TrustWeaver AB DEVELOPMENT Signing Policy

1. Identification

This DEVELOPMENT Signing Policy was issued by TrustWeaver AB under the unique identifier 1.2.752.76.1.762.654.1.2. For development and test purposes 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 signing operations covered by this DEVELOPMENT Signing Policy in the territory of Sweden.

This DEVELOPMENT Signing Policy must remain available on: https://tsod.trustweaver.com/repository.

2. Validity

This DEVELOPMENT Signing Policy was issued on 1 March 2007.

3. Field of application and commitment types

This DEVELOPMENT Signing Policy includes rules for the automated signing of business data.

Signatures created under this DEVELOPMENT Signing Policy aim exclusively to ensure compliance with laws requiring integrity and authenticity of business data.

For purposes of this DEVELOPMENT Signing Policy:

- "Controller" is the legal or natural person that, for itself of for third parties to which it provides services, determines the applicable laws and associated signing requirements (including certificates and signing

processes to be used) to be complied with by the signing service (such laws and requirements will hereafter also be referred to as the "selected laws").
- "Data Owner" is a legal or natural person authorized by TrustWeaver AB to use the signing service.

If permitted under the selected laws, TrustWeaver AB, Controller and Data Owner may be one and the same legal or natural person. Signatures under this DEVELOPMENT Signing Policy shall be created with a private key corresponding to a public key certificate that has been issued in accordance with the selected laws. TrustWeaver AB must protect such private keys in accordance with selected laws and contractual requirements.

The determination of selected laws is made by the Controller. TrustWeaver AB shall follow the Controller's signing instructions in this regard.

TrustWeaver AB will under this DEVELOPMENT Signing Policy apply a signature to all data that are correctly supplied by the Data Owner. TrustWeaver AB does not conduct any substantive review of these data. Signatures created under this DEVELOPMENT Signing Policy do not express or imply TrustWeaver AB's agreement with or approval of the semantics of the signed data. TrustWeaver AB accepts no liability, for the accuracy, completeness, legality and compliance with applicable legal requirements concerning the content and format of business data signed under this DEVELOPMENT Signing 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 Signing 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 Signing Policy.
- Disclose the data to any third party or persons not authorized by the Data Owner to receive it, except with the prior written consent of the Data Owner; or
- Alter, delete, add to or otherwise interfere with the data except as expressly required under this DEVELOPMENT Signing Policy.

To the extent that any data submitted to the signing 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 Data Owner. Processing including signing in accordance with this DEVELOPMENT Signing Policy shall be considered an instruction from the Data Owner.
- 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 signature creation conditions

TrustWeaver AB warrants that its signing practices under this DEVELOPMENT Signing Policy comply with the policy requirements stated herein.

The DEVELOPMENT signing service must in all circumstances comply with any limitations, and respect and notices from the Certification Authority that has issued the certificate(s) to be used for signing under this DEVELOPMENT Signing Policy.

Personnel controls:

- TrustWeaver AB shall check the identity and suitability of all persons operating the signing service.
- Any PIN-codes shall be entered by or under the direct responsibility of the persons who are authorized to sign only. This procedure shall always be carried out unobserved.
- TrustWeaver AB shall provide the training and instructions required for all relevant staff to fulfill their tasks.
- Where a contractor is engaged, appropriate checks shall be made and TrustWeaver AB shall retain all responsibilities and liabilities towards third persons.
- All persons operating the signing service shall be provided with documented procedures on how to operate the system.

Physical controls:

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

Signatures created under this DEVELOPMENT Signing Policy shall at a minimum fulfill the following technical and process requirements:

- The following minimum requirements apply for signing operations:
    - The RSA-key length shall be derived from applicable law. The minimum RSA-key length is 1024 bits.
    - Where required by the applicable law, the private key shall be generated, and signatures shall be created, with compliant hardware and cryptographic software.
    - Where required by applicable law, the signing process shall be limited in either time or volume in between re-authentication (e.g. PIN re-entry) by the certificate holder.
- In case the signature is validated for or on behalf of the Data Owner, certificate validation data shall be obtained from the issuing CA and used for validating the signing certificate. The certificate information shall consist of CA-certificate chains, and the revocation data shall be obtained as OCSP-responses. If such OCSP-responses are not available, revocation data shall be obtained as PKIX CRLs.
- The signature (where relevant, in accordance with the previous bullet, including certificate validation data) shall be time-stamped in accordance with a time-stamping (authority) policy that at a minimum meets the requirements of the time-stamping policy carrying unique identifier 1.2.752.76.1.762.654.1.1.

- Signatures created under this DEVELOPMENT Signing Policy shall include at a minimum the following signed attributes:
    - Message digest.
    - Signing time.
    - Signing certificate (or reference).
    - Signature policy identifier.

The signatures shall also contain one unsigned attribute with a time-stamp over the signature.

5. Minimum required validation controls

Signatures created under this DEVELOPMENT Signing Policy shall not be validated or relied upon for any application or purpose other than those defined in this DEVELOPMENT Signing Policy, or which require signer commitments other than those defined in this DEVELOPMENT Signing Policy.

The verifier of signatures created under this DEVELOPMENT Signing Policy shall at a minimum comply with the validation controls described in the signature validation policy with unique identifier 1.2.752.76.1.762.654.1.3.

END