificate for the Time Stamp Unit, which is issued by the CA.

#### **3.1.3 Uniqueness of Names**

The unique name of the Time Stamp Unit described in the Time Stamp Token, which is issued by the TSA, shall be given by the CA and shall be unique to each Time Stamp Unit.

### **3.2 Applicant Authentication for Service**

The TSA shall confirm the authenticity of applicants for the Service to the extent rational, only if the private information of applicants is submitted upon applications, and approve the use of the Service.

If the private information of applicants is not submitted upon applications, the TSA does not confirm.

### **3.3 Renewal of the Service Contract**

When the service contract is renewed, identification and authentication shall be performed based on the procedure provided in Section 3.2.

### **3.4 Termination of the Service Contract**

When the service contract is terminated, identification and authentication shall be performed based on the procedure provided in Section 3.2.

## **4. Operational Requirements**

### **4.1 Application for Use of the Service**

Any parties who apply for the Service shall enter into an agreement relating to the use of the Service provided by the TSA.

Prior to entering into the relevant agreement, the TSA shall process the applications for the Service, only if the private information of applicants is submitted upon applications to the TSA. If the TSA determines that it is appropriate to provide the Service for the applicants, it shall enter into the agreement for the Service contract and provide information for the identification of Subscribers (applicants) to the Service.

If a party intervenes application for the Service on behalf of applicants, the TSA shall screen the intervening party. If the TSA determines that it is appropriate to provide the Service for the applicants, it shall approve the application for the Service contract from the party, conclude the contract between the TSA and the party, and providing the party the information to use the Service for the identification of Subscribers. In this case, the applicants can use the Service after entering into an agreement to use the Service between the applicants and the party.

### **4.2 Time Stamp Request**

The Subscriber of the Service shall send a Time Stamp request, which includes the hash value of digital data to be Time-Stamped, to the TSA. The communication methods and detailed procedures for Time Stamp requests shall be determined separately.

The Subscriber of the Service shall not make the Time Stamp requests for other purposes than the issuance of Time-Stamps.

### **4.3 Issuance of Time Stamp Token**

Receiving a Time Stamp request from a Subscriber, the TSA shall return the status of the response to the request; accepted, rejected, or else. When the Time Stamp request is properly accepted, the TSA shall generate a Time Stamp Token defined in Section 1.3.2 using any Time Stamp Unit managed by the TSA, and issue it to the Subscriber. As for communication methods and Time Stamp Token issuance procedures used between the Time Stamp Unit and Subscribers, the TSA shall disclose them to Subscribers at no charge, provided that Subscribers sign the Non-Disclosure Agreement.

### **4.4 Verification of Time Stamp Token**

Parties who receive a Time Stamp Token shall verify the Time Stamp Token by using the following methods:

- (1) By comparing the hash value of Time-Stamped digital data with that of a Time Stamp Token, verify that

the Time-Stamped digital data corresponds to the Time Stamp Token, and that the time-stamped digital data is not tampered.

- (2) By using the Public Key Certificate included in a Time Stamp Token, verify the digital signature of the TSA to confirm that the Time Stamp Token is not tampered.
- (3) By verifying the Public Key chain, which is included in a Time Stamp Token, and which includes the CA's certificate, verify the Public Key Certificate is valid.

## **4.5 The Service Suspension and Termination**

### **4.5.1 Suspension of the Service**

In the event of any of the following, the TSA may suspend the Service without prior notice.

- (1) The suspension of the Service is inevitable because of accidents such as a fire, power failure, or illegal access.
- (2) The suspension of the Service is inevitable because of the improvement of operation, or security management. However, the TSA shall notify Subscribers of a suspension due to a regular inspection and maintenance (including inspections and maintenance conducted by the TA or the CA) or the setup of leap seconds described in Section 4.11, no later than one week before the suspension, and such a suspension shall be made public in the website accessible at the URL: <http://www.pfutsa.net/en/>

However, if the TSA is not notified of the contact address, the TSA shall not be responsible to notify the suspension to Subscribers.

- (3) The TA or the CA suspends or terminates the Service, and the TSA determines to suspend the Service.
- (4) A serious malfunction in the system configuration and/or a critical failure related to the system has occurred, and a possibility of spreading damage arises if the Service is continued.
- (5) Any events that may result in serious damage on the whole system of the Service, such as leakage, forgery, or corruption of the Private Key of the TSA.

