

DECISION no. 1259/13.12.2001 regarding the approval of the Technical and Methodological norms for applying the Law no. [455/2001](#) on the Electronic Signature

Considering the provisions stated in art. 107, of the Romanian Constitution, as well as in art. 52 of the Law no. [455/2001](#) on the Electronic Signature,

The Government of Romania passes the decision hereby.

Sole article. - The Technical and methodological norms for applying the Law no. [455/2001](#) on the Electronic Signature, stipulated in the annex which makes integrant part of this decision are hereby approved.

PRIME-MINISTER

ADRIAN NĂSTASE

Countersigns:

Minister of Communications and Information Technology,

Dan Nica

Minister of the Public Finances,

Mihai Nicolae Tănăsescu

ANNEX

TECHNICAL AND METHODOLOGICAL NORMS for applying the Law no. [455/2001](#) on the Electronic Signature

Published in the Official Gazette of Romania no. 847/28.12.2001

TECHNICAL AND METHODOLOGICAL NORMS dated on 13.12.2001 for the approval of the Law no. [455/2001](#) on the Electronic Signature

CHAPTER I: General Provisions

Art. 1

Any person, either natural or legal, located on the Romanian territory can benefit from certification services in order to make use of the electronic signature, on the grounds of the Law no. [455/2001](#) on the electronic signature, hereinafter designated as the Law.

Art. 2

(1) For the purpose of the technical and methodological norms hereby, the terms used have the following definitions:

a) client – the beneficiary of the certification services, who, on the grounds of a contract concluded with a certification services provider, hereinafter designated the Provider, possesses a functional pair public key-private key and has an identity proved by means of a digital certificate issued by that provider;

b) hash-code – function that returns the fingerprint of an electronic document;

c) private key – a digital code possessing a unique character, generated through a hardware device and/or a specialized software. In the context of the digital signature the private key represents the data for creating an electronic signature, as they appear defined by the Law;

d) public key – digital code, the private key pair necessary for verifying the electronic signature. In the context of the digital signature the public key represents the data for verifying the electronic signature, as they appear defined by the Law;

e) electronic signature creation mechanism – a hash-code function is applied on the document, thus obtaining the fingerprint of the document. The private key is applied over the fingerprint of the document by means of an algorithm, thus the electronic signature taking effect;

f) the mechanism for verifying the electronic signature is based on using the public key, the hash-code function and the received electronic signature. The verification of the signature is an automatic operation;

g) web page – electronic document, available on the internet.

(2) For the purpose of these norms, the abbreviations used have the following meanings:

a) ETSI – The European Telecommunications Standards Institute;

b) RFC – designates the documents that have been submitted to public analysis within a process coordinated by the Work Group for Internet Engineering;

c) FIPS – designates federal standards issued by the National Institute of Standards and Technology of the United States of America;

d) IEEE – the Institute of Electrical and Electronics Engineers;

e) ITSEC – designates the European standards and criteria for the assessment of the information systems security;

f) RSA – the encryption algorithm with public key, developed by the Rivest, Shamir and Adleman researchers;

g) DSA – The Digital Signature Algorithm;

h) SHA – The Secured Hash-code Algorithm;

i) PKI – Public Keys Infrastructure;

j) RTF – document format which enables the text alignment, the introduction of special characters, the usage of colours and fonts of various sizes, as well as the insertion of other objects;

k) PDF - format that enables the transfer of electronic documents without affecting the page layout; these type of documents can contain text, images and sounds;

l) PostScript – document format used particularly for printing using PostScript printing devices.

m) TXT - document format containing exclusively text

CHAPTER II: Regulation and Supervision Authority

Art. 3

(1) The regulation and supervision authority, designated hereinafter the Authority, generates or purchases a functional pair of private key-public key and must protect its private key, using a viable system and taking all necessary precautions to prevent loss, disclosure, modification or unauthorized use of its private key.

(2) The private key cannot be deduced by no means from its pair public key.

Art. 4

The Authority manages the Registry of the certification services providers, designated hereinafter the Registry

Art. 5

The informational content and the structure of the Registry are presented in the annex no.1.

Art. 6

(1) The update of the Registry is performed exclusively by the Authority and targets all the modifications occurred from the provider's status – accreditation, accreditation period expiry date, suspension, development of the types of certificates provided.

(2) Following each update, the Authority transmits the provider a copy of the document stipulated at item 43 of the annex no. 1.

Art. 7

The authority manages the data using an information system able to ensure the security of the communications systems, transactions and data under the established standards - ISO/IEC 15408-1, 2, 3 and ISO 17799. In this regard it is used a solution which ensures the management of a replicated data base, guaranteeing the permanent access via the Internet.

