fair[&]smart Time-Stamp Policy

Document identification

OID : **1.3.6.1.4.1.52568.1.1.2**

Version : **2.0**

Effective Date : **2019-03-08**

Document Name : **FairAndSmart - Time-Stamp Policy - v2**

Document history

Date	Version	Autor	Changes
2018-03-02	1.0	JBL	initial version / OID=1
2019-02-22	2.0	NRU	new CA / OID=2

1. Introduction

fair[&]smart is a company dedicated to the service delivery of secured data exchange platform. To this end the development of the “fair[&]smart Time-Stamp Authority” (hereinafter TSA) whose activity operates mandated by the present document.

2. Present document scope and area of application

This document is the application for all the interveners in the service of time stamp issued by the TSA and by third parties who accept the issued time-stamp. All must know and accept the content of the present document of policies and practices in order to establish reliance in the time stamp services provided by the TSA and adapt their actions willingly.

This is also a reference document to third party entities and independent organizations that need to verify or certify that the TSA acts are compatible with the policies and practices here described.

3. References

This Time-Stamp Policy meets the following requirements :

- General Policy Requirements for Trust Service Providers: ETSI EN 319 401 V1.1.1
- Policy requirements for time-stamping authorities: ETSI TS 102 023 V1.2.2
- Policy and Security Requirements for Trust Service Providers issuing Time-Stamps: ETSI EN 319 421 V1.1.1
- Time stamping profile: ETSI TS 101 861 V1.4.1
- Cryptographic Suites: ETSI TS 119 312 V1.1.1
- Internet X.509 Public Key Infrastructure TimeStamp Protocol (TSP): RFC 3161
- Policy Requirements for Time-Stamping Authorities (TSAs): RFC 3628

4. Definitions and abbreviations

4.1. Definitions

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

- Relying Party: A Party relying on a time-stamp provided by the fair[&]smart TSA.
- Subscriber: Individuals or organisations using the time-stamp services provided by a TSA and agreeing explicitly to its terms and conditions.

- TSA Disclosure Statement: Policies and practices of a TSA that require particular emphasis or disclosure to subscribers and relying parties.
- TSA Practice Statement: Statement of the practices that a TSA employs in issuing timestamp tokens.
- TSA system: composition of IT products and components organized to support the provision of time-stamping services.
- Time-stamping authority: Authority which issues time-stamp tokens.
- Time-stamp policy: Rules applied by the TSA, when generating a time-stamp token.
- Time-stamp token: Data object that binds the existence of digital data to a particular time. This serves as positive proof that certain data existed at this particular time.
- Time-stamping unit: Hardware and software components which are managed as a unit to provide time-stamp tokens from a single time source.

4.2. Abbreviations

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

- CA: Certification Authority
- CPS: Certification Practice Statement
- CRL: Certificate revocation list
- CSR: Certificate Signature Request
- ETSI: European Telecommunications Standards Institute
- OCSP: Online Certificate Status Protocol
- OID: Object Identifier
- PKCS: Public Key Cryptographic Standards
- PKI: Public Key Infrastructure
- RSA: Rivest Shamir Adleman
- TSA: Time-stamping Authority
- TST : Time-stamp Token
- TSU: Time-stamping Unit
- URL: Uniform Resource Locator

4.3. Subscriber

fair[&]smart is the only subscriber authorized to use this TSA.

4.4. Time-Stamp Policy and TSA Practice Statement

This section explains the relative roles of Time-stamp policy and TSA practice statement. It places no restriction on the form of a time-stamp policy or practice statement specification.

The time-stamp policy states "what is to be adhered to," while a TSA practice statement states "how it is adhered to", i.e., the processes it will use in creating time-stamps and maintaining the accuracy of its clock.

The present document specifies a time-stamp policy to meet general requirements for trusted time-stamping services. The TSA practice statements explain how these requirements are met.

5. General concepts

5.1. Time-stamp Service

The TSA time stamp service provides third parties with software systems. The technological mechanism demonstrates the existence of digital content during a particular time. TSA achieves this by signing the digital content at the time of certification.

The signature used is a digital signature named “time-stamp” and includes the date and time obtained from a reliable source at the time of the signature.

The provision of time-stamping services is broken down into the following component services for the purposes of classifying requirements:

- Time-stamping provision: This service component generates time-stamp tokens.
- Time-stamping management: The service component that monitors and controls the operation of the time-stamping services to ensure that the service is provided as specified by the TSA. This service component is responsibile for the installation and de-installation of the time-stamping provision service. For example, time-stamping management ensures that the clock used for time-stamping is correctly synchronized with UTC.