### **4.5.2 Cancellation of Suspension of the Service**

When causes of the suspension of the Service are eliminated, the TSA shall cancel the suspension of the Service after confirming, by using the predetermined procedures, that the causes are eliminated.

### **4.5.3 Suspension of the Service to Subscribers**

In the event of either of the following, the TSA may suspend the Service to the relevant Subscriber without prior notice:

- (1) Default of obligations by a Subscriber
- (2) Request for the suspension of the Service by a Subscriber

#### **4.5.4 Cancellation of Suspension of the Service to Subscribers**

If causes of the suspension of the Service are eliminated at the relevant Subscriber, the TSA shall cancel the suspension after confirming, by using the predetermined procedures, that the causes are eliminated.

#### **4.5.5 Revocation of the Service**

In the event of any of the following event, the TSA may terminate the Service to the relevant Subscriber:

- (1) When a Subscriber submits the application for the cancellation of the contract.
- (2) When a Subscriber breaches or defaults the performance of any of the provisions of this TPS and such breach or default is not cured within a reasonable period
- (3) When the TSA terminates the Service
- (4) When any of the following occurs to a Subscriber:
  - a) The clearinghouse publicize that the checks of the Subscriber bounces and financial institutions suspend business transactions.
  - b) The supervisory authority orders the Subscriber to terminate or suspend its business.
  - c) A third party files a petition for provisional attachment or disposition, or forcible execution against the Subscriber, and there is a fact that it is difficult for the Subscriber to perform the provisions of this TPS.
  - d) A petition of bankruptcy or that of commencement of procedures such as liquidation, special liquidation, rejuvenation, or corporate reorganization procedures in accordance with the Commercial Law is filed.
  - e) The dissolution, consolidation, or assignation of the whole or an important part of business is resolved.
  - f) The financial situations of the Subscriber are deteriorated or causes of such deterioration are recognized.
  - g) The Subscriber practically falls under the control of a third party, which may well damage the TSA.

### **4.6 Security Inspection Procedure**

The TSA shall record information related to the Service and inspect it on a regular basis in order to maintain the security and reliability of its system.

#### **4.6.1 Information to be Recorded in Security Inspection Log**

Information to be recorded in the security inspection log shall be that of important events related to the system security of the TSA. The recording of the following is compulsory:

- (1) Issuance records of Time Stamp Tokens (or copies of issued Time Stamp Tokens)
- (2) Records of Time Audits conducted by the TA (or copies of Time Attribute Certificates)
- (3) Records of all processes from the conclusion of the service contract with Subscribers and the commencement of use of the Service to the termination of the contract and the Service
- (4) Records of generation and revocation of Key Pairs used in the TSA
- (5) Records and permits of the comings and goings (to/from the facilities of the TSA)
- (6) Records of operations performed in the TSA system
- (7) Records of malfunctions in the TSA system
- (8) Records of unauthorized accesses to the TSA system

#### **4.6.2 Inspection Frequency of Security Inspection Log**

The TSA shall inspect security inspection logs at least once a month.

#### **4.6.3 Protection of Security Inspection Log**

The TSA shall protect security inspection logs from tampering, deletion, and outflow according to the predetermined methods and procedures.

#### **4.6.4 Procedure for Storage of Security Inspection Log**

The TSA shall store security inspection logs according to the predetermined methods and procedures.

#### **4.6.5 Collection of the Security Inspection Log**

The TSA shall collect data of important events relating to security and keep records in security inspection logs on a regular basis.

#### **4.6.6 Assessment of Vulnerability**

The TSA shall assess the security vulnerability with respect to the operation and system of TSA. If any problem is detected in security mechanisms, the problem is reported to a person in charge of the TSA. If the problem is identified in the course of the reevaluation, corrective action shall be taken.

### **4.7 Archive**

#### **4.7.1 Type of Archive**

Archive data shall be stored as described below. The numbers in parentheses represent the archival storage period of each.

