Qualified Electronic Signatures Act (SFS 2000:832)

The following is hereby enacted1

Introductory provision

§ 1 The purpose of this Act is to facilitate the use of electronic signatures, through provisions regarding secure signature creation devices, qualified certificates for electronic signatures, and the issuance of these certificates.

The Act applies to certificate providers that are established in Sweden, and issue qualified certificates to the public.

Definitions

§ 2 For the purposes of this Act the following definitions apply: *Electronic signature*: data in electronic form attached to or logically associated with other electronic data, and used to verify that the content originates from the alleged issuer, and has not been altered.

Advanced electronic signature: an electronic signature that

a) is uniquely linked to a signatory,
b) is capable of identifying the signatory,
c) is created using means that are under the signatory's sole control, and
d) is linked to other electronic data in such a way that any alteration to the said data can be detected.

Qualified electronic signature: an advanced electronic signature based on a qualified certificate and created by a secure signature creation device.

Signatory: a natural person who is authorised to control a signature creation device.

Signature creation data: unique data, such as codes or secret cryptographic keys, used to create an electronic signature.

Signature creation device: software or hardware used to implement the signature creation data.

Secure signature creation device: a signature creation device that meets the requirements set forth in § 3.

Signature verification data: data, such as codes or open cryptographic keys, used to verify an electronic signature.

Certificate: an attestation in electronic form that links signature verification data to a signatory and confirms the said signatory's identity.

Qualified certificate: a certificate that complies with the requirements set forth in § 6 or 7.

Certificate provider: the legal or natural person who issues certificates or who guarantees that the certificate of others complies with certain requirements.

Secure signature creation devices

§ 3 A signature creation device declared to be secure must ensure that the signature is satisfactorily protected against forgery. The device shall further ensure that the signature creation data

1. can practically occur only once,
2. cannot be derived by reasonable means, and
3. can be satisfactorily protected by the legitimate signatory against use or access by others.

A secure signature creation device may not alter the data to be signed electronically, or prevent the data from being presented to the signatory prior to the signature process.

§ 4 The requirements relating to secure signature creation devices set forth in § 3, shall be deemed to be satisfied by hardware or software devices that comply with the standards for electronic signature products, the reference numbers of which have been established by the Commission of the European Communities and published in the Official Journal of the European Communities.

§ 5 A device declared a secure signature creation device may be released onto the market or used to create a qualified electronic signature only if it meets the requirements set forth in § 3. The determination of whether these requirements have been fulfilled shall be made by a body designated for that purpose, pursuant to the Technical Conformity Assessment Act (1992:1119).

A determination by a body designated for the same purpose by another State belonging to the European Economic Area shall be deemed the equivalent of a determination pursuant to the first clause of this section.

Qualified certificates

§ 6. In order to be called a qualified certificate, a certificate shall be issued for a specific period of validity by a certificate provider that meets the requirements set forth in §§ 9–12, and any regulations issued under § 13, and shall contain:

1. an indication that the certificate has been issued as a qualified certificate,
2. the name and address of the certificate provider, and information regarding the state in which it is established,
3. the name of the signatory, or a pseudonym which shall be identified as such,

4. special information regarding the signatory if that information is relevant to the purpose for which the certificate is intended,
5. signature verification data that corresponds to the signature creation data under the control of the signatory at the time of issue,
6. information regarding the period of validity of the certificate,
7. the identity code of the certificate,
8. the advanced electronic signature of the certificate provider, or an electronic signature with an equivalent level of security, and
9. an indication of any limitations on the use of the certificate, or of any limits on the value of transactions for which the certificate can be used (transaction limit).

More detailed provisions regarding requirements pursuant to the first clause of this section may be issued by the Government or by supervisory body acting pursuant to Government authority.

§ 7 If a certificate satisfying the requirements of points 1-9 of the first clause of § 6 has been issued by a certificate provider not established in Sweden, the certificate shall be deemed to be qualified provided that:

1. The certificate provider is established in another state within the European Economic Area, and is permitted to issue qualified certificates there,
2. The certificate provider satisfies requirements equivalent to those contained in §§ 9-12 and the regulations issued under § 13, and is accredited in another state belonging to the European Economic Area, or
3. The certificate is guaranteed as being qualified by a certificate provider referred to in point 1 or the first clause of § 6.

Issuance of qualified certificates

§ 8 A certificate provider intending to issue qualified certificates to the public is required to notify the authority designated by the Government (the supervisory authority), before beginning these operations.

§ 9 A certificate provider that issues qualified certificates to the public shall conduct its operations in a reliable manner, and shall:

1. employ personnel who possess the expert knowledge and experience required for these operations, especially with regard to management, technology and security procedures,
2. apply such administrative and management routines that conform to recognised standards,
3. use trustworthy systems and products that are protected against modification and which ensure technical and cryptographic security,
4. maintain sufficient financial resources to conduct its operations in accordance with the provisions set forth in this Act, and bear the risk of liability for damages,
5. have secure routines to verify the identity of those signatories to whom qualified certificates are issued,

6. maintain a prompt and secure system for the registration and immediate revocation of qualified certificates, and
7. take measures against forgery of qualified certificates and, where applicable, guarantee full confidentiality during the process of generating signature creation data.

