

Act of 15 June 2001 No. 81
relating to electronic signature
(Electronic Signature Act)

Last updated by Act of 20 December 2002 No.110, entered into force on 1 January 2003.

(Unofficial translation. NPT is without any responsibility of any mistakes. All use of this translation is the sole responsibility of the user.)

Chapter I General rules

§ 1 Purpose of the Act

This Act concerns arrangements for the secure and effective use of electronic signatures. It lays down requirements for qualified certificates, for the issuers of such certificates and for secure signature creation devices.

§ 2 Scope and extent of the Act

This Act applies to issuers of certificates who are established in Norway. With the exception of § 6 second sub-paragraph and § 7, which apply to all electronic signatures, the conditions laid down are general conditions for the use of qualified electronic signatures.

The King may issue regulations providing that the Act shall apply to Svalbard and Jan Mayen.

§ 3 Definitions

For the purposes of this Act:

1. *electronic signature* means data in electronic form which are attached to other electronic data and which serve as a method of authentication;
2. *advanced electronic signature* means an electronic signature which
 - a. is uniquely linked to the signatory;
 - b. is capable of identifying the signatory;
 - c. is created using means over which the signatory has sole control, and
 - d. is linked to other electronic data in such a manner that any change in those data after signature is detectable;
3. *qualified electronic signature* means an advanced electronic signature based on a qualified certificate and created by an approved secure signature creation device;
4. *signatory* means a person who holds a signature creation device and acts either on his own behalf or on behalf of another natural or legal person;

5. *signature creation data* means unique data, such as codes or private keys, which are used by the signatory to create an electronic signature;

6. *signature creation device* means software or hardware used to create electronic signatures with the help of signature creation data;

7. *signature verification data* means unique data such as codes or public keys which are used to verify an electronic signature;

8. *signature verification device* means software or hardware used to verify electronic signatures with the help of signature verification data;

9. *certificate* means a link between signature verification data and the signatory which confirms the signatory's identity and is signed by the issuer of the certificate;

10. *certificate issuer* means a natural or legal person who issues certificates or offers other services related to electronic signatures.

§ 4 *Qualified certificate*

The term "qualified certificate" shall be used solely in respect of certificates which meet the requirements of this section and are issued for a limited period by a certificate issuer who meets the requirements in §§ 10 - 15.

A qualified certificate shall contain the following information:

- a) an indication that the certificate is issued as a qualified certificate;
- b) the identity of the certificate issuer and the State in which he is established;
- c) the name of the signatory or his pseudonym with the information that it is a pseudonym;
- d) any further information on the signatory which may be relevant to use of the certificate;
- e) signature verification data which correspond to the signature creation data under the control of the signatory;
- f) an indication of the beginning and end of the period of validity of the certificate;
- g) the identification code of the certificate;
- h) the advanced electronic signature of the certificate issuer;
- i) limitations on use of the certificate, if applicable, and
- j) limits on the value of transactions for which the certificate can be used, if applicable.

Further details of the content of qualified certificates may be given in regulations prescribed by the King.

§ 5 *Requirements for qualified electronic signatures used in communications with and within the public sector*

The King may lay down more detailed rules on the requirements which shall be made of qualified electronic signatures to be used in communications with and within the public sector.

§ 6 Legal effects of electronic signatures

If, in a law or regulation or in any other manner, a requirement is laid down for signatures in order to obtain a specific legal effect, and the provision may be implemented electronically, a qualified electronic signature shall in every case meet such a requirement. An electronic signature which is not qualified may meet such a requirement.

§ 7 Collection and use of personal data

A certificate issuer may only collect personal data directly from the person to whom the data refer or with his express consent, and only to the extent necessary for the issue or maintenance of a certificate. The data may not be collected in or processed for other purposes unless the person to whom the data apply has given his express consent to this.

The Data Inspectorate shall supervise compliance with this provision. The provisions of the Personal Data Act §§42-47 with regulations apply insofar as they are appropriate regarding the Data Inspectorates supervision.