- (1) Audit reports (15 years)
- (2) Issuance records of Time Stamp Tokens (or copies of issued Time Stamp Tokens) (15 years)
- (3) Records of Time Audits conducted by the TA (or copies of Time Attribute Certificates) (15 years)

- (4) Records of all processes from the conclusion of the service contract with Subscribers and the commencement of use of the Service to the termination of the contract and the Service (15 years)
- (5) Records of generation and invalidation of Key Pairs used in the TSA (15 years)
- (6) Records and permits of the comings and goings (to/from the facilities of the TSA) (3 years)
- (7) Records of operations performed in the TSA system (3 years)
- (8) Records of malfunctions in the TSA system (3 years)
- (9) Records of unauthorized accesses to the TSA system.(3 years)

#### **4.7.2 Protection of Archived Data**

Archive data shall be protected from tampering, deletion, and outflow according to the predetermined processes and procedures. It shall also be kept in a magnetic-free environment at an appropriate temperature and humidity.

#### **4.7.3 Archive Retention**

Archive data shall be maintained in accessible state during the archival storage period.

### **4.8 Key Renewal**

The TSA shall renew a key pair 10 years before the expiration of Public Key Certificate, and revoke the previous Private Key securely according to the predetermined procedures. However, the TSA shall not request the revocation of Public Key Certificates.

### **4.9 Recovery from Compromise and Disaster**

#### **4.9.1 Actions for Destruction of Hardware, Software, or Data**

If hardware, software, and/or data is destroyed, they shall be immediately recovered by using backups of hardware, software, and data.

#### **4.9.2 Requirements of Revocation of Time Stamp Token**

If the Private Key of the Time Authentication server of the CA or the TA, or that of the Time Stamp Unit of the TSA is compromised, the CA shall revoke the Public Key Certificate of the relevant Private Key (it is posted in the Revocation List of the CA), and all Time Stamp Tokens issued by using the said Private Key shall at once be revoked. If an incorrect Public Key Certificate is issued by the CA to the TSA, and if a Time Stamp Token is issued with an incorrect Public Key Certificate attached, all Time Stamp Tokens shall at once be revoked when those are found to be incorrect.

### **4.9.3 Conditions for Free Issuance of Time Stamp Token**

If Time Stamp Tokens are revoked according to the previous Section, the TSA shall issue Time Stamp Tokens with limits of no more than the number of the relevant Time Stamp Tokens, without charge, upon Subscribers' requests only in the following cases. However, if the Private Key algorithm of the CA, TA, or TSA is compromised, the relevant Time Stamp Tokens shall not be issued without charge.

- (1) In the cases where the TSA's Private Key is compromised, except for the case described in Section 2.2.2 (7)
- (2) In the cases where the TSA received an incorrect Time Attribute Certificate of the TA
- (3) In the cases where the TSA issued a Time Stamp Token using an incorrect Public Key Certificate

### **4.9.4 Private Key Compromise Control**

When the Private Key of the Time Stamp Unit is compromised, the TSA shall suspend the Service and do the following:

- (1) Submit the application for the revocation of Public Key Certificates of the Time Stamp Unit to the CA;
- (2) Submit the application for destruction and re-generation of the Private Key of the Time Stamp Unit;
- (3) Submit the application for issuance of the Public Key Certificate for the new key of the Time Stamp Unit;
- (4) Notify Subscribers of a compromise of the Private Key.

### **4.9.5 Restoration of Facilities at Disasters**

If the facilities of the TSA are damaged by a disaster, the TSA shall restore them using spare machines and backup data.

## **4.10 Termination of the Service**

- (1) The TSA may terminate the Service in case of any one of the following:
  - a) A malfunction of the system components and/or serious failure related to the system occurs, and the extent of damage may increase if the Service is continued to be provided;
  - b) An event that causes serious damage to the whole system of the Service, such as a leakage, forgery, or compromise of the Private Key of the TSA, occurs;
  - c) The services of the TA or the CA are suspended or terminated, and it becomes difficult for the TSA to continue the Service;
  - d) In addition to the above, the TSA determines that the Service should be terminated for some reasons;
- (2) When the termination of the Service is determined, Subscribers and Relying Parties shall be notified of the Service termination, the revocation date of the Public Key Certificate of the Time Stamp Unit, and the

organization in which the backup and archive data of the TSA is kept in storage and the disclosure method of the said data, no later than 60 days, in principle, before the termination of the Service.

