Signature Validation Policy

TrustWeaver AB

Copyright (c) 2016 TrustWeaver AB. All rights reserved.

IMPORTANT LEGAL NOTICE
Copyright © 2016, TrustWeaver AB. All rights reserved.
This document contains TrustWeaver AB proprietary information, which is protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, or translated into another language, without TrustWeaver's prior written consent.
TrustWeaver is a trademark of TrustWeaver AB.

1. Identification

This Signature Validation Policy was issued by TrustWeaver AB (“TrustWeaver”) under the unique identifier 1.2.752.76.1.199.699.1.10.

TrustWeaver's contact information is:

TrustWeaver AB
Kungsgatan 27
SE-111 56 Stockholm
Sweden

Telephone: +46 8 41 005 790

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

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

2. Validity

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

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

3. Field of application and commitment types

This Signature Validation Policy includes rules for validation of electronic signatures or seals on business documents.

For purposes of this 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 to use the signature validation service.

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

Validation data created under this 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 Signature Validation Policy.

Copyright (c) 2016 TrustWeaver AB. All rights reserved.

TrustWeaver will under this TrustWeaver Signature Validation Policy validate all signatures that are correctly supplied to the validation service by the Verifier.

TrustWeaver shall take all necessary steps to ensure that the confidentiality of business data that is submitted in conjunction with validation requests under this TrustWeaver Signature Validation 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 Validation Policy.

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

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

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

The TrustWeaver 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 TrustWeaver Signature Validation 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.

TrustWeaver Signature Validation Service validation process of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that:

- the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature;
- the qualified certificate was issued by a qualified trusted Certificate Authority and was valid at the time of signing;
- the signature validation data corresponds to the data provided to the relying party;
- the unique set of data representing the signatory in the certificate is correctly provided to the relying party;

Copyright (c) 2016 TrustWeaver AB. All rights reserved.

- the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;
- the electronic signature was created by a qualified electronic signature creation device;
- the integrity of the signed data has not been compromised.

TrustWeaver Signature Validation Service used for validating the electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.

Validation under this TrustWeaver Signature Validation Policy shall include at a minimum the following cryptographic 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 validation data consists of CA-certificate chains and revocation data.
- 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 TrustWeaver Signature Validation Policy shall be extended with a number of unsigned attributes that proves successful validation, and/or a validation report shall be returned. The validation report may be signed where required by applicable jurisdictions.

Signatures which have not been successfully validated do not contain any such attributes, and no validation report will be returned.

Copyright (c) 2016 TrustWeaver AB. All rights reserved.