Trust Services Practice Statement

TrustWeaver AB

IMPORTANT LEGAL NOTICE

1. Introduction

This document describes the practices and procedures followed by TrustWeaver AB (TrustWeaver) in the provisioning of Trust Services.

For information about TrustWeaver services please contact:

TRUSTWEAVER AB
Kungsgatan 27, 4tr
111 56 Stockholm
SWEDEN

Telephone: +46 8 41 005 790
Fax: +46 8 21 29 20

Registered in Sweden Org no. 556613-6262

2. Definitions

eIDAS Regulation: means Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 *on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.*

Subscriber: means a natural or legal person to whom TrustWeaver provides the Trust Services.

Relying Party: means a natural or legal person that relies upon an electronic identification or a trust service.

Trust Service: means qualified validation services provided by TrustWeaver as defined in the eIDAS Regulation.

3. Obligations and liability

3.1. TrustWeaver obligations

This document applies only to the provision of Trust Services under the eIDAS Regulation.

TrustWeaver provides its Trust Services in accordance with the requirements and procedures set out in this Practice Statement and related policies and practice statements. TrustWeaver offers its Trust Services under non-discriminatory practices.

TrustWeaver ensures that all requirements defined in this Practice Statement are implemented and remain applicable to the Trust Services provided.

TrustWeaver complies with all legal obligations applicable to the provisioning of its Trust Services. TrustWeaver fulfills general security requirements set out in article 19 and 24 of the eIDAS Regulation as further developed in ETSI EN 319 401 *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.*

In relation to the qualified validation Trust Services, TrustWeaver provides qualified validation of qualified electronic signatures in accordance with article 33 of the eIDAS Regulation and relevant sections of ETSI EN 319 102-1 *Electronic Signatures and*

Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.

The provision of Trust Services is subject to an external conformity assessment performed at least every 24 months by a Conformity Assessment Body and the qualified status is supervised by the Supervisory Body appointed by Sweden, *Post- och telestyrelsen*.

Records concerning the operation of the Trust Services are made available to affected parties upon legitimate request for the purposes of providing evidence of the correct operation of the Trust Services for the purposes of legal proceedings.

3.2. Subscribers obligations

Subscribers are obliged to maintain confidentiality of the passwords and applicable credentials to use the Trust Service and promptly communicate TrustWeaver any circumstance raising suspicion or risk of them being compromised.

3.3. Obligations of all external organizations

Certification Authorities supporting the Trust Services are subject to the fulfillment of applicable obligations under Regulation (EU) 910/2010, in particular, section 4.

Two external suppliers providing data center collocation services to TrustWeaver are responsible for ensuring redundant power generation, smoke, temperature, humidity, and water leakage detection monitors and a fire suppression system, as well as physical security and monitoring systems alerting any attempt of unauthorized access to its perimeter. TrustWeaver monitors implementation of applicable controls on a regular basis.

3.4. TrustWeaver Liability

TrustWeaver is liable for the performance of all its obligations to the extent prescribed by the legislation of Sweden.

TrustWeaver has appropriate insurance arrangements to cover TrustWeaver provision of Trust Services to ensure compensation for damages caused by an intentional or negligent violation of TrustWeaver obligations under the eIDAS Regulation.

TrustWeaver is not liable for:

- any damage arising from a signatory or a Subscriber failing to maintain the secrecy of the passwords and applicable credentials to use the Trust Service;
- the non-performance of its obligations if such non-performance is due to faults or security problems of any public authority;
- non-fulfillment of its obligations if such non-fulfillment is caused by a Force Majeure event.

3.5. Dispute Resolution

Unless otherwise agreed between TrustWeaver and the Subscriber in writing, and to the extent permitted under the applicable law, all disputes arising out or in connection with the provision of the Trust Services by TrustWeaver shall be submitted to the courts of Stockholm (Sweden).

3.6. Confidentiality

All confidential and proprietary information disclosed to TrustWeaver in the use of Trust Services shall be Confidential Information. Confidential Information does not include information that: (i) enters the public domain through no fault of TrustWeaver; (ii) is communicated by a third party to TrustWeaver free of any obligation of confidence; (iii) has been independently developed by TrustWeaver without reference to any Confidential Information of the disclosing party; (iv) was in TrustWeaver's lawful possession prior to disclosure and had not been obtained either directly or indirectly from the disclosing party, or (v) is required to be disclosed by law, provided TrustWeaver has promptly notified the disclosing party in writing of such requirement and allowed the disclosing party a reasonable time to oppose such requirement.

