Signicat-TSP001 Disclosure statement & Terms and conditions

Document ID:	Signicat-TSP001
Owner:	COO
Version:	Version 1.6
Date:	2020-03-25
Distribution:	Public

Definitions and abbreviations

Definition	Explanation
ASP Agreement	The ASP Agreement entered into between Signicat and the Subscriber, whereby Signicat provides certain services to the Subscriber.
ETSI	European Telecommunications Standards Institute.
NTP	Network Time Protocol.
OID	Object Identifier.
Relying Party	A recipient of a Time-stamp who relies on that Time-stamp.
Signicat	Signicat AS, the trust service provider, a Norwegian company with business registration number 989 584 022, maintaining its principle place of business at Gryta 2B, 7010 Trondheim.
Subscriber	The receiver of the TSA Service from Signicat (referred to as the "Customer" in the ASP Agreement).
Time-stamp	Data in electronic form that binds other electronic data to a particular time establishing evidence that these data existed at that time.
TSA Service	Time Stamp Authority Service, meaning highly reliable time-stamping services provided by a trust service provider.
TST	Time-stamp token. In compliance with the time-stamp protocol defined in RFC 3161, defines a structure containing a datum (typically a hash) and a time-stamp, and an electronic seal binding them together in a non-reputable manner.
TSP/TSPS	Time-stamp policy/Time-stamp practice statement.
UTC	Coordinated Universal Time.

1. Scope

The present document provides high-level disclosures regarding the TSA Service from Signicat and sets out a brief description of the TSA Service as well as the terms and conditions for using it (the *"Disclosure Statement & Terms and Conditions"*). The purpose this document is to highlight the policies and procedures of the TSA that require particular emphasis or disclosure to Subscribers or Relying Parties. This document does not constitute the entire agreement between the Subscriber and Signicat. The provision of the TSA Service from Signicat to the Subscriber is governed by the ASP Agreement, and the policies and practices applicable to the TSA Service are specified in the TSP/TSPS. This version of the document has been approved for use by the management of Signicat, and is subject to amendment and change in accordance with the policies and guidelines adopted, from time to time, by Signicat.

2. Policy

Signicat issues qualified electronic Time-stamps whose function is to prove that a datum existed before a point in time, by binding a time-stamp to the datum and sealing them.

Signicat operate in accordance with the EU Regulation No. 910/2014 (the "*eIDAS Regulation*"), as well as the “Signicat-TSP002 Time-stamp policy”, identified by OID: ***2.16.578.1.46.1.14.3.6*** (the TSP/TSPS), which is fully compliant with the ETSI Best practice time-stamp policy as defined in ETSI EN 319 421 v1.1.1, identified by OID: ***0.4.0.2023.1.1.***

To the extent that the provision of the TSA Service requires Signicat to process personal data, such data is processed in accordance with Directive 95/46/EC and with effect from May 25 2018 in accordance with the Regulation (EU) 2016/679 (General Data Protection Regulation). The data processing agreement for such processing is enclosed as an appendix to the ASP Agreement.

The applied signing algorithm is **sha256-with-ecdsa**, with **256**-bit key length.

3. Subscribers’ obligations

Subscribers are obliged to use the TSA Service in accordance with any applicable agreement with Signicat, including, but without limitation, the ASP Agreement and this Disclosure Statement & Terms and Conditions.

Subscribers are obliged to inform their Relying Parties about their obligations, correct use of the time-stamps and of any relevant conditions as stated in this Disclosure Statement & Terms and Conditions, the ASP Agreement, and the TSP/TSPS. Subscriber shall ensure that all Relying Parties are bound by terms and conditions no less stringent than the terms and conditions set forth in any such agreements entered into between Subscriber and Signicat.

Subscribers and Relying Parties shall, when relying on a Time-stamp, verify that the Time-stamp has been correctly signed and that the public key certificate has not been revoked or otherwise compromised at the time of verification, taking into account any limitations on the usage of the Time-stamp or other precautions prescribed in agreements or elsewhere.

Time-stamps issued by Signicat shall not be used in activities in violation of any applicable law.

The Subscriber shall notify Signicat without undue delay should any breach of security or loss of integrity come to the knowledge of the Subscriber.

4. Reliance limits

Signicat ensures that the clock of the TSA Service is synchronized with UTC within the declared accuracy of one (1) second.

The TSA Service event logs are retained for at least five (5) years to suffice as evidence in case it is needed. These logs contain every issued Time-stamp within that period.

5. Liability

Signicat is liable for the fulfillment of its obligations as specified in the TSP/TSPS, Signicat makes no express or implied representations or warranties relating to the availability or accuracy of the TSA Service.

Signicat's liability for damages under the TSP/TSPS shall in any event not exceed Signicat's liability pursuant to the terms and conditions of the ASP Agreement.

Without limiting the foregoing, Signicat accepts no liability whatsoever towards the Subscriber, Relying Parties, or any other third person, for:

(i) any loss suffered attributable to the Subscriber's faults, security problems or non-performance of its obligations;
(ii) liability for indirect loss (including data loss) or indirect damages of any kind, in contract tort or otherwise;
(iii) errors or delays that are outside Signicat's reasonable control, including without limitation general internet failure, line delays, power failure or faults of any machines, and;
(iv) the non-performance of its obligations if such non-performance is due to faults or security problems of the supervisory body, the data protection supervision authority, Trusted List, any other public authority, or any other third party.

6. Refund policy

Refunds shall be provided for the term after which the termination event occurs if the customer has paid for the service in advance. Refunds shall not be subject to any additional payments other than the return of monies already paid to Signicat.

7. Insurance

Signicat will have and maintain appropriate liability insurances for the provision of the TSA Service.

8. Limitations on the use of the service

Use of the TSA Service is limited to activities that do not violate any applicable law.

The expected lifetime of a public key certificate for the Signicat-TSP002 Time-stamp policy is four (4) years.

9. Termination

Signicat will inform all Subscribers before it terminates the TSA Service, and will maintain the relevant documentation and information in accordance with the applicable policy.

10. Applicable law, complaints and dispute resolution

The TSA Service, the TSP/TSPS and this Disclosure Statement & Terms and Conditions are governed by the law governing the ASP Agreement.

Any disputes or complaints between Signicat and Subscribers and/or Relying Parties shall be settled by negotiations in good faith. If the parties fail to reach an amicable settlement, the dispute shall be submitted to dispute resolution in the manner and jurisdiction set forth in the ASP Agreement.

In the event a dispute or complaint resolution process is initiated relating to a Time-stamp generated by the TSA Service, Signicat shall respond in thirty (30) calendar days with a reply in coherence with the comment received. In all instances, Signicat shall demonstrate compliance with the TSP/TSPS.

Additional terms defined in mutual agreements with the Subscriber may apply, such as the ASP Agreement, and will have precedence over this Disclosure Statement & Terms and Conditions.

All dispute or complaint requests shall be directed to Signicat support desk – support@signicat.com. The dispute or complaint requests will be automatically registered as tickets in the Signicat support system and followed-up by support staff.

11. Conformity

Signicat has qualified status in the Norwegian Trusted List, and by that, is also listed as a qualified trust service provider in the European Union Trusted Lists - EUTL.

Consequently, Signicat issues qualified time-stamps as defined in the eIDAS Regulation, and is subject to a yearly assessment by an accredited body. The resulting audit results and certification are published at www.signicat.com.

12. Contact information

Signicat AS

Gryta 2B
N-7010 TRONDHEIM
Norway

Telephone: +47 400 03 410
E-mail: support@signicat.com