Signature Policy

TrustWeaver AB

1. Identification

This Signature Policy was issued by TrustWeaver AB (“TrustWeaver”) under the unique identifier 1.2.752.76.1.199.699.1.9.

TrustWeaver's contact information is:

TrustWeaver AB
Kungsgatan 27
SE-111 56 Stockholm
Sweden

Telephone: +46 8 41 005 790

TrustWeaver performs its signing operations covered by this TrustWeaver Signature Policy in the territory of Sweden.

This TrustWeaver Signature Policy must remain available on: http://www.trustweaver.com/policies.

2. Validity

This TrustWeaver Signature Policy was issued on 9 February 2016. TrustWeaver Signature Policy is approved by TrustWeaver management and is regularly reviewed.

TrustWeaver may incorporate changes to this Signature Policy at any time by publishing such amended Signature Policy on its website. The updated Signature Policy shall specify when the amendments will come into effect.

3. Field of application and commitment types

This TrustWeaver Signature Policy includes rules for creation of electronic signatures or seals on business documents. The signatures may be created in batch mode or individually. :

For purposes of this TrustWeaver Signature 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 to use the signing service.

If permitted under the selected laws, TrustWeaver, Controller and Data Owner may be one and the same legal or natural person. Signatures under this TrustWeaver Signature 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

must protect such private keys in accordance with selected laws and contractual requirements.

TrustWeaver will under this TrustWeaver Signature Policy apply a signature to all data that are correctly supplied by the Data Owner. TrustWeaver does not conduct any substantive review of these data. Signatures created under this TrustWeaver Signature Policy do not express or imply TrustWeaver's agreement with or approval of the semantics of the signed data.

TrustWeaver shall take all necessary steps to ensure that the confidentiality of data which comes into its possession or control in the course of providing services under this TrustWeaver Signature Policy be maintained using reasonable data security measures. TrustWeaver shall not alter, delete, add to or otherwise interfere with the data except as expressly required under this TrustWeaver Signature Policy.

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

- TrustWeaver shall process such personal data only in accordance with instructions from the Data Owner. Processing including signing in accordance with this TrustWeaver Signature Policy shall be considered an instruction from the Data Owner.
- TrustWeaver 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 as data controller.

4. TrustWeaver signature creation conditions

TrustWeaver warrants that its signature practices under this TrustWeaver Signature Policy comply with the policy requirements stated herein.

The TrustWeaver signature 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 TrustWeaver signature Policy.

TrustWeaver shall ensure the implementation of procedures, processes and security measures in compliance with the requirements set out in ETSI EN 319 401 *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers* in order to minimize the operational and financial threats and risks associated to the service.

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

- The RSA-key length shall be derived from applicable law. The minimum RSA-key length shall be 2048 bits and the minimum hash algorithm shall be SHA-256. Other RSA-key lengths and hash algorithms may be used if explicitly required by specific jurisdictions.
- Where required by the applicable law, the private key shall be generated, with compliant hardware Qualified Signature Creation Device (QSCD).

- Where required by the applicable law, the private key shall be stored and protected in the QSCD.
- The type of certificate used for signature creation operation shall meet the cryptographic requirements, applicable law and regulations.
- The certificate shall be enrolled to the Signature Service in accordance with the CA's procedures.
- Where required by the applicable law, the signatures shall be created by the QSCD in conjunction with cryptographic software. Authentication data must be managed in accordance with the requirements in each jurisdiction and type of signature. At a minimum the person who are authorized to create signatures must provide a PIN code for accessing the private key. When required by specific legislation or signature types, One Time Password (OTP) schemas may be used in addition to PIN codes.
- 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 signature (where relevant, in accordance with the previous bullet, including certificate validation data) may 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 1.2.752.76.1.199.699.1.8.
- Signatures created under this Signature Policy shall include at a minimum the following signed attributes:
    - Message digest.
    - Signing time.
    - Signing certificate (or reference).
    - Signature policy identifier.

5. Minimum required validation controls

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

The verifier of signatures created under this Signature Policy shall at a minimum comply with the validation controls described in this policy.