LEGISLATION TRANSLATION

9 JULY 2001
LAW DETERMINING SOME RULES CONCERNING THE LEGAL FRAMEWORK OF ELECTRONIC SIGNATURES AND CERTIFICATION SERVICES

UNOFFICIAL ENGLISH TRANSLATION – CONSOLIDATED VERSION[1]

By **Johan Vandendriessche**[2]

Albert II, King of Belgians,

To all those who are and will be, Our Salute,

Parliament has adopted and We enact what follows:

CHAPTER I. – *General provision*

Article 1. This law regulates a matter under article 78 of the Belgian Constitution.

CHAPTER II. – *Definitions and field of application of this law*

Part 1. – Definitions

Art. 2. This law implements Directive 1999/93/EC of the European Parliament and of

the Council of 13 December 1999 on a Community framework for electronic

signatures.

For the purposes of this law and the decrees providing for its enforcement,

1° "electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.

2° "advanced electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication and which meets the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using means that the signatory can maintain under his sole control;

(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

3° "certificate" means an electronic attestation, which links signature-verification data to a natural or legal person and confirms the identity of that person;

1 *This version is consolidated to 30 March 2012. Bibliographical information can be found at the end of this document.*

2 *The author will appreciate receiving comments or remarks in view of improving this translation at the following addresses: johan@adv-vandendriessche.be.*

4° "qualified certificate" means a certificate, which meets the requirements laid down in Annex I of this law and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II of this law;

5° "holder of a certificate" means a natural or legal person to whom a certification-service-provider has issued a certificate;

6° "signature-creation data" means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;

7° "secure-signature-creation device" means a signature-creation device, which meets the requirements laid down in Annex III of this law;

8° "signature-verification-data" means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an advanced electronic signature;

9° "signature-verification device" means configured software or hardware used to implement the signature-verification-data;

10° "certification-service-provider" means any legal or natural person who issues certificates or provides other services related to electronic signatures;

11° "electronic-signature product" means hardware or software, or relevant components thereof, which may be used by a certification-service-provider for the provision of electronic-signature services or may be used for the creation or verification of electronic signatures;

12° "Public Service" means the public service of the Ministry of Economic Affairs, charged with tasks related to the accreditation and supervision of certification-service-providers that are established in Belgium and authorised to issue qualified certificates;

13° "entity" means the institution that has proved its competence by the certificate delivered to it by the Belgian Accreditation System in correspondence with the Law of 20 July 1990 concerning the accreditation of certification and inspection institutions as well as test laboratories or by equivalent institutions established within the European Economic Area.

Part 2. – Field of application

Art. 3. This law provides rules concerning the legal framework of electronic

signatures and provides the legal status applicable to the activities of certification-service-providers as well as the obligations of these certification-service-providers, without prejudice to the legal rules concerning the representation of legal persons.

This law also introduces a voluntary accreditation system.

CHAPTER III. – *General principles*

Art. 4. § 1. Except if otherwise provided by law, no person can be forced to conclude legal acts by electronic means.

§2. The activities of a certification-service-provider are not subject to a prior authorisation.

Certification-service-providers delivering qualified certificates shall however, either within the month following the publication of this law or prior to the commencement of their activities inform the Public Service of:

- the name of the certification-service-provider;

- the geographical address at which the certification-service-provider is established;

- the contact details where the certification-service-provider can be easily reached, including the electronic mail address;

- if applicable, the profession, references and identification numbers (trade register, VAT) of the certification-service-provider;

- evidence that the certification-service-provider has taken an insurance to cover the liabilities under article 14;

The Public Service will provide a receipt within five working days following the communication.

§3. The King may impose, by Decree decided upon after deliberation in the Council of Ministers, additional requirements for the use of electronic signatures in the public sector. Such requirements shall be objective, transparent, proportional and nondiscriminating and shall relate only to the specific characteristics of the application concerned. Such requirements may not constitute an obstacle to cross-border services for citizens.