Art. 8

The Authority makes public, for consultation, the following data from the registry:

- a) type of provider – natural or legal person;
- b) name or designation of the provider;
- c) date when it started the activity;
- d) provider's public key;
- e) indications regarding the accreditation – accredited or unaccredited;
- f) accreditation period - start/end;
- g) indications regarding the right of issuing qualified certificates
- h) description of the provider's general policy;
- i) provider's organization type – trade company, autonomous directorate, public institution, non-governmental organisation, other types;
- j) address or headquarters - country, city, county/district, street number, block of flats, wing, apartment, postal code;
- k) nationality, for legal person;
- l) citizenship, for natural person;

- m) telephone, fax, e-mail, web page address;
- n) categories of services destined for the public: certificates type, instructions for use, for each type of certificate
- o) types of devices for creating the electronic signature used;
- p) status of the devices – homologated or not;
- q) status of the provider: operational, suspended, ceased activity, activity pending to be transferred, activity with authority identified problems pending for remedy, - indicating the deadline;
- r) provider's history: activity starting date, suspension periods, periods when it had the right to issue qualified certificates, other similar situations.

Art. 9

- (1) The information stipulated by art. 8 of these technical and methodological norms are available for the, on the Internet, in the Authority's web page.
- (2) The web page will contain information concerning the Law on the electronic signature, the technical and methodological norms regarding the applying of the law on the electronic signature, general information on the use of the electronic signature, new information in the field of the electronic signature, references to the certification services providers' web pages.
- (3) The Authority will permanently publish the Internet technologies which allow consulting the information stipulated at paragraph. (1) and (2).

CHAPTER III: Providers of Certification Services

SECTION 1: Shared Provisions

Art. 10

- (1) A provider is bound to generate or to purchase a functional pair of private key-public key and to protect its private key, using a viable system and taking the necessary precautions to prevent loss, disclosure, modification or unauthorized use of its private key.
- (2) The private key cannot be deduced by any means from its pair public key.

Art. 11

(1) Before starting the activity the provider will notify the Authority, in accordance with the form stipulated by annex no. 2.

(2) All data will be submitted to the Authority on hard and electronic copy, the electronic document being digitally signed by the provider and submitted in one of the following formats: RTF, PDF, TXT and PostScript.

Art. 12

(1) The registration in the Registry will be made based on an individual request.

(2) Upon the receipt of the request the Authority includes the provider's data into the Registry and generates for him an identification code comprising the activity starting year, month and date as well as the provider's running number.

SECTION 2: Provision of the Qualified Certification Services

Art. 13

(1) The provider can offer certification services based on simple and qualified certificates.

(2) The qualified certificate will have the structure in accordance with the annex no. 3, under ETSI TS 101 862 v. 1.2.1. (2001-06), RFC 2459, and with the Recommendations ITU-T X. 509.

(3) The Authority will publish the possible modifications of the described format, based on the evolution of the technologies or of the internationally recognized norms in field.

(4) The certificate also has an extension section. The list of the most commonly used extensions is provided in the annex no. 4.

(5) The identification code of the qualified certificate is made by linking the provider's identification code to the running number of the certificate.

(6) The personal identification code of the subscriber results by linking the provider's identification code, the initials of the subscriber's name or pseudonym and its running number in the list of clients with the same initials.

Art. 14

(1) In order to issue qualified certificates, the provider has to observe the requirements stipulated by art. 20-22 of the Law.

(2) The provider has to prove to the Authority that they possess the financial resources to cover any damages that may be caused while developing the certification activity, and have to be able to cover any losses undergone by a person whose behavior is based on the legal effects of the qualified certificates, amounting to the equivalent in lei of the sum of 10,000 euro for each ensured risk. The ensured risk represents each type of damage produced, even if more such damages are produced as a consequence of the provider's non-observance of an obligation stipulated by the Law. The provider will have to submit a letter of guarantee issued by a specialized financial institution or an insurance policy with an insurance company, for the authority, with at least an equal value to the equivalent in lei of the amount of 500,000 euro; the letter of guarantee has to have a similar form to that provided in the annex no. 5.

(3) The provider has to ensure a security level of the systems, communications, transactions and data under the established standards - ISO/IEC 15408-1,2,3; ISO 17799; ETSI TS 101 456 v.1.1.1. (2000-12); ITSEC-E3 FIPS 140-1.

(4) The provider has to ensure fast operation of the certificates registry, in accordance with the art. 20 letter b) of the Law; the registry's structure is shown in the annex no. 6.

(5) The provider has to use only secured devices for creating the electronic signature.

(6) The Authority verifies the data contained by the submitted documentation, within maximum 10 days, in relation to the established standards and to the technical and methodological norms hereby.