This subdivision of services is only for the purposes of clarifying the requirements specified in the current document and places no restrictions on any subdivision of an implementation of time-stamping services.

5.2. Time Stamp Authority

fair[&]smart TSA issues secure time-stamp tokens (TST) for users of fair[&]smart services.

fair[&]smart TSA assumes the overall responsibility for the provision of the time-stamping services.

fair[&]smart TSA is identified in the digital certificate used for the time-stamping services.

5.3. Documents identification

The OID of fair[&]smart are structured as follows :

- positions 1 to 7 : 1.3.6.1.4.1, the IANA OID pool,
- position 7 : 52568, issued by the IANA for fair[&]smart,
- position 8 : 1, timestamping-related operations,
- position 9 : 1 for this document,
- position 10 : the version of this document.

5.4. Standards compliance

fair[&]smart provides the service of time-stamp according to the regulation standards in each of the following areas:

- Service policies and practices: ETSI TS 102 023 (2008)-Electronic Signatures and Infrastructures (ESI) – Policy Requirements for Time-stamping Authorities.
- Definition of the services of time-stamp: RFC 3161, Internet X.509 Public Key Infrastructures Time-Stamp Protocol (TSP)

This document determines the general rules of TSA operations, without pretending or being its purpose to include detailed technical specifications regarding the infrastructure sub-systems, networks & communications, organizational, operating procedures, measures and security controls.

The time-stamps submitted in each moment by the TSA are subject to the policy and practices, which are gathered in this document version and are in force at such moment. Each version must be considered applicable during its life span.

6. Time-Stamp policy

6.1. Overview

This TSA policy comprises a set of rules and processes to be used for issuing trustworthy time-stamp tokens in accordance ETSI EN 319 421.

6.2. Identification

The OID (Object Identifier) of this policy is the TSA 1.3.6.1.4.1.52568.1.1.2 .

The OID is included in the time stamps performed by TSA.

6.3. Information for relying parties

fair[&]smart provides to users using time-stamps signed by TSU's certificates, informations about the revocation status of TSU's certificates used by the TSA.

These informations are published through several servers:

- Web Servers:
  - http://crl.certigna.fr/entityca.crl
  - http://crl.dhimyotis.com/entityca.crl
- OCSP Servers:
  - http://entityca.ocsp.certigna.fr
  - http://entityca.ocsp.dhimyotis.com

The TSA issues to the users and subscribers:

- The Time-stamp Policy;
- The certificates used by TSU and the associated CA certificates (root and subordinate CA);

The CA issues to the users and subscribers:

- The Certification Policy of the CA issuing TSU's certificats;
- The Certificate Revocation List (ARL / CRL);
- The Certification Practice Statement of the CA issuing TSU's certificats

The subscribers and users can access the certificates of CA that are signing the certificates of UH at the following addresses:

- https://www.certigna.fr/autorites
- https://www.dhimyotis.com/autorites

7. Certification Policy Statement

fair[&]smart TSA certificate are issued by certigna. Relevant information can be found on certigna web site : https://certigna.fr .

8. Obligations and Liability

8.1. General

The fair[&]smart TSA ensures conformance with the requirements prescribed in this TSA policy.

8.2. TSA Obligations

The fair[&]smart TSA guarantees that time-stamp tokens are issued in accordance with the following:

- Issue the time stamps in accordance with the TSA´s Policy and Practices document,

- The time-stamping unit (TSU) is in accordance with a minimum UTS time accuracy of +/- 1 second,
- the fair[&]smart TSA provides a time-stamping service of high availability backed up by redundant infrastructure. The availability is guaranteed as long as none of the following occur: planned technical interruptions, natural disasters, wars, acts of terrorism, strikes, failures of the Internet or other causes,
- Revise internal system audits,
- Publish possible incidents on TSA´s web about possible incidents that could affect issued stamps indicating if the stamps are affected.

8.3. Relying Parties Obligations

When relying on a time-stamp token, the Relying Party shall verify that the time-stamp token was correctly signed and that the private key used to sign the time-stamp token has not been revoked.

During the validity period of the TSU's certificate, the validity of the signing key can be verified on the CA CRL.

If the verification takes place after expiry of the certificate's validity period, the relying party shall check whether the employed hash function, algorithms, and cryptographic key lengths can still be deemed secure.

For further terms and conditions applicable to Relying Parties, refer to the TSA Disclosure Statement.

8.4. Liability

The TSA may not be held liable for any unauthorized or improper use of time-stamps issued by its time-stamping service.

The TSA shall under no circumstances be held liable for any damage caused using the timestamps issued by the TSA.