§4. Without prejudice to article 1323 and following of the Civil Code, an advanced electronic signature, realised by means of a qualified certificate and made by a secure-signature-creation device shall be assimilated with a written signature, irrespective of the fact of the signature being made by a natural person or a legal person.

§5. The legal effectiveness of an electronic signature and its admissibility as evidence in legal proceeding shall not be denied solely on the grounds that it is:

- in electronic form; or

- not based upon a qualified certificate; or

- not based upon a certificate issued by an accredited certification-service-provider;

or

- not created by a secure-signature-creation device.

§6. The signature of a holder of a certificate can be made manifest in an equivalent form that satisfies the requirements of article 2, §2, 2°.

Art. 5. § 1. Without prejudice to the law of 8 December 1992 on the protection of individuals with regard to the processing of personal data, a certification-service-provider issuing certificates destined for public use may only collect personal data directly with the person concerned or only collect personal data with explicit consent, provided this is necessary for the issuance and storing of the certificate. The data may not be collected or processed for other purposes without explicit consent of the person concerned.

§2. If the holder of the certificate uses a pseudonym and if the investigation requires it, the certification-service-provider shall provide all information concerning the identity of the holder of the certificate in the situations and under the conditions provided in article 90ter and 90decies of the Code of Criminal Procedure.

CHAPTER IV. – *Electronic-signature products*

Art. 6. If an electronic-signature product corresponds with the standards, of which the reference numbers are published in the *Official Journal of the European Union* in accordance with the procedure provided by Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, this product shall be considered as complying with the requirements of annex II, littera f), and annex III of this law.

Art. 7. § 1. The requirements concerning secure-signature-creation device are listed in Annex III of this law.

§ 2. The competent organisms, appointed by the Public Service, shall confirm the conformity of the secure-signature-creation devices with the requirements listed in Annex 3 of this law. The list of appointed organisms shall be transmitted to the European Commission.

§ 3. The King shall determine the requirements, which the abovementioned organisms must meet.

§ 4. The conformity determined by another organism, appointed by another Member State of the European Economic Area, shall be recognised in Belgium.

CHAPTER V. – *Certification-service-providers issuing qualified certificates*

Part 1. – Qualified certificates

Sub 1. – Tasks

Art. 8. § 1. The certification-service-provider shall investigate the complementarities of the data for the creation and the verification of the certificate prior to the issuance thereof.

§ 2. The certification-service-provider shall issue one or more certificates to any person requesting so, after he has verified the identity and, if applicable, the special attributes of that person.

§ 3. Concerning legal persons, the certification-service-provider shall keep a register with the identity and special attributes of the natural person that can represent the legal person and who use the signatures related to the certificate. The register shall be kept in such a manner that the identity of the natural person can be determined with each use of the signature.

Art. 9. The certification-service-provider shall provide a copy of the certificate to the candidate-holder of the certificate.

Art. 10. The certification-service-provider shall keep a register containing all certificates that he issues and their

expiry dates.

Sub 2. – Requirements concerning qualified certificates

Art. 11. § 1. The qualified certificates must meet the requirements listed in Annex I of this law.

§ 2. The certification-service-providers issuing qualified certificates must meet the requirements listed in Annex II of this law.

Sub 3. – Revocation of qualified certificates

Art. 12. § 2. The certification-service-provider will revoke the certificate immediately upon the request of an identified holder of a certificate.

§ 2. The certification-service-provider shall also revoke the certificate if:

1° serious indications exist to presume that the certificate was issued on the basis of wrong or falsified information, that the information contained in the certificate does no longer correspond to the reality or that the confidentiality of the information used to create the signature has been impaired;

2° the Courts ordered a measure set forth under article 20 § 4, b);

3° the certification-service-provider ceases its activities without them being taken over by another certification-service-provider offering equal quality and safety guarantees;

4° the certification-service-provider has been informed about the death of a natural person or the dissolution of the legal person that is holder of the certificate;

Except if the holder of the certificate is deceased, the certification-service-provider shall inform the holder of the certificate about the revocation of the certificate and shall motivate this decision. The certification-service-provider shall inform the holder of the certificate one month prior to the revocation.