(7) The Authority has to inform the provider within maximum 10 days, regarding the observance of the requirements and, if the case may be, to supplement documentation.

(8) In case all criteria are observed, the Authority issues the decision upon which the provider acquires the right to provide qualified certification services and updates the registry noting the new status of the provider. The decision is communicated to the provider on hard and electronic copy, digitally signed by the Authority.

(9) Should the documentation be unfilled in properly or not accomplishing the requirements, the Authority issues a motivated decision by means of which it rejects the request of the provider of being granted the right to provide qualified certification services. The decision is communicated to the provider on hard and electronic copy, digitally signed by the Authority.

Art. 15

In case that the requirements stipulated by art. 20-22 of the Law are no longer observed, the Authority will decide to suspend the right of the respective provider to issue qualified certificates, until the remedy of the shortcomings and fulfillment of all legal requirements. The decision is communicated to the provider on hard and electronic copy, digitally signed by the Authority.

SECTION 3: Voluntary Accreditation

Art. 16

- (1) The provider who wishes to develop the activity as an accredited provider has to require the obtaining of an accreditation from the Authority.
- (2) For this purpose, the provider has to fulfil all the necessary requirements regarding the issuing of qualified certificates and to use secured devices for generating the electronic signature, homologated by an Authority-agreed agency.
- (3) The verifications will be made both on the declarations contained in the documentation submitted to the Authority and on the consistenct among the systems, procedures and practices stated and the physically existing ones.
- (4) The audit is carried out by the Authority or by a third party assigned by the latter, in accordance with the European norms stated for this type of activity.
- (5) The Authority has to inform the provider within maximum 30 days about the requirements fulfillment and to require, if necessary, the filling-in of the documentation.

Art. 17

- (1) In case it is acknowledged that all criteria are achieved, the Authority decides the accreditation of the provider.
- (2) The accreditation decision, the conditions and the effects of the suspension or of the withdrawal are notified to the provider on hard and electronic copy, digitally signed by the Authority.
- (3) Upon the provider's request, the Authority updates the registry by inscribing the new status of the accredited provider. Information about guarantees, devices homologation and accreditation period are introduced.

Art. 18

- (1) The accreditation period is of 3 years and can be renewed.
- (2) The renewal procedure is identical to the procedure for obtaining the accreditation.

Art. 19

The accreditation decision will be suspended if the following cases occur:

- a) it is acknowledged that the provider no longer fulfils one or more of the requirements stipulated for being granted the accreditation decision. In this case the Authority notifies

the provider and establishes a period of maximum 30 days in which the provider has to remedy the notified deficiencies;

b) launch of the provider's bankruptcy procedure.

Art. 20

The Authority withdraws the accreditation decision if the following cases occur:

a) if the provider does not remedy the deficiencies stipulated by the art. 19, letter a), within the deadline granted by the Authority;

b) if there occurs a final and revocable legal adjudgment which states the provider's bankruptcy.

SECTION 4: Agreement of the Homologation Agents

Art. 21

(1) The decision of accepting the homologation agents is taken based on the request of the agency submitted to the Authority and following the verification of the requirements stipulated by the European norms for this type of activity.

(2) The acceptance decision is valid for 1 year and can be renewed.

(3) The decision is withdrawn in case it is acknowledged that the agency no longer fulfils the requirements stipulated by paragraph (1) and (2). The Authority transmits an explanatory note to the agency describing the reasons for withdrawing the acceptance decision.

CHAPTER IV: Usage procedures of the electronic signature

Art. 22

The functioning principle and the usage procedures of the electronic signature are provided in the annex no. 7.

Art. 23

Any individual or legal person who expresses their wish to be issued a certificate by a provider, have to:

a) provide the required information for the desired type of certificate, in accordance with the form mentioned in the annex no. 8;

b) generate or purchase a functional pair private key-public key; the private key cannot be deduced in any manner from its pair public key

c) prove the functionality of the private key-public key pair;

d) protect the private key against stealing, damaging, modifications of content or other discredits; it is forbidden to duplicate the private key;

e) propose a name or a distinctive pseudonym for identification;

f) submit for the provider's examination: the request for providing a certificate, the agreement to observe the obligations as client and the public key.

Art. 24

Upon the receipt of the certificate issuance application the respective provider will verify, before the certificate's issuance, the following aspects:

a) if the applicant of the certificate is the person identified according to the application, making use of the proper procedure for that category of the certificate;

b) if the certificate's applicant possesses the private key corresponding to the public key listed in the certificate;

c) if the information listed in the certificate is accurate.

Art. 25

(1) The duration for verifying the information within the application and for issuing the certificate cannot exceed:

a) one working day, for simple certificates;

b) 5 working days, for qualified certificates.

(2) The deadlines stipulated at paragraph (1) are calculated from the date when the provider receives all the information requested for this purpose.