The TSA cannot be implicated by delays or losses suffered by the transmitted data on which a time-stamp is requested by the application service.

The TSA cannot be held liable for problems due to force majeure, within the meaning of the Civil Code.

9. TSA Practice and Disclosure Statements

9.1. TSA Practices Statement

The TSA practice statement defines how fair[&]smart is to adhere to the relevant requirements.

This TSA Practice Statement and other relevant documentation will be published on: https://tsa.fairandsmart.com/policy.

The TSA Disclosure Statement is included in chapter 9.2 of this TSA policy document.

9.2. TSA Disclosure Statement

The terms and conditions, set forth herein, are binding to all Relying Parties using fair[&]smart time-stamping services.

The fair[&]smart TSA is an internal service of fair[&]smart.

For contact information, refer to chapter “Corporate Information”.

Each time-stamping token issued by fair[&]smart Time-stamping service includes the policy objectidentifier in chapter “Information for relying parties”.

The TSA ensures time accuracy compliant with the minimum UTC time accuracy standards of +/- 1 second. The fair[&]smart TSA will not issue time-stamp tokens, if the time accuracy is no longer secured.

The following fields are present in the time-stamping answer:

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

A Relying Party's obligations and information on how Relying Party can verify the trustworthiness of the TST are described in chapter “Relying Parties Obligations”.

fair[&]smart may charge fees for the services offered by fair[&]smart TSA.

fair[&]smart maintains records on the operations of the fair[&]smart TSA, in accordance with chapter FIXME.

9.3. Key management Lifecycle

9.3.1. TSA keys generation

fair[&]smart generates the cryptographic keys in a physically secured environment by personnel in trusted roles.

Keys are generated using the following guidelines :

- Algorithm generation: RSA
- Size: 2048 bits.

9.3.2. TSU private key protection

The fair[&]smart TSA ensures that the confidentiality and integrity of their keys is maintained.

9.3.3. Rekeying TSU's Key

TSU signature password expires in the following cases:

- When the certificate of the public password used for its verification expires.
- When it has been compromised.
- When technological devices with computing capacities have compromised the technological strength by using violated cryptographic algorithms.
- When the TSU is damaged or destroyed contained in the private password.
- When the lifetime expires, it will be renewed by a new one with the security guarantees contained in this document.

TSA will never use an expired password.

9.3.4. TSU public key distribution

The TSU signature key is available at https://tsa.fairandsmart.com/certificate .

The TSU signature key certificates are available at https://tsa.fairandsmart.com/chain

9.3.5. TSU certificate

The TSA guarantees the integrity and authenticity of the TSU signature verification (public) keys:

- The TSU signature verification (public) keys is made available to relying parties in a public key certificate.
- The TSU does not issue time-stamps before its signature verification (public key) certificate is loaded into the TSU.
- When obtaining a signature verification (public key) certificate, the TSA verifies that this certificate has been correctly signed (including verification of the certificate chain of the trusted certification authority).

The validity period of TSU's certificate is fixed to 2 years. This period is not longer than the cryptographic lifetime of the associated private key.

9.3.6. TSU private key use duration

The duration of use of a TSU private key is limited to 2 years.

9.3.7. TSU private key end-of-life

The TSA ensures the destruction of the private key and its copies when the end of the period of use of this private key has been reached.

9.4. Timestamping

9.4.1. Precision

Maximum precision error during time-stamp: 1 second. TSU are monitored to detect changes in clock calibration and/or synchronization problems that threaten to compromise the declared accuracy.

9.4.2. Time Management

The TSA service uses stratum 2-3 timeserver as a reliable time sources, by means of communications protocol NTP and from the following pools :

- 0.ubuntu.pool.ntp.org
- 1.ubuntu.pool.ntp.org
- 2.ubuntu.pool.ntp.org
- 3.ubuntu.pool.ntp.org
- ntp.ubuntu.com

9.4.3. Access to the TSA client service

fair[&]smart TSU can not be used for timestamping from outside fair[&]smart infrastructure.