§ 3. The revocation of a certificate is permanent.

Art. 13. § 1. The certification-service-provider shall take the necessary measures to be able to respond immediately and at any moment to a request to revoke a certificate.

§ 2. The certification-service-provider shall mention the revocation of a certificate in the electronic register mentioned in article 10 immediately after the decision thereof.

Sub 4. – The liability of certification-service-providers issuing qualified certificates

Art. 14. § 1. By issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:

a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;

b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;

c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both; unless the certification-service-provider proves that he has not acted negligently.

§ 2. A certification-service-provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the certification-service-provider proves that he has not acted negligently.

§ 3. A certification-service-provider may indicate in a qualified certificate limitations on the use of that certificate, provided that the limitations are recognisable to third parties. The certification-service-provider shall not be liable for damage arising from use of a qualified certificate, which exceeds the limitations placed on it.

§ 4. A certification-service-provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit

is recognisable to third parties. The certification-service-provider shall not be liable for damage resulting from this maximum limit being exceeded.

Sub 5. – Ceasing of the activities of certification-service-providers issuing qualified certificates

Art. 15. § 1. The certification-service-provider issuing qualified certificates shall notify the Public Service within a reasonable period of his intention to cease his activities as a qualified certification-service-provider, as well as of any decision, which may result in the ceasing of his activities. In that case, the certification-service-provider must ascertain whether or not its activities can be taken over by another certification-service-provider offering the same level of quality and security. If this is not possible, the certification-service-provider shall revoke the certification two months after the notification thereof to the holders of the certificate. In that case, the certification-service-provider shall take the necessary measures to comply with the obligations of Annex II, i).

§ 2. The certification-service-provider will immediately inform the Public Service when it ceases its activities for reasons independent of its will or bankruptcy. The certification-service provider shall take care to revoke the certificates and will take the necessary measures to meet the obligation under Annex II, i) of this law.

Sub 6. – Certificates issued as qualified certificates by foreign certification-service-providers

Art. 16. § 1. A qualified certificate, destined for public use, issued by a certification-service-provider established in a Member State of the European Economic Area shall be equivalent to the qualified certificates issued by a certification-service-provider established in Belgium.

§ 2. The qualified certificates, destined for public use, issued by a certification-service- provider established in a third country, shall be equivalent from a legal point of view to the qualified certificates issued by a certification-service-provider established in Belgium if:

a) the certification-service-providers meets the requirements of the national regulations implementing Directive 1999/93/EC of the European Parliament an of the Council of 13 December 1999 on a Community framework for electronic signatures and if it has been accredited on the basis of the voluntary accreditation system of a Member State of the European Economic Area; or

b) a certification-service-provider established in the European Community, meeting all requirements of the national regulations implementing Directive 1999/93/EC of the European Parliament an of the Council of 13 December 1999 on a Community framework for electronic signatures, guarantees the certificate; or

c) the certification-service-provider is recognised within the framework of bilateral or multilateral agreements between the European Community and third countries or international organisations.

Part 2. – Accredited certification-service-providers

Art. 17. § 1. Certification-service-providers that meet all requirements under Annex II, issue qualified certificates according to the requirements of Annex I and use secure-signature-creation devices according to the requirements of Annex III, may request the Public Service for an accreditation.

The accreditation foreseen by this law is the result of an evaluation, by the entity determined in article 2, 13°, of the conformity with the requirements under Annex I, II and III and, if applicable, with those requirements connected to other services and products delivered by certification-service-providers.

§ 2. The King shall determine the conditions referred to under § 1 and shall determine:

1° the procedure to award, suspend and retract the accreditation;

2° the charge owed to the "Fund for accreditation" for the issuance, management and control of the accreditation;

3° the period during which the demands can be investigated;

4° the rules for the control of certification-service-providers;

§ 3. The choice to use an accredited certification-service-provider shall be free.