Art. 26

The provider cannot issue a certificate without the expressed consent of the person on behalf of which it is issued.

Art. 27

A certificate is valid for maximum 1 year from the date when it is notified to the client.

Art. 28

The certificate can be transmitted to the applicant in the following manners:

- a) personally;
- b) via postal services, with acknowledgement of receipt;
- c) via electronic mail – only for simple certificate; any observations, if there may be, are notified to the provider in the same manner.

Art. 29

By accepting the certificate the client:

- a) assumes the responsibility to control the private key and takes measures to prevent the key's disclosure, modification or unauthorized use;
- b) certifies the trustworthiness of the information contained in the certificate
- c) commits to use the certificate exclusively for authorized purposes, in accordance with the law;
- d) does not have the right to use the private key corresponding to the public key listed in the certificate, in order to sign other certificates, except for the cases in which this has been expressly stipulated in the contract concluded with its provider

Art. 30

(1) The provider directly manages the public keys of the clients, either individuals or legal persons. The management of the public keys implicitly presupposes granting all certification services stipulated in the contract with the clients.

(2) The certification services refer to the issuance, verification, suspension, renewal, revocation and provision of information concerning the issued certificates, as well as their safe preservice during their validity, to which a period of minimum 10 years is added since the expiry of the certificate's validity period, in accordance with the provisions of the art. 20 lett. h) of the Law.

(3) The services for verifying the electronic signatures are automatically assured, through the Internet, such services being expressly stated under the contract.

Art. 31

- (1) The archives of a provider found in the circumstance stipulated at art. 24, paragraph (4) of the Law are taken over by the Authority.

(2) The information form regarding the ceasing of the activity of a certification services provider is stipulated by the annex no. 9.

(3) In case the Authority orders a provider's cease of activity and there is no provider able to take over the former's activity, the Authority will ensure the certificates revocation, if the revocation had not already been performed by the provider, on the provider's expense; the Authority will take over and maintain the archives and the electronic registry, without permanent connection to the Internet.

Art. 32

A provider can require the issuance of a certificate from another provider, the latter managing thus the public key of the former. This case is stipulated in the annex no. 10.

CHAPTER V: Technical Details

SECTION 1: Signature creation data

Art. 33

The Authority's electronic signature creation data are generated using an isolated, viable system, specially designed for this purpose, protected against unauthorized use.

Art. 34

The Authority will use the RSA algorithm for the electronic signature.

Art. 35

(1) The minimum length of the private key used by a subscriber for creating the extended electronic signature has to be of minimum:

- a) 1,024 bytes for the RSA algorithm;
- b) 1,024 bytes for the DSA algorithm;
- c) 160 de bytes for the DSA algorithm based on elliptic curves.

(2) The length does not include the sequence of 0 bytes from the most representative positions.

(3) The repeated generation of electronic signature creation data must not lower its safety level, the uniqueness condition being mandatory. The procedures of generating electronic signature creation data which by repeated use might reduce the key quality are excluded.

Art. 36

(1) The minimum number of bytes of the electronic signature creation data determined based on really randomly technical numbers is of:

- a) 1,024 bytes for the RSA algorithm;
- b) 1,024 bytes for the DSA algorithm;
- c) 160 de bytes for the DSA algorithm based on elliptic curves.

(2) It is forbidden to use pseudo-random numbers as starting point in generating the signature creation data.

(3) If the generating system is used for obtaining keys for more than one subscriber, the quality of the elements generated has to be verified statistically at least once a month. The results of the tests performed have to be recorded. In case the result of the test is negative, all the certificates issued from the date of the last test will be revoked.

Art. 37

(1) If the signature creation data are generated by the certification services provider, the latter has to ensure the confidentiality both of these data and of those based on which the keys have been generated.

(2) The same dispositions are applied for the transfer of the signature creation data in the signature creation devices, as well as of the subscriber's identification data necessary for using the device.

Art. 38

If the signature creation data are generated by a third party, this party has to use viable generating devices, protected against unauthorized use.
Each access to the device for generating the signature creation data has to be monitored.

SECTION 2: Systems and Procedures Used for Electronic Signature Creation

Art. 39

The Authority uses only the hash-code SHA-1 function and the RSA encryption algorithm.
It is forbidden to use the Chinese abstract theorem of the rests.

Art. 40

(1) In order to obtain an extended electronic signature the following hash-code functions can be used:

a) RIPEMD - 160;

b) SHA-1 function.

(2) Pseudo-random numbers can be used for enlarging the length of the document fingerprint. The encryption algorithms of the fingerprint, in case of the extended electronic signature, are:

a) RSA;

b) DSA;

c) DSA on elliptic curves according to ISO/IEC 14883-3, annex A.2.2, IEEE standard P1363, sections 5.3.3, 5.3.4

(3) In case of the algorithms involving random numbers, pseudo-random numbers can be used.