- (3) The TSA shall securely destroy all the Private Keys of the Time Stamp Unit immediately after the termination of the Service.
- (4) The TSA shall delete all the private information immediately after the termination of the Service.

#### **4.11 Time Synchronization with UTC**

- (1) Time synchronization Control

By using the "SecureNTP Time Certificate Service" provided by the TA, the TSA shall control the clock of all Time Stamp Units so that the time of the clock is synchronized with UTC at a predetermined accuracy.

- (2) Setup of Leap seconds

By using the "SecureNTP Time Certificate Service" provided by the TA, the TSA shall set up leap seconds for all Time Stamp Units.

#### **4.12 Time Traceability**

- (1) The TSA shall use time distributed by the TA as the time source of the TSA and keep the records of Time Audits conducted by the TA so as to secure the traceability of the time used for Time-Stamping.
- (2) The TA shall secure the time traceability to UTC by comparing its time with a time distributed based on the Service Practice Statement provided by the National Time Authority, and by keeping the data in storage.

## **5. Physical, Procedural, and Personnel Security Management**

### **5.1 Physical Management**

#### **5.1.1 Location and Structure**

The facilities of the TSA shall be built in areas not damaged easily by floods, earthquakes, fires, and other disasters, and quakeproofing, fireproofing, and intrusion-prevention measures shall be implemented on the structure. In addition, equipment shall be installed in a safe place kept from disasters and intrusion.

No signs indicating of the TSA shall be posted at the entrance of the building, floor, and room used for the TSA.

#### **5.1.2 Physical Access**

The TSA shall limit accesses to each room of the TSA to authorized personnel. Persons for whom access to each room and equipment is authorized shall be defined. Persons other than those authorized shall follow predetermined procedures to access to rooms and equipment.

The TSA facilities shall be monitored by guards with a monitoring system for 24 hours 7 days a week.

#### **5.1.3 Power and Air Conditioning**

The important devices of the TSA shall be connected to an uninterruptible power supply (UPS) in case of power failures. If a power failure lasts for hours, power shall be provided from the private electric generator within a certain period. The TSA shall equip the facility with the air conditioner to maintain an adequate operating environment for the devices and working environment for the personnel.

#### **5.1.4 Flood-Control Measures**

A building and a room of the building used for the TSA shall be equipped with hydrostats and have the waterproofed ceiling and floor.

#### **5.1.5 Anti-earthquake Measures**

The building used for the TSA shall be earthquake-proof, and measures shall be taken to prevent all equipment and appliances from toppling over and falling down.

#### **5.1.6 Anti-Fire Measures**

The building used for the TSA shall be fireproof; and the room shall be compartmented and equipped with fire extinguishers or the like.

### **5.1.7 Media Storage**

Media containing archive and backup data shall be stored in a cabinet that can be locked in a room for which the comings and goings of personnel are well monitored, and monitoring of the comings and goings shall be conducted according to the predetermined procedures.

### **5.1.8 Material Disposal**

Documents and media containing confidential information shall be disposed in an appropriate manner according to the predetermined procedures.

### **5.1.9 Off-Site Backup**

Backup copies of media containing important data shall be stored in a different location away from the TSA in a secure manner according to the predetermined procedures.

## **5.2 Procedure Management**

For the implementation of important services such as the startup and termination of the Time Stamp Unit as well as the generation of the Time Stamp Unit key, trusted personnel shall be appointed.

In order for an operator to operate the system, the system shall identify and certify the operator as an authorized person. Critical operations such as generation and renewal of the Time Stamp Unit key shall be performed in the presence of more than one person.

When the TSA entrusts the Service to an agency, the TSA shall maintain physical, procedural, and personnel security in accordance with provisions in this chapter by obligating the agency to comply with those provisions and operate the Time Stamp Unit according to detailed procedure manuals that the TSA shall provide

## **5.3 Personnel Management**

### **5.3.1 Background, Qualification, Experience, and Prerequisite Conditions**

The TSA shall verify personnel's eligibility to provide the Service prior to assignment and allocation of the personnel. The personnel's eligibility shall be verified based on the résumé and personal information held by the Human Resource Department of the TSA; the personal information includes, criminal records, careers (e.g. qualifications), business experiences, and expertise required for fulfilling job responsibilities.

