



TrustWeaver AB DEVELOPMENT Time-Stamping Policy

1. Identification

This DEVELOPMENT Time-Stamping Policy was issued by TrustWeaver AB under the unique identifier 1.2.752.76.1.762.654.1.1. For development and test only!

TrustWeaver AB's contact information is:

TrustWeaver AB ADDRESS:

Wallingatan 12
111 60 Stockholm
Sweden

ATTN/REF: Security Officer

EMAIL: securityofficer@trustweaver.com

PHONE: 08-41005790

TrustWeaver AB performs its operations covered by this DEVELOPMENT Time-Stamping Policy in the territory of Sweden.

This DEVELOPMENT Time-Stamping Policy must remain available on:
<https://tsod.trustweaver.com/repository>.

2. Validity

This DEVELOPMENT Time-Stamping Policy was issued on 1 March 2007.

3. Field of application and commitment types

This DEVELOPMENT Time-Stamping Policy includes rules for the automated time-stamping of business data.

TrustWeaver AB will under this DEVELOPMENT Time-Stamping Policy apply a time-stamp to all data that are correctly supplied to the time-stamping service. TrustWeaver AB does not conduct any substantive review of any data submitted in conjunction with a time-stamping request. Time-stamps created under this DEVELOPMENT Time-Stamping Policy do not express or imply the TrustWeaver AB's agreement with or approval of the semantics of the data submitted in conjunction with a time-stamping request. TrustWeaver AB accepts no liability, for the accuracy, completeness, legality and compliance with applicable legal requirements concerning the content and format of business data time-stamped under this DEVELOPMENT Time-Stamping Policy.

TrustWeaver AB shall take all necessary steps to ensure that data which comes into its possession or control in the course of providing services under this DEVELOPMENT Time-Stamping Policy be maintained using reasonable data security measures. TrustWeaver AB shall not:

- Use the data, nor reproduce the data in whole or in part in any form except as required under this DEVELOPMENT Time-Stamping Policy.
- Disclose the data to any third party or persons not authorized by the submitter of the data to receive it, except with the prior written consent of submitter of the data; or
- Alter, delete, add to or otherwise interfere with the data except as expressly required under this DEVELOPMENT Time-Stamping Policy.

To the extent that any data submitted to the time-stamping service is personal data within the meaning of the applicable laws:

- TrustWeaver AB shall process such personal data only in accordance with instructions from the submitter of the data. Processing including time-stamping in accordance with this DEVELOPMENT Time-Stamping Policy shall be considered an instruction from the submitter of the data.
- TrustWeaver AB shall take such technical and organizational measures against unauthorized or unlawful processing of such personal data and against accidental loss or destruction of, or damage to, such personal data as are appropriate to TrustWeaver AB as data controller.

4. TrustWeaver AB time-stamping conditions

TrustWeaver AB warrants that its time-stamping practices under this DEVELOPMENT Time-Stamping Policy comply with the policy requirements stated herein.

Time-stamps created under this DEVELOPMENT Time-Stamping Policy must meet at a minimum the following rules.

Personnel controls:

- TrustWeaver AB checks the identity and suitability of all persons operating the time-stamping service.
- TrustWeaver AB provides the training and instructions required for all relevant staff to fulfill their tasks.
- Where a contractor is engaged, appropriate checks are made and TrustWeaver AB retains all responsibilities and liabilities towards third persons.
- All persons operating the time-stamping service are provided with documented procedures on how to operate the system.

Physical controls:

- Physical access to the operational facilities is allowed only for authorized personnel under controlled procedures.
- All removable media are stored under appropriately secure conditions.

Time-stamping under this DEVELOPMENT Time-Stamping Policy must at a minimum fulfill the following technical and process requirements:

- The signature on the time-stamp must at a minimum be created using a 2048-bit RSA-key. The time-stamp signing key pair is generated using controlled procedures, and is protected by the physical and personnel controls as defined above.
- Time-stamp tokens should be fully synchronized with UTC. This time synchronization is ensured by local system clock.
- Time-stamps successfully created under this DEVELOPMENT Time-Stamping Policy must include at a minimum a TimeStampToken Information with OID 1.2.840.113549.1.9.16.1.4 as defined in RFC 3161.

END