(4) Other procedures of signature creation are considered to be equivalent if they offer the same security level certified by a recognized authorized body.

Art. 41

If, for launching the electronic signature creation procedure it is used an access method specially designed to prevent unauthorized use, the respective code must not be reused for other purpose

Art. 42

The format of the electronic signature has to be in accordance with the legal provisions in field - PKCS#7 Syntax standard of encrypted messages.

Art. 43

The result of the verification of an extended electronic signature is safe only if a device for verifying the electronic signature is used, device specified by the certification services provider who issued the certificated based on which the signature is validated.

SECTION 3: Qualified certificates

Art. 44

In case of renewing a qualified certificate, a new certificate is issued containing the same identification and electronic signature verification data, but with other validity data.

Art. 45

According to the provisions of the art. 13, the format of the qualified certificate has to be described by the provider using a formal standard language - CCITT or the recommendations of the ITU-TX.208 -, in a document attached to the notification submitted to the authority.

Art. 46

The electronic registry for recording the issued certificates has to correspond to an internationally recognized format. The following standards are recommended:

- a) 1988 CCITT (ITU-T) X.500/ISO IS9594;
- b) RFC 2587 Internet X.509 Public keys infrastructure LDAPv2;
- c) RFC 2587 Internet X.509 Public keys infrastructure – certificates and CRL profile;
- d) RFC 2589 - LDAPv3 Extensions for dynamic folder services.

SECTION 4: Certificates revocation and time stamping

Art. 47

The provider has to inform the clients and the third parties who may influence the client's attributes inscribed on the qualified certificate regarding the manner in which they can require the certificate revocation.

Art. 48

(1) The time stamping proves the existence of certain data at a certain specified moment in time.

(2) By applying such a timestamp, hereinafter called time-stamp, the existence of certain information at the respective time can be proven.

(3) The time stamping services can be provided by the provider or by third parties, in accordance with the established standards - ETSI TS 101 861 Time stamping; ETSI TS 101 733 v1. 2.2 (2000-12); RFC3161 Internet X.509 PKI Time stamping Protocol.

(4) In order to mention the date and time, services based on qualified certificates are used as well as the Central Europe date and time, taking into account the hour change – summer/winter time. The maximum allowed error is of 1 minute.

CHAPTER VI: Other dispositions

Art. 49

The Authority has to verify a provider at least once at 2 years or when the working procedures are changed.

Art. 50

(1) The Authority orders the suspension of the provider's activity until the causes which determined measure taking in the following situations ceased:

- a) the provider breached the confidentiality obligations stipulated by the art. 15, paragraph (1) of the Law;
- b) the provider does not notify the Authority according to the conditions stipulated by the art. 13, paragraph (1) and (2) of the Law;
- c) complementary to the application of the infringement sanction stipulated by the art. 45 of the Law;
- d) the provider does not pay the compensation within the established date, compensation which he was bound for through a final and revocable decision given by a legal court;
- e) The provider does not pay, within maximum 10 days, the cost of the operations stipulated by the art. 31, paragraph (3).

(2) Within this period, the Authority verifies the provider and communicates the identified shortcomings. The Authority establishes a deadline of maximum 30 days within which the provider has to solve the encountered issues.

(3) If the provider does not remedy the deficiencies within the given term, the Authority orders the cease of activity and/or the withdrawal of the accreditation decision and/or the suspension of the right to issue qualified certificates, depending on the identified issues and on the types of services offered by the provider.

(4) During the time when the activity is ceased, the provider is bound to ensure the services of certificates suspension/revocation and verification as well as the consultation of the electronic registry through the Internet, except the case when the deficiencies are found at the level of these systems.

Art. 51

In the contexts stipulated by the art. 50, paragraph (1), letter d) and e), the Authority has the right to issue claims on the letter of guarantee or on the insurance policy, to the extent of the created damage.

Art. 52

(1) The electronic signature creation devices represent products associated to the electronic signature, in accordance with the art. 4 item 15 of the Law.

(2) The products associated to the electronic signature are presumed to accomplish the requirements stipulated by the item 8 and by the art. 20, letter f) of the Law, in case they are conformous to at least one of the following:

a) Romanian standards or their relevant parts, which adopt those harmonized European standards the reference numbers of which have been published in the Official Gazette of the European Communities, to the extent to which the respective conditions are covered by these standards;

b) the harmonized European standards the reference numbers of which have been published in the Official Gazette of the European Communities, to the extent to which the respective conditions are covered by these standards;

c) the Romanian standards or their relevant parts, adopted in accordance with the legal dispositions in force, to the extent to which the respective conditions are covered by these standards and there are no Romanian standards of the category of those provided by letter a), which can be applied.