Art. 18. The Public Service shall:

1° award the accreditations and retract them. This task is

subject to procedures and shall be executed by persons and services differing from those specified under article 20, §2;

2° coordinate the coherent and transparent application of the accreditation principles and procedures applicable under this law;

3° supervise the audit procedures of the entities specified under article 2, 13°), as well as the activities of these entities in the frame of the accreditation procedures;

4° transmit the following to the European Commission and to the countries of the European Economic Area:

a) the information concerning the voluntary accreditation systems elaborated under this law;

b) the name and the address of all certification-service-providers accredited under this law;

5° perform the notifications specified under article 11 of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for electronic signatures.

CHAPTER VI. - *Holders of a certificate*

Art. 19. § 1. As soon as the signature-creation data has been created, the holder of the certificate shall be solely responsible for the confidentiality of these data.

§ 2. If doubts exist concerning the confidentiality of the signature-creation data or if the data contained in the certificate do not any longer correspond to the reality, the holder of a certificate must have it revoked.

§ 3. If a certificate expires or if it is revoked, the holder of a certificate may no longer use the corresponding data to create a signature beyond the expiry date or the date of the revocation of the certificate for the purposes of signing this data or to let this data be certified by another certification-service-provider.

CHAPTER VII. - *Supervision and sanctions*

Art. 20. § 1. The King shall determine, by Royal Decree decided upon after deliberation in the Council of Ministers, the rules concerning the supervision of certification-service-providers, as well as the means of redress that can be applied by the Public Service.

§ 2. The Public Service shall be charged with the supervision of the certification-service- providers issuing qualified certificates to the public. Under the conditions determined by the King, the Public Service shall be competent to demand the certification-service-providers all information necessary to determine whether or not they respect this law.

§ 3. If the Public Service establishes that a certification-service-provider issuing qualified certificates does not respect this law, it shall inform the certification-service-provider thereof and shall determine a reasonable period during which the certification-service-provider must take all measures necessary to comply with this law.

§ 4. If the certification-service-provider did not take the necessary measures within this period of time, the Public Service shall institute proceedings before Court in order to:

a) prohibit the certification-service-provider from issuing qualified certificates, and

b) to order the certification-service-provider to inform the holders of the qualified certificates issued by this certification-service-provider, that these certificates do no longer comply with the conditions of this law.

5° If the certification-service-provider accredited under article 17 of this law did not regularise the situation within the abovementioned period of time, the Public Service shall revoke its accreditation.

The certification-service-provider shall, without any delay, mention the revocation of the accreditation in its electronic register and inform the holders of the certificate thereof without any delay.

Art. 21. § 1. Whomever falsely assumes the quality of accredited certification-service-provider shall be punishable with an imprisonment of 8 days up until 3 months and with an fine of [5000] up to [50000] [Euros], or with one of these punishments alone.

§ 2. Upon conviction on the ground of the offence mentioned under paragraph 1, the competent court may order the full or partial publication of the judgment in one or more journals, under the conditions it sets forth and on the costs of the convicted party.

Promulgate this law, order that it be dressed with the

country's seal and published in the Belgian State Gazette.

Brussels, 9 July 2001

ALBERT

On behalf of the King:

The Minister of Economic Affairs

Ch. PICQUE

The Minister of Justice

M. VERWILGHEN

The Minister of Telecommunication, and State Companies and Participations

R. DAEMS

Dressed with the country's seal:

The Minister of Justice

M. VERWILGHEN

___

Notes

(1) Chamber of Representatives

Ordinary session 1999-2000.

Parliamentary documents. – Draft law n° 322/1

Parliamentary session 2000-2001.

Parliamentary documents. – Amendment n° 322/2 – Report n° 322/3 – Text adopted by the Commission for Enterprises, Scientific policy, Education, National scientific and cultural institutes, commerce and agriculture n° 322/4 – Text adopted in Plenary Session and transmitted to the Senate n° 322/6 – Report n° 322/7 – Text adopted in Plenary Session and transmitted to the King to be enacted n° 322/8.