Chapter II Secure signature creation devices

§ 8 Requirements for secure signature creation devices

A secure signature creation device shall ensure that the signature is protected against forgery in a satisfactory manner. A secure signature creation device shall also ensure that signature creation data:

- a) in practice can occur only once and that their secrecy is reasonably assured;
- b) cannot reasonably be derived, and
- c) can be reliably protected by the legitimate signatory against use by others.

A secure signature creation device may not alter data in electronic form which are to be signed or prevent the data from being presented to the signatory before being signed.

§ 9 Approval of secure signature creation devices

Approval as a secure signature creation device, cf. § 8, is given by the body appointed by the King. The King may in regulations lay down more detailed provisions on that body and on requirements for secure signature creation devices.

Approval from a corresponding body in another State which is a party to the EEA Agreement shall be considered equivalent to approval under the above paragraph.

The requirements in § 8 shall be considered to have been met when the hardware or software used conforms to the standards for electronic signature products which the European Commission lays down and which are published in the Official Journal of the European Communities.

Chapter III Requirements for issuers of qualified certificates

§ 10 Requirements applying to activity

Issuers of qualified certificates shall carry out and manage their activities in a responsible manner so that they can provide secure, reliable and efficient certification services.

Certificate issuers shall at any time have sufficient financial resources to enable them to operate in accordance with the requirements laid down in or pursuant to this Act.

§ 11 Requirements for products and devices

Issuers of qualified certificates shall use reliable products and devices which are protected against alteration and which provide technical and cryptographic security in supporting processes.

The requirements set out in the above paragraph shall be considered to have been met if certificate issuers use products and devices which are approved by a body in accordance with § 9 first and second paragraphs or comply with standards laid down by the European Commission under § 9 third paragraph.

Certificate issuers shall take steps to guard against the forgery of certificates. If issuers create signature creation data, they shall guarantee the confidentiality of those data during the creation process.

§ 12 Requirements for directory and withdrawal services

Issuers of qualified certificates shall ensure the operation of a prompt and secure directory and withdrawal service and shall ensure that it is possible to determine the date and time when a certificate becomes valid or is withdrawn.

§ 13 Requirements for checks on the identity of signatories

Issuers of qualified certificates are responsible for ensuring that the identity of signatories and other relevant data on signatories are checked by means of secure routines.

Information on the routines referred to in the above paragraph shall be publicly accessible.

§ 14 Requirements for the storage of information

Issuers of qualified certificates shall store all relevant information on qualified certificates for a reasonable period, and for not less than ten years after the certificate has been registered on the withdrawal list.

Issuers of certificates shall use reliable devices for the storage of certificates in verifiable form, such that

- a) the authenticity of the information may be checked;
- b) the certificates are publicly accessible only in cases where the holder has given his consent, and

c) any technical changes compromising these security requirements are apparent to the operator.

Issuers of qualified certificates may not store or copy the signatory's signature creation data.

§ 15 Requirements for information on conditions, limitations and the like

Before the issuer of a certificate enters into an agreement to issue a qualified certificate, he shall inform the other party in writing of

- a. the conditions and limitations on use of the certificate;
- b. any voluntary accreditation or certification schemes, and
- c. procedures for complaints and the settlement of disputes.

Information under the above paragraph may be sent electronically provided it is sent in a form which is directly readable by the other party. It must also be possible for this information to be checked by the recipient of the signature.

§ 16 Additional requirements

More detailed rules on which requirements may be laid down for issuers of qualified certificates in order to comply with the provisions in §§ 10-15 may be given in regulations prescribed by the King.

Chapter IV Supervision and sanctions

§ 17 Supervision of issuers of qualified certificates

The King may designate a body to supervise compliance with this Act and regulations.

The supervisory body may demand the information and documents it needs to carry out its tasks and may fix a deadline for sending them in .

The supervisory body may order that any circumstances which conflict with provisions issued in or pursuant to this Act shall cease and may lay down conditions which must be fulfilled to ensure that the activity in question complies with the law.