(3) The list of standards stipulated by the paragraph (2) is published by means of an order of the Ministry of communications and information technology.

Art. 53

The secured devices for creating the electronic signature, recognized as being in accordance with the requirements of the annex III of the 1999/93/EC Directive by an institution designated by one of the European Union member states to perform determinations of the conformity of these devices, are considered to be homologated in the sense of the art. 11, paragraph (2) of the Law.

Art. 54

In accordance with the art. 40 of the Law, the qualified certificate, issued by a provider registered in one of the European Union member states, is recognized as being equivalent in terms of legal effects with the certificate issued by a certification services provider domiciled or headquartered in Romania, under the European Association Agreement between Romania, on one hand and the European Community and the member states, on the other hand.

Art. 55

The annexes no. 1-10 are integrant part of these technical and methodological norms.

ANNEX No. 1 to the technical and methodological norms

Domain	Electronic signature	Domain code	SMEL
Document title	INFORMATIONAL CONTENT AND STRUCTURE OF THE ELECTRONIC SIGNATURE CERTIFICATION SERVICES PROVIDERS' REGISTRY	Document code	01
		Page	2
1.	Running number of the recording, automatically generated		
2.	Provider's identification code (FSC)		
3.	Provider type natural/legal person		
4.	Name of the trade company/Name of the provider (for natural person)		
5.	Activity starting date		
6.	Provider's public key		
7.	Guidelines on the accreditation (accredited/unaccredited)		
8.	Accreditation period start/end		
9.	Guidelines regarding the right to issue qualified certificates		
10.	Description of the FSC general policy		
11.	Description of the FSC systems		
12.	FSC code of practices and procedures		
13.	Company organization form (PIC/Ltd/Autonomous directorate/Public institution, non-governemental organization, other types)		
14.	Address (country, city, county/sector, street, number, block, wing, floor apartment, postal code)		
15.	Nationality		
16.	Citizenship		
17.	Telephone, fax, email, web page address		

18.	Commerce registry code/Fiscal code (for legal person)
19.	Bank of the provider
20.	Number of the provider's bank account
21.	Type of the provider's guarantee
22.	Insurance company/Financial institution that guarantees the provider's financial capability
23.	Insured amount/ Covered amount through the letter of guarantee
24.	Creditworthiness certificate attributes: document number, date, issued by..., verified by..., verification date/hour
25.	Attributes of the letter of guarantee: document number, date, issued by..., verified by..., verification date/hour
26.	Insurance contract attributes: document number, date, issued by..., verified by..., verification date/hour
27.	Headquarters lease contract attributes: document number, date, issued by..., verified by..., verification date/hour
28.	Headquarters property contract: document number, date, issued by..., verified by..., verification date/hour
29.	Attributes of the certificate regarding the state debts: document number, date, issued by..., verified by..., verification date/hour, issued by the bank through which the company makes current payments and cashing
30.	Services categories destined for the public (type of certificates and security procedures used, certificates structure, usage, for each type of certificate)
31.	Types of devices for creating the electronic signature used
32.	Devices status (if they are homologated or not)
33.	Homologation agency (if it is the case)
34.	FSC technical certification attributes: document number, date, issued by..., verified by..., verification date/hour
35.	Critical situations: field that may contain references to the last critical situation (for instance the temporary cease of the FSC activity due to technical problems.

	Modification of the FSC procedures, sanctions etc)
36.	Date and hour of the last update
37.	Date and hour of the last verification
38.	Provider's status (operational, suspended, ceased activity, activity pending for transfer, pending for identification by the ARS – indicating the deadline)
39.	Reasons for suspension/restart/cease of activity (if the case may be)
40.	FSC that retakes the certificate's management (in case the provider's cease of activity)
41.	Declaration confirming the accuracy of the information above, electronically signed by the FSC and/or ARS
42.	Identity of the operator from the ARS who introduced/modified/deleted the registration
43.	A document containing all the previous data, electronically signed by the MCIT operator who introduced the registration

At rows 10, 11 and 12 the provider has to make reference to:

- a) certificate request procedure;
- b) types of pseudonyms allowed, if the case may be;
- c) method of including the supplementary attributes in the certificate;
- d) working hours;
- e) manner of generating the data for creating the provider's signature;
- f) format of the data for creating the provider's signature;
- g) generation procedure for the creation data of the clients' signature;
- h) format of the clients' signature creation data;
- i) hash functions and encryption procedures used;
- j) list containing the products associated to the electronic signature used and recommended;

- k) format of the documents that may be electronically signed;
- l) certificates' format and validity period;
- m) technical standards and access methods to the electronic registry of recording the issued certificates;
- n) time intervals in which date and hour electronic time stamping services are offered and, if the case may be, in accordance with the art. 52 of the technical and methodological norms;
- o) detailed methods for verifying the signatures;
- p) description of the practices, procedures and systems which ensure the data security and integrity, the permanent authorized access to them and which prevent any unauthorized access;
- q) personnel policies;
- r) personnel structure;
- s) partnerships and policy in field.