Acts of the Chamber of Representatives. – Full report: 15 February 2001 – Adoption:

14 June 2001.

Senate:

Ordinary Session 2000-2001.

Documents of the Senate. – Draft law transmitted by the Chamber of Representatives n° 2-662/1 – Amendments° 2-662/2 and 3 – Report n° 2-664/4 – Text amended by the Commission n° 2-664/5 – Amendments n° 2-664/6 – Text adopted in Plenary Session and transmitted to the Chamber of Representatives n° 2-664/7.

Acts of the Senate. – 17 May 2001

Formalities prescribed by Directive 98/34/EC

The formalities prescribed by Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations have been fulfilled (notification 2000/0050/B).

___

ANNEX I

Requirements for qualified certificates

Qualified certificates must contain:

a) an indication that the certificate is issued as a qualified certificate;

b) the identification of the certification-service-provider and the country in which it is established;

c) the name of the signatory or a pseudonym, which shall be identified as such;

d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;

e) signature-verification data which correspond to 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 identity code of the certificate;

h) the advanced electronic signature of the certification-service-provider issuing it;

i) limitations on the scope of use of the certificate, if

applicable; and

j) limits on the value of transactions for which the certificate can be used, if applicable.

___

ANNEX II

Requirements for certification-service-providers issuing qualified certificates

Certification-service-providers must:

a) demonstrate the reliability necessary for providing certification services;

b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;

c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;

d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;

e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognized standards;

f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;

g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;

h) maintain sufficient financial resources to operate in conformity with the requirements laid down in this law, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;

i) record all relevant information concerning a qualified certificate for a useful period of 30 years, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;

j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;

k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;

l) use trustworthy systems to store certificates in a verifiable form so that:

- only authorised persons can make entries and changes,

- information can be checked for authenticity,

- certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and

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

___

ANNEX III

Requirements for secure signature-creation devices

1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:

a) the signature-creation-data used for signature

generation can practically occur only once, and that their secrecy is reasonably assured;

b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;

c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.

2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

___

ANNEX IV

Recommendations for secure signature verification

During the signature-verification process it should be ensured with reasonable certainty that:

a) the data used for verifying the signature correspond to the data displayed to the verifier;

b) the signature is reliably verified and the result of that verification is correctly displayed;

c) the verifier can, as necessary, reliably establish the contents of the signed data;

d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified;

e) the result of verification and the signatory's identity are correctly displayed;

f) the use of a pseudonym is clearly indicated; and

g) any security-relevant changes can be detected.

Bibliographical information[3]

Act of 9 July 2001 determining some rules concerning the legal framework of electronic signatures and certification services (Belgian State Gazette of 29 September 2001).

Act of 13 December 2010 modifying the Act of 21 March 1991 on the reform of some economic public companies, the Act of 17 January 2003 on the legal status of the regulatory authority of the Belgian postal and telecommunications sector and modifying the Act of 9 July 2001 determining some rules concerning the legal framework of electronic signatures and certification services (Belgian State Gazette of 31 December 2010).

Act of 31 May 2011 on several provisions in relation to telecommunications (Belgian State Gazette of 21 June 2011).[4]

Act of 15 February 2012 modifying the Act of 9 July 2001 determining some rules concerning the legal framework of electronic signatures and certification services (Belgian State Gazette of 7 March 2012).

Johan Vandendriessche is a member of the editorial board and a lawyer at the Bar of Leuven.

http://www.adv-vandendriessche.be/

3 *This chapter provides an overview of the acts that are incorporated in this consolidated version. Reference is made to the official title of the act and its publication date.*

4 *This Act repeals, before their entry into effect, the modifications that were made by the abovementioned Act of 13 December 2010 to the original Act of 9 July 2001 determining some rules concerning the legal framework of electronic signatures and certification services. Consequently, the original text remains applicable.*