4. Trust Service Practices

4.1. Trust Services Practice Statement Management

TrustWeaver Practice Statement is approved by TrustWeaver management and its applicability is ensured by regular internal and external audits. TrustWeaver Practice Statement is reviewed annually or in conjunction with major updates of the Trust Services.

TrustWeaver may incorporate changes to this Practice Statement at any time by publishing such amended Practice Statement on its website and communicating material changes to it to its customers through a bulletin. The updated Practice Statement shall specify when the amendments will come into effect.

4.2. Terms and Conditions of the Trust Service

All prospective subscribers will receive, prior to entering into a contractual relationship with TrustWeaver, the applicable terms and conditions of the Trust Service, drafted in a clear and comprehensive manner.

4.3. Practices for Signature Validation Services

4.3.1. Signature Validation Services Practice Statement

This Signature Validation Services practice statement is based on ETSI TR 102 041 and complies with the TrustWeaver AB Signature Validation Policy with OID 1.2.752.76.1.199.699.1.10. All ETSI EN 319 401 requirements are covered by the general statements of TrustWeaver's Trust Services in this document. This section addresses specifically the Signature Validation Services practice statements derived from EU regulation 910/2014 articles 32 and 33 in conjunction with ETSI EN 319 102-1.

4.3.2. Signature Validation

Signature validation process selection: The following validation processes (in ETSI EN 319 102-1 terms) may be selected by the client application but the choice is constrained by limitations of the signature format that has been applied:

- Validation Process for Basic Signatures.

- Validation process for Signatures with Time and Signatures with Long-Term Validation Data.
- Validation process for Signatures with Archival Data.

Signature validation process:

a. The format of the signature is identified and unknown formats are rejected.
b. The certificate is extracted from the signature or from a local repository of pre-configured certificates.
c. The status of the certificate as a Qualified Certificate is verified.
d. The status of the CA as a Qualified CA is verified.
e. Verification that the certificate was issued for a key residing on a QSCD.
f. Revocation status information for the certificate is collected and the freshness of that information is determined.
g. The Certificate and certificate chain is validated at a time that takes into account the presence of any recognized time-stamps.
h. The integrity of the document is verified.
i. A validation report is created based on the results in step a-h.
j. The validation report (see section "Validation Report") is returned from TrustWeaver Signature Validation Service to the application.

Validation Report: TrustWeaver Signature Validation Service produces a comprehensive validation report of the validation in accordance with ETSI EN 319 102-1, allowing the client to inspect details of the decisions made during validation and investigate the detailed causes for the status indication. The validation report also outputs the identity of the certificate indicating the presence of a pseudonym as well as statements on the qualified status of the certificate. When a qualified signature is confirmed, the validation report is signed by the TrustWeaver Signature Validation Service.

4.4. Practices for Time-Stamping Services

4.4.1. Time-Stamping Services Practice Statement

This Time-Stamping Services practice statement is based on ETSI EN 319 421 and complies with the TrustWeaver AB Time-Stamping Policy with OID 1.2.752.76.1.199.699.1.8. All ETSI EN 319 401 requirements are covered by the general statements of TrustWeaver's Trust Services in this document. This section addresses specifically the Time-Stamping Services practice statements of ETSI EN 319 421.

The signature on the time-stamp is at a minimum created using the SHA-256 algorithm and 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 in the sections above.

Time-stamp tokens are fully synchronized with CET/CEST. This time synchronization is ensured by the NTP-protocol. Only reliable time sources are used and monitored for consistency.

4.4.2. Cryptographic controls

Key generation: The generation of the Time-stamping Unit’s (TSU) signing key(s) is undertaken in a physically secured environment (as per section 4.6.4) by personnel in trusted roles (as per section 4.6.3). The personnel authorized to carry out this function is limited to those required to do so under the TSA's practices.

Cryptographic algorithm: The TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing electronic time-stamps is RSA 2048 with SHA-256, in accordance with commonly accepted practices for electronic time-stamps.