ANNEX No. 2 to the technical and methodological norms

Domain	Electronic signature				Domain code	SMEL	
Document title	NOTIFICATION FORM TO THE ARS FOR THE PROVIDERS OF ELECTRONIC SIGNATURE CERTIFICATION SERVICES				Document code	02	
					Page	2	
FSC natural/legal person		Country	City	Sector	Street	no	
Address*		block	floor	appt.	Postal code		
		Phone	Fax		E-mail	Web	
Trade Registry registration code		Fiscal code		Type of company**			
Bank	Bank account no.		Property document no. – headquarters				

		lease contract no.	
Nationality		Citizenship	
*) Headquarters of the Trade Company/Address of the natural person **) Plc, Ltd., Autonomous directorate			
Offered certification services***	Certificates issuance		
	Simple	Qualified, with distribution to the client of DSCS****	Qualified, without distribution to the client of DSCS
Activity starting date			
Security procedures used (to be detailed)			
Types of DSCS used:			
) The answer will be "Yes" or "No" *) Secured Device for Creating Electronic Signature			

Domain	Electronic signature	Domain code	SMEL
Document title	NOTIFICATION FORM TO THE ARS FOR THE PROVIDERS OF ELECTRONIC SIGNATURE CERTIFICATION SERVICES	Document code	02

NOTIFICATION – LIABILITY

I, the undersigned notify the Authority for Electronic Signature Regulation and Supervision (ARS)* regarding the development of the certification services mentioned in this document, starting from the date.....(the date will be mandatorily filled in).

I commit to develop my activity in accordance with the provisions of the Law no. 455/18.07.2001 regarding the electronic signature which I bound to observe in respect to its letter and its meaning.

I also bound to observe the Romanian methodological norms regarding the application of the electronic signature as well as the European and international standards in field and to notify the clients the practical certification instructions,

the terms and conditions of using the electronic signature made available by my company.

I hereby attach the following documentation:

1. Headquarters lease contract or property document.
2. Certificate from the Financial Administration which the company relates to, regarding the up to date payment of the state debts.
3. Creditworthiness certificate or letter of guarantee from the bank through which the company performs current payments and cashing.
4. Copy of the insurance contract made in the name of the company, amounting to 500,000 EURO (only for accredited Certification Services Providers who issue qualified certificates).
5. Copy of the Guarantee Certificate (only for Certification Services Providers who issue qualified certificates):
 - a. For issuing qualified certificates, the providers I submit:

a guarantee from a financial institution in the favor of the ARS, amounting to at least 500,000 EURO at the bank... and I bound to cover the damages that I may cause to the client, up to the amount of 10,000 EURO/ensured risk or

an insurance policy to an insurance company in the favor of the ARS of at least 500,000 EURO at the bank... and I bound to cover the damages that I may cause to the client, up to the amount of 10,000 EURO/ensured risk
6. Public key
7. FSC general policy
8. Description of the FSC systems.
9. FSC code of procedures and practices
10. I require/ do not require the accreditation of the ARS (the statement which does not stand valid will be stricken through).

COMPANY REPRESENTATIVE
Date and hour

On behalf of the ARS, received the
mentioned documentation

ANNEX No. 3 to the technical and methodological norms

Domain	Electronic signature				Domain code	SMEL
Document title	QUALIFIED CERTIFICATE CONTENT AND STRUCTURE				Document code	02
					Page	2
Data about the FSC						
Name of the Certification Services Provider						
Address*	Country	City	Sector	Street	no	
	block	floor	appt.	Postal code		
	Phone	Fax		E-mail		
Citizenship/Nationality						

*) If it is legal person, its headquarters

Domain	Electronic signature				Domain code	SMEL
Document title	QUALIFIED CERTIFICATE CONTENT AND STRUCTURE				Document code	03
					Page	2
Data about the client						
First and last name ¹						
Pseudonym						
Address ²	Residence country		County/Sector			

	City		Street		No.	
	Block		Wing		Apart.	
	Postal code		Phone		Fax	
	E-mail			Web page		
Other information which the client wants to be included in the certificate						
Certificate type	QUALIFIED CERTIFICATE					
Public key						
Subscriber personal identification code						
Certificate identification code						
Extensions of the signature (see Annex 4 of the Methodological norms regarding the application of the electronic signature)						
Certificate validity period						
Information regarding the certificate's usage extents						

EXTENDED ELECTRONIC SIGNATURE OF THE ISSUING FSC

¹ For legal persons, the official organisation designation will be filled in.