### **5.3.2 Training Requirements**

The TSA shall provide its personnel who perform the Service with training in accordance with educational programs defined separately.

### **5.3.3 Retraining Frequency and Requirements**

The TSA shall provide its personnel who perform the Service with training regularly in accordance with the educational programs other than the initial training.

### **5.3.4 Sanctions for Unauthorized Actions**

Appropriate disciplinary actions shall be issued in accordance with working regulations, other related rules, or employment agreements, against personnel who commit, intentional or accidental, unauthorized actions or other violations of this TPS, practical rules, manuals, or procedures related to the Service.

### **5.3.5 Documentation Supplied to Personnel**

The following documents are provided to the personnel who perform the Service if necessary for performing their duties.

- (1) Manuals of facilities and devices of the TSA
- (2) Practice statements and procedure manuals related to operation of the TSA.

## **6. Technical Security Management**

### **6.1 Key Pair Generation and Installation**

#### **6.1.1 Key Pair Generation**

The Key pair of the Time Stamp Unit shall be generated by using the cryptographic module (HSM) in the presence of persons concerned.

#### **6.1.2 Time Stamp Unit Public Key Registration with Certification Authority**

The Public Key of the Time Stamp Unit shall be registered with the CA by using predetermined procedures to receive the Public Key Certificate.

#### **6.1.3 Receipt of Route Certificate from Certification Authority**

The TSA shall store route certificates received from the CA and mid-certificates necessary for verifying those certificates from Public Key certificates of the Time Stamp Unit to the relevant route certificates, securely and reliably.

#### **6.1.4 Receipt of Route Certificate for Public Key Certificate of Time Authority**

The TSA shall store route certificates of the CA used for certifying the Public Key of the Time Authentication server, which is received from the TA, securely and reliably.

#### **6.1.5 Key Size**

RSA 2048-bit keys shall be used as the key of the Time Stamp Unit.

#### **6.1.6 Hardware / Software for Key Generation**

The Time Stamp Unit shall use a cryptographic module that satisfies the standards defined in 6.2.1.

#### **6.1.7 Purpose of Use of Key**

The Time Stamp Unit key shall be used for digital signatures applied to the Time Stamp Token issued by the TSA.

### **6.2 Private Key Protection**

#### **6.2.1 Standards for Cryptographic Modules**

The Time Stamp Unit key shall be generated and stored by using the cryptographic module (HSM) certified as FIPS (Federal information processing standard) 140-2 Level 3 or higher.

### **6.2.2 Private Key Multi-Personnel Management**

The Private Key of the Time Stamp Unit shall be generated, activated, and revoked under administration of more than one person.

### **6.2.3 Private Key Escrow**

A Private Key escrow shall not be used.

### **6.2.4 Private Key Backup**

Private Key backup shall not be conducted.

### **6.2.5 Private Key Archival**

The Private Key shall not be archived.

### **6.2.6 Private Key Entry into Cryptographic Module**

The Private Key of the Time Stamp Unit shall be generated and stored in the cryptographic module (HSM).

### **6.2.7 Method of Activating Private Key**

The Private Key of the Time Stamp Unit shall be activated by entering the activation data in the cryptographic module under administration of more than one person.

### **6.2.8 Method of Deactivating Private Key**

The Private Key of the Time Stamp Unit shall be deactivated by performing predetermined operations on the cryptographic module (HSM) under administration of more than one person.

### **6.2.9 Method of Destroying Private Key**

The Private Key of the Time Stamp Unit in the cryptographic module (HSM) shall be destroyed according to predetermined procedures under administration of more than one person.

## **6.3 Validity Period of Public Key and Private Key**

The validity period of the Public Key Certificate for the Time Stamp Unit shall be 11 years on and after the commencement date.

The active period (duration of use) of the Private Key shall expire 10 years before the expiration date of the Public Key Certificate and the key pair shall be replaced before the expiration of the active period. However, if the Private Key is compromised or the possibilities of compromise arise, the key shall be subject to a revocation and shall be renewed before the expiration date.

## **6.4 Activation Data**

### **6.4.1 Activation Data Generation and Installation**

Activation data for the Private Key of the Time Stamp Unit shall be generated and installed according to the predetermined procedures.