Key protection: The TSU private signing key is held and used within the TrustWeaver Signature Validation Service.

TSU certificate: The TSU signature verification certificate is issued by TrustWeaver’s Certification Authority.

The TSU does not issue electronic time-stamps before its public key certificate is loaded into the QSCD.

Re-keying TSU’s key: The life-time of TSU's certificate is 12 years.

The TSU key is re-keyed and the signature verification certificate is renewed annually.

4.4.3. Time-stamping

Electronic time-stamp issuance: Electronic time-stamps conform to the electronic time-stamp profile as defined in RFC 3161.

The electronic time-stamps are issued securely and shall include the correct time. This is ensured by the following measures:

- The time values the TSU uses in the electronic time-stamp are derived from trusted time sources.
- The time included in the electronic time-stamp is synchronized with UTC.
- The electronic time-stamps are signed using the key generated exclusively for this purpose (as stated in section “Cryptographic Controls”).
- The electronic time-stamp generation system rejects any attempt to issue electronic time-stamps if the signing private key has expired.

Clock synchronization with UTC: The TSU clock is synchronized with UTC according to the accuracy defined in the TrustWeaver AB Time-Stamping Policy. The accurate time is retrieved from recognized and reliable time sources over the NTP protocol (RFC 5905).

4.5. TrustWeaver Management Operation

4.5.1. Security Management

TrustWeaver complies will all relevant legal requirements related to security management applicable to the provisioning of the Trust Services. Conformity with such legal requirements and recognized European standards is assessed at least every 24 months by external auditors. Internal controls and monitoring activities are performed regularly by means of automated and human auditing and testing.

TrustWeaver's management approves TrustWeaver´s Information Security Policy, which sets out corporate aims and commitments, risk management principles as well as a disciplinary process for personnel failing to comply with TrustWeaver policies and practices. Risk assessments are performed regularly and residual risks are accepted by TrustWeaver management.

Adequate security controls and operational principles applicable to the facilities, personnel and information assets relevant for the provisioning of the Trust Services are further developed in lower level information security policies. Regular reviews ensure that TrustWeaver´s Information Security Policy is duly updated to regulatory, organizational and product changes.

TrustWeaver communicates its Information Security Policy to all employees and external parties affected by it.

The Information Security Policy is further developed in practices and processes under the supervision of TrustWeaver's Chief Security Officer.

4.5.2. Asset Management

TrustWeaver maintains updated inventories of its assets, including information assets. Security and asset classification is assigned in consistency with the risk assessment.

Media containing sensitive data is securely handled and disposed when no longer required. This includes a thorough erasure process or a secure disposal for physical media containing sensitive data.

4.5.3. Management of Personnel

TrustWeaver personnel have all the necessary experience and/or qualifications to carry out the duties specified in their employment contract and applicable job descriptions. Appropriate qualifications and experience, ID, and criminal background checks are performed in accordance with applicable laws to ensure the trustworthiness of prospective employees before gaining access to TrustWeaver's information systems.

Regular training sessions on security and privacy are held at least yearly. Attendance to such training or review of the recordings of such training is mandatory for all TrustWeaver employees.

TrustWeaver's management appoints Trusted Roles with job duties critical for the trustworthy provision of the Trusted Services. These include:

- **Security Officer:** Overall responsibility for security practices.

- **System Administrator:** Authorized to install, configure and maintain production systems. Also authorized to perform system backups and recovery.
- **System Auditor:** Authorized to view production system audit logs.

The principle of least privilege oversees the management of access and privileges configuration, and the impartiality of TrustWeaver personnel is ensured by enforcing segregation of duties between Trusted Roles. Access to information and data is subject to access controls to ensure that access privileges are granted under a strict need to know basis.

4.5.4. Physical and environmental security

Environmental and physical controls are designed to ensure that physical risks to assets are minimized.

All components critical for the provision of the Trusted Services are located in secured facilities subject to access controls through the perimiter, monitoring and alarms to detect intrusion. Only pre-authorised personnel has access to these secured facilities. Records are maintained of all entries to such facilities.