The requirements contained in point 3 of the first clause shall be deemed to be satisfied by hardware or software devices that comply with the standards for electronic signature products, the reference numbers of which have been established by the Commission of the European Communities and published in the Official Journal of the European Communities.

§ 10 A certificate provider that issues qualified certificates to the public shall

1. immediately revoke a certificate at the request of the signatory, or where there are other grounds for doing so,
2. ensure that the date and time when the certificate is issued or revoked can be determined precisely, and
3. ensure that the signature creation data and the signature verification data generated by the certificate provider can be used in a co-ordinated manner.

§ 11 A certificate provider that issues qualified certificates to the public must keep a record of all relevant information concerning the certificates for a reasonable period, depending on the type of certificate and other circumstances. The certificate provider must also employ trustworthy systems to store qualified certificates in verifiable form, so that

1. only authorised persons can make additions and changes,
2. the authenticity of the information can be verified,
3. the certificates are publicly available for review only with the consent of the certificate holder, and
4. any technical changes that may compromise these security requirements are apparent to the operator.

The certificate provider may not store or copy signature creation data.

§ 12 Before entering into a contract regarding the issuance of a qualified certificate, the certificate provider shall inform the party seeking the certificate in writing and in readily understandable language regarding

1. limitations and other conditions for the use of the certificate,
2. the existence of a voluntary accreditation or certification scheme pursuant to the Technical Conformity Assessment Act (1992:1119), and
3. procedures for complaints and dispute settlements.

The information indicated in the first clause may be transmitted electronically.

The information shall also be made available on request to others that depend on the certificate.

§ 13 More detailed regulations regarding the requirements pursuant to §§ 9- 12 may be issued by the Government or by the supervisory body acting under Government authorisation.

Damages

§ 14 A certificate provider issuing certificates declared to be qualified to the public , is liable for damages for any injury or loss caused to anyone relying on such a certificate, due to:

1. the certificate provider not having fulfilled the requirements set forth in § 10,
2. the certificate provider not having fulfilled the requirements set forth in the first clause of § 6, or
3. the certificate, when issued, having contained incorrect information.

The certificate provider, however, is not liable to pay damages if the provider can show that the injury or loss was not caused by the negligence of the certificate provider. Neither is the certificate provider liable for damages for an injury or loss arising from the use of a qualified certificate in violation of those limitations of use or the transaction limit clearly stated in the certificate.

The provisions set forth in points 2 and 3 of the first clause and in the second clause apply also to a certificate provider that guarantees that the certificates of another certificate provider are qualified.

§ 15 Contractual terms that are to the detriment of the party relying on the certificate, pursuant to the provisions of § 14, shall not apply to that party.

Processing of personal data

§ 16 A certificate provider that issues certificates to the public may collect personal data only directly from the data subject, or with the latter's explicit consent, and only insofar as it is necessary for the purposes of issuing or maintaining the certificate. The data may not be collected or processed for any other purposes without the explicit consent of the data subject.

Qualified electronic signatures

§ 17 If a requirement of a handwritten signature or its equivalent, contained in a law or regulation may be satisfied by electronic means, a qualified electronic signature shall be deemed to fulfil this requirement. However, in communication with or between government authorities, the use of electronic signatures may be subject to additional requirements.

Supervision

§ 18 The supervisory authority shall supervise the compliance with this Act and the regulations issued based on this Act.

The supervisory authority shall also keep and make public a list of the certificate providers that have provided notification pursuant to § 8, and that issue qualified certificates pursuant to this Act.

§ 19 The supervisory authority is entitled to receive, upon request, the information and documents needed in order to conduct its supervision.

The supervisory authority is entitled to obtain access to such areas, premises and other spaces, with the exception of dwellings, where activities subject to supervision are carried on.

The supervisory authority is entitled to obtain the assistance of the enforcement service regarding its supervision pursuant to the first and second clauses of this section.

§ 20 The supervisory authority may issue the injunctions and prohibitions required to ensure compliance with this Act, or with regulations issued pursuant to this Act.

The supervisory authority may order a certificate provider that issues certificates to be qualified to the public and declares them to be qualified, to completely or partially cease its activities, provided less far reaching measures have proven to be ineffective. The authority may decide how the operation shall be concluded.

§ 21 Directions and prohibitions issued under this Act may be subject to conditional fines.

Charges

§ 22 The Government, or the supervisory authority, if so authorised by the Government, may issue regulations concerning the liability for certificate providers issuing qualified certificates to the public to pay charges for the operation of the supervisory authority under this Act.

Appeals

§ 23 Decisions by the supervisory authority under this Act, or pursuant to regulations issued under it, may be appealed to the administrative courts.

Appeals to the Administrative Court of Appeal may not be made without leave to appeal.

The supervisory authority may decide that its decisions shall go into effect immediately.