The supervisory body may require an IT audit to be carried out at the premises of issuers of qualified certificates and may appoint an auditor to carry out that audit. Issuers may be required to pay for the audit.

The supervisory body may deprive a certificate issuer of the right to use the designation "qualified certificate" if the issuer seriously or repeatedly fails to comply with the rules laid down in the Act.

The King may issue more detailed regulations on the activity of the supervisory body.

§ 18 *Registration of issuers of qualified certificates*

A certificate issuer may not issue qualified certificates before notification of registration has been sent to the supervisory body. Changes in information already registered and new information to be registered shall be reported to the supervisory body without undue delay.

§19 *Access to premises, etc*

In connection with the checks it makes, the supervisory body may demand access to premises where the activity being supervised is carried out.

The supervisory body may carry out any checks it considers necessary and require any assistance from staff on the spot which may be necessary to enable the checks to be carried out.

§15 of the Act of 10 February 1967 relating to procedure in cases concerning the public administration, which relates to practices to be observed during investigations, shall apply.

§ 20 *Coercive fine*

In order to ensure that provisions issued in or pursuant to this Act are observed, the supervisory body may rule that certificate issuers shall pay a continuous daily fine to the State until the activity which contravenes the law has ceased or orders and conditions laid down under this Act are observed

The fine shall not be due before the deadline for appeals has expired. If an appeal is lodged against the decision relating to a coercive fine, no fine shall be due before the appeal has been heard unless the appeal body decides otherwise.

The supervisory body may waive a fine incurred.

§ 21 *Penalties*

Anyone who wilfully or with gross negligence

- a) fails to register/send in the notification referred to in § 18;
- b) fails to supply the information referred to in § 17;
- c) processes personal information in contravention of §§ 7 and 14, or
- d) gives incorrect or misleading information to the supervisory body

shall be fined.

Complicity shall be punished in the same manner.

§ 22 *Compensation*

Issuers who issue certificates stated to be qualified or who guarantee such certificates issued by another issuer are liable for damage caused to any natural or legal person who had had reasonable grounds for relying on:

- a) the accuracy at the time of issue of the information given on the certificate;
- b) the certificate's containing all the information required under § 4;
- c) the signature creation data and signature verification data belonging together in unique manner provided that the certificate issuer creates them both;
- d) the signatory's holding correct signature creation data at the time when the certificate was issued, or
- e) the certificate's being recorded on the withdrawal list, cf. § 12.

Certificate issuers are liable under the above paragraph unless they establish that they or the person for whom they are standing as guarantor have not acted negligently.

Certificate issuers are not liable for damage caused by use of the certificate in contravention of clear limitations on its use, or use in connection with values exceeding limits.

§ 23 Appeals

Appeals may be lodged with the body appointed by the King against decisions made by the supervisory body or provisions laid down in or pursuant to this Act.

§ 24 Fees

The King may in regulations provide that certificate issuers liable for registration under § 18 shall pay a fee. Fees may not exceed the costs of the activity of the supervisory body.

Chapter V International aspects

§ 25 Legal recognition of qualified certificates from issuers established outside Norway

Certificates from issuers established within the EEA shall be considered as qualified certificates under this Act provided that they meet the requirements for qualified certificates in the country in which the issuer is established.

Qualified certificates from issuers established in a country outside the EEA shall be granted legal recognition on a par with qualified certificates from issuers within the EEA, provided that:

- a. the issuer fulfils the requirements laid down in a EEA state and has been approved under a voluntary approval scheme in that state;
- b. a certificate issuer who is established within the EEA and who meets the requirements in this state in which the issuer is established stands guarantor for the issuer, or
- c. the certificate or the issuer is recognised under multilateral or bilateral agreements between Norway, the EU, third countries or international organisations.

Chapter VI Entry into force and transition rules

§ 26 Entry into force

This Act comes into force on the date determined by the King.

§ 27 Transition rules

Issuers of qualified certificates shall, within six months of entry into force of this Act, register in accordance with § 18 or, by the same deadline, cease to call the certificates qualified or use a designation which gives the impression that they are qualified.