Redundancy is implemented on power and network connections, security controls and critical infrastructue to ensure that any potential malfunction does not affect the full operational availability of the Trust Services and to avoid loss or compromise of assets. Facilities hosting critical systems are equipped with humidity, temperature and smoke control systems.

Video cameras or other monitoring mechanisms trigger alerts to on-duty personnel upon access to facilities hosting critial systems.

4.5.5. Operation security management

TrustWeaver uses trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them. Appropriate mechanisms are deployed and regularly reviewed to ensure protection of TrustWeaver network and information systems from malicious code. Patch management practices are enforced to address vulnerabilities in a timely manner, depending on its severity.

Operational systems and application software are subject to strict change management control, including testing, risk assessment, fallback and approval procedures.

4.5.6. Business Continuity and Incident Management

TrustWeaver has a documented incident response plan and vulnerability monitoring and management processes to address, in a timely and co-ordinated manner, incidents and to limit the impact of breaches of security. These procedures foresee the notification to the appropriate parties within 24 hours in line with the applicable regulatory rules in case of any breach of security or loss of integrity that has a significant impact on the Trust Service provided and on the personal data maintained therein. TrustWeaver Privacy Officer is involved in assessing interests of data subjects in case of any potential security breach.

Audit logs are regularly reviewed by Trusted Role personnel and an alert system detects potential attacks.

TrustWeaver's Continuity Dinsaster Recovery Plan defines the procedures implemented to ensure that, in the event of a disaster (including failure of critical components of TrustWeaver systems), operations can be restored as soon as possible.

In the event of a breach of security or loss of integrity having a significant impact on the Trust Service, TrustWeaver will inform Subscribers, Relying Parties and appropriate public bodies without undue delay and in any event within 24 hours after having become aware of such incident.

4.5.7. Network Management

TrustWeaver computer systems are segmented into zones, with strictly defined security controls. All systems within a given zone are subject to the same security controls and communications between zones is restricted.

A strict separation between development and test and production systems is maintained to reduce the risks of unauthorized access or changes to the production system.

Intrusion Detection Systems (IDS) configurations are defined and regularly reviewed. Logs are reviewed daily and alerts are triggered and resolved in a timely manner.

Network vulnerability scans and penetration tests are regularly performed.

4.5.8. Records concerning the use of Trust Services

TrustWeaver maintains records concerning the operation of the Trust Services for the purposes of providing evidence of the correct operation of the Trust Services. These records will only be disclosed to available to law enforcement authorities under court order and to persons with right to access to them upon legitimate request.

These records are maintained under confidentiality in redundant facilities to ensure availability throughout the period they are maintained.

Full log backups are created weekly and logs are retained for a minimum period of five (5) years. The electronically archived records are maintained in redundant servers subject to physical and logical access controls.

5. Trust Service Termination

Before TrustWeaver terminates a Trust Service the following procedures will be executed:

- TrustWeaver informs the following parties about the termination: all subscribers and other entities with which TrustWeaver has agreements. In addition, this information will be made available to other relying parties (e.g. by publishing the notice of termination on TrustWeaver's website).
- TrustWeaver shall, if applicable, terminate authorization of all subcontractors to act on behalf of TrustWeaver in carrying out any functions relating to the trust services.
- TrustWeaver shall transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of TrustWeaver for a

reasonable period, unless it can be demonstrated that TrustWeaver does not hold any such information.

- TrustWeaver's private keys, including backup copies, shall be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.
- Where possible, TrustWeaver should make arrangements to transfer provision of trust services for its existing customers to another Trust Service Provider.
- To the extent required under the applicable regulations, TrustWeaver notifies the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities.

6. History

Document history			
Version	Updates	Applicable date	Publication date
v.1.0	Internal draft	N/A	N/A
v.1.1	Definition for Signature Service	July 1st 2016	August 2016
v.1.2	Description of data collocation service center	April 7th 2017	April 2017
v.2.0	Removed previous statements on the Signature Services (remote signing) as this is not a defined Trusted Service under the Regulation. Not substantial formatting typographic mistakes and enhanced description of mandatory yearly employee training	May 1st 2018	April 2018
v.2.1	Removed signature and time stamping operations details as these are not defined Trusted Services provided by TrustWeaver under the Regulation.	1st July 2019	June 2019