### **6.4.2 Activation Data Protection**

Activation data used in the TSA, including the one for the Private Key of the Time Stamp Unit, shall be protected and managed according to the predetermined rules.

## **6.5 Computer Security**

The TSA shall establish computer security standards and confirm that these standards are complied with at the time of installing computer devices and hardware/software of time-related equipment.

## **6.6 Network Security**

The TSA shall establish network security standards and confirm that these standards are complied with at the time of installing and operating the system.

## **6.7 Cryptographic Module Engineering Management**

Cryptographic Module Engineering Management shall be defined in Section 6.1.1 and 6.2.1.

## **7. Management of Time-Stamping Service Practice Statement**

### **7.1 Modification of TPS**

The TSA shall modify this TPS if necessary according to the predetermined procedures.

### **7.2 Publication and Notification Policies of TPS**

When this TPS is modified, the TSA shall make public the modified Statement, clearly stating the date on which the revision becomes effective.

The notification shall be given to the Subscribers to the Service by sending postal mail or e-mail to the registered addresses, and to the Relying Party by posting this TPS in the Repository.

## 8. Time Stamp Token Profile

(Time Stamp Token)

ContentType	
ContentType	Content type Type: OID Value: 1 2 840 113549 1 7 2 (pkcs7-signedData)
Content	
SignedData	
version	CMS version Type: INTEGER Value: 3
digestAlgorithms	Hash algorithm information used by the signer
DigestAlgorithmIdentifier	
algorithm	Hash algorithm object ID Type: OID Value: 2 16 840 1 101 3 4 2 3 (SHA-512)
parameters	Cryptographic algorithm argument Type: NULL Value: None
encapContentInfo	Contents information to be signed
eContentType	Content type Object ID Type: OID Value: 1 2 840 113549 1 9 16 1 4 (id-smime-ct-TSTInfo)
eContent	Contents (Signature target data = TSTInfo) Type: OCTET STRING Value: der-encoded TSTInfo
certificates	Certificate chain
certificate	Public Key Certificate of the TSA (* Refer to CPS of CA)
attrCert	Time Attribute Certificate of TA (*Refer to TPS of TA)
signerInfos	Signer information

signerInfo	
version	<p>CMS version</p> <p>Type: INTEGER</p> <p>Value: 1</p>
sid	<p>Signer ID</p>
issuer	<p>Certificate issuer name (* It conforms to the Public Key Certificate)</p>
serialNumber	<p>Certificate Serial number</p> <p>Type: INTEGER</p> <p>Value: Unique integer</p>
digestAlgorithm	<p>Hash function algorithm used by the signer</p>
algorithm	<p>Hash algorithm object ID</p> <p>Type: OID</p> <p>Value: 2 16 840 1 101 3 4 2 3 (SHA-512)</p>
parameters	<p>Cryptographic algorithm argument</p> <p>Type: NULL</p> <p>Value: None</p>
signedAttrs	<p>Signature Attribute</p>
Attribute	<p>Attribute</p>
attrType	<p>Attribute type</p> <p>Type: Object ID</p> <p>Value: 1 2 840 113549 1 9 3 (ContentType)</p>
attrValues	<p>Attribute value</p>
AttributeValue	<p>Attribute value</p> <p>Type: Object ID</p> <p>Value: 1 2 840 113549 1 9 16 1 4 (id-smime-ct-TSTInfo)</p>
Attribute	<p>Attribute</p>
attrType	<p>Attribute type</p> <p>Type: Object ID</p> <p>Value: 1 2 840 113549 1 9 4 (messageDigest)</p>

attrValues	
AttributeValue	Attribute type Type: OCTET STRING Value: Contents hash value
Attribute	Attribute
attrType	Attribute type Type: Object ID Value: 1 2 840 113549 1 9 16 2 12 (id-aa-signingCertificate)
attrValues	
SigningCertificate	Certificate signature
certs	Certificate
ESSCertID	Certificate identifier
certHash	Public Key Certificate hash value Type: OCTET STRING Value: Public Key Certificate hash value
issueSerial	Issuer name and serial number
issure	Issuer's name of Public Key Certificate (*In accordance with the Public Key Certificate)
serialNumber	Public Key Certificate serial number Type: INTEGER Value: Unique integer
ESSCertID	Certificate identifier
certHash	Time Attribute Certificate hash value Type: OCTET STRING Value: Time Attribute Certificate hash value
signatureAlgorithm	Algorithm used for signature
algorithm	Signature hash algorithm object ID Type: OID Value: 1 2 840 113549 1 1 13 (SHA-512 with RSA Encryption)

parameters	Signature hash algorithm argument Type: NULL Value: None
signature	Signature value Type: OCTET STRING Value: Signature value