9.4.4. Registration and operation inquiry

TSA maintains a registration of the stamps performed and can be consulted for its verification at https://tsa.fairandsmart.com

9.4.5. Time-Stamps management

9.5. Verification of time stamps

The certificate chain used by TSA are the following:

- Primary Authority Certification :
  - C=FR
  - O=Dhimyotis
  - CN=Certigna
  - Footprint SHA1: B1:2E:13:63:45:86:A4:6F:1A:B2:60:68:37:58:2D:C4:AC:FD:94:97
  - Valid between 29/06/2007 17:13:05 CEST and 29/06/2027 17:13:05 CEST
- Intermediate Authority :
  - C=FR
  - O=DHIMYOTIS
  - OU=0002 48146308100036
  - CN=Certigna Entity CA
  - Footprint SHA1: C2:72:7C:C1:73:4C:D4:A2:BC:DB:EB:47:46:B5:9B:35:76:8B:6D:28
  - Valid between 25/11/2015 11:24:07 CET and 22/11/2025 11:24:07 CET
- fair[&]smart :
  - C=FR
  - O=FAIR AND SMART
  - OU=0002 82092467800015
  - CN=FAIR AND SMART - FAIRANDSMART - TIMESTAMPING
  - SN=T11774001
  - Footprint SHA1: 04:7E:B5:1B:2A:9C:53:D3:EC:19:56:51:26:43:32:77:D0:32:7C:56

  - Valid between 21/02/2019 16:15:55 CET and 20/02/2021 16:15:55 CET

The Primary Authority Certification of fair[&]smart publishes a list of revoked certificates (CRL) at :

- Web Servers :
  - http://crl.certigna.fr/entityca.crl
  - http://crl.dhimyotis.com/entityca.crl
- OCSP Servers :
  - http://entityca.ocsp.certigna.fr
  - http://entityca.ocsp.dhimyotis.com

9.6. TSA management

9.6.1. Personnel Security

All staff must work within the TSA components must sign the internal security charter. This charter contains a confidentiality clause which applies both in respect of third parties and users. It lists the roles of each employee within the PKI. It is co-signed by the employee and the security officer. Skills matching of personnel involved in the TSA is checked in compliance with its duties on the components.

The concerned staff receives adequate information and training prior to any change in systems, procedures or organization.

Any member of the TSA staff acting in contradiction with established policies and procedures of this CP and internal processes and procedures of theTSA, or negligently or maliciously, will have its privileges revoked and will be subject to administrative sanctions or judicial proceedings.

9.6.2. Physical and Environmental Security

Physical or electronic access to TSA sub system hardware is restricted to authorized technical personnel.

9.6.3. Operation Security

The TSA system components are secured and correctly operated throught the following mechanisms :

- The integrity of TSA system components and information are protected against viruses, malicious and unauthorized software,
- Incident reporting and response procedures are designed to minimize damage from security incidents and malfunctions,
- Media used within the TSA trustworthy systems are secured to protect media from damage, theft, unauthorized access and obsolescence,
- Trusted and administrative roles that impact on the provision of time-stamping services follow established procedures,
- Media containing sensitive data are securely disposed of when no longer required.

- Capacity demands is monitored to build an adapted capacity planning,
- TSA security operations are separated from other operations

9.6.4. Network security

The TSA system access is limited to properly authorized individuals :

- Systems are protected by firewalls and proxies,
- System access are filtered,
- Breach detection and regular security audits are in place.

9.6.5. Compromise of TSA Services

The following procedures are applied if a TSU's private signing keys is compromised or loses its calibration :

- The TSA's disaster recovery plan takes in account time-stamp tokens which have been issued during the period,
- A description of compromise that occurred will be made available,
- The TSU will not issue time-stamp tokens until steps are taken to recover from the compromise
- information will be published to identify the time-stamp tokens which may have been affected, unless this breaches the privacy of the TSAs users or the security of the TSA services.

9.6.6. TSA termination

fair[&]smart TSA being used for internal purpose, no backup will be kept after TSA terminaison. In particular :

- TSU private keys, including backup copies, will be destroyed in a manner such that the private keys cannot be retrieved,
- TSU certificates will be revoked.

9.6.7. Recording of Information Concerning Operation of Time-Stamping

(to be documented, see 7.4.11 in RFC 3628)

9.7. Organizational

(to be documented, see 7.5 in RFC 3628)

10. Policy Administration

10.1. Corporate Information

This document and the services provided are owned by Fair And Smart and address in Metz (France), 11, Rampart Saint Thiebault – 57000 Metz (France).

Current version of this document may be downloaded from https://tsa.fairandsmart.com/policy. These CP/CPS are designed according to international standards based on RFC 3647.

10.2. Modifications and duration

fair[&]smart reserves the right to exercise at any moment modifications and updates to the provision of services, contents, configuration, availability and information presentation as well as the present conditions of use without prejudice to the acquired rights. It also reserves the right to suspend temporarily the access and to perform maintenance work or improvements without resulting in claims, liquidated or indirect damages for this concept other than those indicated in paragraph “Liability”.

10.3. Applicable law and jurisdiction

The operating conditions of this service shall be governed and interpreted according to French legislation. Any controversy that may exist between parties in relation to what is established is subject to the courts and tribunals of Metz.