TrustWeaver AB DEVELOPMENT Signature Validation Policy

1. Identification

This DEVELOPMENT Signature Validation Policy was issued by TrustWeaver AB under the unique identifier 1.2.752.76.1.762.654.1.3. 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 validation operations covered by this DEVELOPMENT Signature Validation Policy in the territory of Sweden.

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

2. Validity

This DEVELOPMENT Signature Validation Policy was issued on 1 March 2007.

3. Field of application and commitment types

This DEVELOPMENT Signature Validation Policy includes rules for the automated validation of business data.

This DEVELOPMENT Signature Validation Policy aims to complement any data elements provided by the TrustWeaver AB's signature validation service as evidence that signatures are correctly verified by TrustWeaver AB's DEVELOPMENT signature validation service. TrustWeaver AB warrants that signatures that are returned by TrustWeaver AB's DEVELOPMENT signature validation service with the minimum unsigned attributes specified in this DEVELOPMENT Signature Validation Policy have been successfully validated in accordance with the conditions contained herein.

Signature validation performed under this DEVELOPMENT Signature Validation Policy aims exclusively to ensure compliance with laws requiring integrity and authenticity of business data.

For purposes of this DEVELOPMENT Signature Validation 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 signature validation requirements to be complied with by the signature validation service (such laws and requirements will hereafter also be referred to as the "selected laws").
- "Verifier" is a legal or natural person authorized by TrustWeaver AB to use the signature validation service.

If permitted under the selected laws, TrustWeaver AB, Controller and Verifier may be one and the same legal or natural person.

The determination of selected laws to be complied with by the validation service is made by the Controller. TrustWeaver AB shall follow the Controller's validation instructions in this regard.

Validation data created under this DEVELOPMENT Signature Validation Policy may not be relied upon for any application or purpose other than those defined in the signature policy incorporated in or associated to the validated signature, or for any application or purpose which requires signature validation commitments other than those defined in this DEVELOPMENT Signature Validation Policy.

TrustWeaver AB will under this DEVELOPMENT Signature Validation Policy validate all signatures that are correctly supplied to the validation service by the Verifier. TrustWeaver AB does not conduct any substantive review of signed or unsigned business data that are submitted in conjunction with validation requests. Signature validation performed under this DEVELOPMENT Signature Validation Policy does not express or imply TrustWeaver AB's agreement with or approval of the semantics of the business data that are submitted in conjunction with validation requests. TrustWeaver AB accepts no liability, for performing any actions required under applicable law to verify the accuracy, completeness, legality and compliance with applicable legal requirements concerning the content and format of business data that are submitted in conjunction with validation requests.

TrustWeaver AB shall take all necessary steps to ensure that business data that are submitted in conjunction with validation requests under this DEVELOPMENT Signature Validation 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 Signature Validation Policy.
- Disclose the data to any third party or persons not authorized by the Verifier to receive it, except with the prior written consent of the Verifier; or
- Alter, delete, add to or otherwise interfere with the data except as expressly required under this DEVELOPMENT Signature Validation Policy.

To the extent that any data that are submitted in conjunction with validation requests under this DEVELOPMENT Signature Validation Policy are personal data within the meaning of the applicable laws:

- TrustWeaver AB shall process such personal data only in accordance with instructions from the Verifier. Processing including performing signature validation in accordance with this DEVELOPMENT Signature Validation Policy shall be considered an instruction from the Verifier.
- 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 validation conditions

TrustWeaver AB warrants that its validation practices under this DEVELOPMENT Signature Validation Policy comply with the policy requirements stated herein.

The DEVELOPMENT validation 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 validation under this DEVELOPMENT Signature Validation Policy.

Personnel controls:

- TrustWeaver AB shall check the identity and suitability of all persons operating the signing service.
- 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 validation 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.

Validation under this DEVELOPMENT Signature Validation Policy must include at a minimum the following controls:

- Cryptographic verification of the digital signature.
- Certificate validation data is obtained from the issuing CA and used for validating the certificate associated with the private signing key. The certificate information consists of CA-certificate chains, and the revocation data is obtained as OCSP responses. If such OCSP responses are not available, revocation data are obtained as PKIX CRLs.
- The chain of CA-certificates is validated.

- The certificate associated with the private signing key is validated with respect to CA's signature, expiration, and revocation status.

Signatures successfully validated under this DEVELOPMENT Signature Validation Policy must be extended with at a minimum the following unsigned attributes:

- Complete certificate references.
- Complete revocation information references.
- Certificate values.
- Revocation information values.
- Signature validation policy identifier.
- Archive time-stamp in accordance with a time-stamping (authority) policy that at a minimum meets the requirements of the time-stamping policy with unique identifier 1.2.752.76.1.762.654.1.1.

Signatures which have not been successfully validated do not contain any of the attributes above.

The following activities of the signature validation process are logged:

- Operation - i.e. Validate.
- Result code - success or failure.
- Source - client's SSL authentication certificate details and/or IP-address.
- InputType - format of the data in the validation request.
- OutputType - expected format of the validated signature.
- JobType - optional extension to the validation operation.
- SenderTag - sender's signature identifier (e.g. country code).
- ReceiverTag - receiver's signature identifier (e.g. country code).
- InDataHash - hash of the data in the request.
- OutDataHash - hash of the data in the response.
- SignatureValidationPolicy - the OID of this policy.
- CertificatePolicy - the OID of the signer's certificate policy.

END