(TSTInfo)

version	
version	Version of Time Stamp Protocol Type: INTEGER Value: 1
policy	
TSAPolicyId	TSA Policy Object ID Type: OID Value: 0 2 440 200185 1 2 2
MessageImprint	
MessageImprint	Hash algorithm and hash value of data subjected to Time-Stamping
hashAlgorithm	Hash algorithm
AlgorithmIdentifier	Hash algorithm object ID
algorithm	Type: OID Value: 2 16 840 1 101 3 4 2 3 (SHA-512)
parameters	Cryptographic algorithm argument Type: NULL Value: None
hashedMessage	Hash Value Type: OCTET STRING Value: Hash value
SerialNumber	
serialNumber	Time Stamp Token Serial number Type: INTEGER Value: Unique integer

GenTime	
GenTime	Time at which Time Stamp Token is issued Type: GeneralizedTime Value: YYYYMMDDhhmmss[.sssss]Z
Accuracy	
Accuracy  millis	Time Stamp Time Accuracy  Time accuracy (ms) Type: INTEGER Value: millisecond
Ordering	
Ordering	Ordering in time accuracy Type: BOOLEAN Value: FALSE
Nonce	
nonce	Nonce (random numbers) Type: INTEGER Value: Random numbers
Tsa	
GeneralName directoryName	TSA identification information Public Key Certificate owner's DN (* It conforms to Public Key Certificate)
Extensions	
extensions	Extended area Not to be used

## Appendix: Abbreviations and Definitions

Abbreviation/Term	Description
CA	Certification authority
PKC	Public Key certificate
PKI	Public Key infrastructure
NIST	National Institute of Standards and Technology
RSA	One of Public Key cryptosystems taking advantage of a characteristic of prime factorization; that is, it is difficult to factorize a number with a large number of digits
SHA-1, SHA-512	One of hash algorithms. It is used as the standard hash algorithm or Secure Hash Standard (SHS) by the U.S. Government by NIST
TSA	Time Stamp authority
TSU	Time Stamp unit
TST	Time Stamp Token
TA	Time authority
UTC	Coordinated universal time
X.509	ITU-T Advice specifying a standard format of digital certificate necessary for Public Key Infrastructure. It is international standardized as ISO/IEC9594-8
Coordinated universal time (UTC)	The time coordinated with "leap second" in order to keep the deviation between the international atomic time (TAI) and the world time based on the rotation of the Earth becoming no less than 0.9 second
Public Key Certificate (PKC)	Public Key Certificate specified in ITU/ISO X.509. A certificate that the Public Key matches the Private Key of the owner
International Atomic Time (TAI)	TAI began at midnight GMT (Greenwich mean time) on the first day of 1958
Time Attribute Certificate (TAC)	A time-related certificate issued by a TA when a time audit is conducted on a customer's devices (such as Time Stamp Unit) by the TA
Time Authority (TA)	An organization that provides the certificate services related to the time. It distributes the standard time for the Time Stamp Unit and provides time-audit services on the time used by the TSA
Time Stamp Authority (TSA)	A trusted third party that issues Time Stamp Tokens based on PKI technology
Time Stamp Unit (TSU)	A server that issues Time Stamp Tokens that conforms to the RFC3161 Time Stamp protocol
Time Stamp Token (TST)	Digital information digital-signed by the Time Stamp Authority (TSA) based on the

	system complying with RFC3161
Certification Authority (CA)	An organization that issues Public Key Certificate in PKI
Japan Standard Time (JST)	The Japan standard time managed and sent by an independent administrative institution, National Institute of Communication Technology (NICT)  The Japan standard time is 9 hours ahead of UTC
Repository	A system to store the related information necessary for verification of Time Stamp Token