² For legal persons, the organization headquarters address will be filled in.

ANNEX No. 4 to the technical and methodological norms

Domain	Electronic signature	Domain code	SMEL
Document title	STANDARDIZED EXTENSIONS OF THE CERTIFICATES FOR THE ELECTRONIC SIGNATURE	Document code	04
		Page	2
Extension	Used by	Usage	Critical

A. Information about keys and certification policy			
AuthorityKeyIdentifier Identifier for the authority public key	All	Identifies the public key corresponding to the private key used by the Certification Provider to sign this certificate	No
KeyIdentifier Identifier of the public key	All	Sole identifier, depending on the algorithm used	No
AuthorityCertIssuer Name of the certificate issuer	All	Identifies the the certificate issuing authority; together with the serial number, alternative to the key identifier	No
AuthorityCertSerialNumber Certificate serial no.	All	Used with Name of the certificate's issuer	No
SubjectKeyIdentifier Identifier of the subject's key	All	Identifies various keys for the same subject	No
KeyUsage Usage of the key	All	Defines specific purposes for using the key (for instance, digital signature, key agreement...)	Optional
PrivateKeyUsagePeriod Usage period of the private key	All	Only for the digital signature keys. The signatures on documents dated outside the period are invalid	Optional
CertificatePolicies Certification policies	All	Identifiers and qualifiers who identify and qualify the certification policies applied to a certificate	Optional
PolicyIdentifiers Identifiers of certification policies	All	OID = policy identification object	Optional
PolicyQualifiers Attributes of the certification policy	All	More information on the certification policies	Optional
PolicyMappings Overlapping of policies	AC	Indicate equivalent policies	Optional
B. Certificate and FSC attributes			
SubjectAltName Alternative name of the subject	All	Used to list the alternative names (for instance the name RFC822, the address X400, the IP address...)	Optional
IssuerAltName Alternative name of the	All	Lists the alternative names	Optional

issuer			
SubjectDirectoryAttributes	All	Lists all wanted attributes (for instance supported algorithms)	Optional
C. Certification path constraints			
BasicConstraints	All	Constraints regarding the subject's role (for instance the path length)	YES
CA Certification Authority	AC	The path length is significant only if the cA value – Real	YES
PathLenConstraint Constraints regarding the certification path length	AC	The AC number which are allowed in the certification path; 0 indicates that the AC may issue certificates only to the final entity	YES
NameConstraints Constraints related to the name	AC	Limits the consecutive AC certification referring to the following two parameters: PermittedSubtrees and ExcludedSubtrees	Optional
PermittedSubtrees		Names outside the subtree indicates are not allowed	Optional
ExcludedSubtrees		Indicates the excluded subtrees	
PolicyConstraints Constraints of the certification policy	All	Constraints the certificates issued by the AC to the policies mentioned in the following parameter; These are used in conjunction to the second or third parameter	Optional
PolicySet Set of certification policies	All	Those certification policies to which the constraints are applied	Optional
RequireExplicitPolicy	All	Shows the number of certificates that may occur in the indicated path, before an explicit policy is required	Optional
InhibitPolicyMapping Overlapping of the inhibition policies	All	Shows the number of certificates that may occur in the indicated path, before the overlapping of the policies should still be allowed	Optional
D. Identification of the revoked certificates list			
CrIDistributionPoints LCR distribution points	All	Mechanism of dividing the long LCRs in short lists	
DistributionPoint	All	Location from which the LCR can be obtained	Optional

Reasons	All	Reasons why the certificates are included in the LCR	Optional
CRLIssuer	All	Name of the component issuing the LCR	Optional

“NO” – means that the standard requires that the extension should be uncritical

“OPTIONAL” means that the issuing FSC may choose if the extension is critical or uncritical.

“YES” means that the standard “Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocated List Profile” – standard recommended by ETSI – permits the respective field to be critical or uncritical, but it is recommendable that it should be considered critical.

ANNEX No. 5 to the technical and methodological norms

HEADER OF THE FINANCIAL INSTITUTION

Date Subject

This address confirms that

.....(financial institution) irrevocably guarantees the payment/payments ordered by (FSC) amounting to the extent of (minimum 500,000 euro) from the account (FSC account).

This guarantee refers to the conditions stipulated by the law and by the methodological norms regarding the application of the electronic signature. This letter of guarantee is valid until (validity date of the letter of guarantee).

For verifications, please contact (financial institution contact).

.....
(signature of the financial institution representative)

.....
(signature of the FSC representative).

ANNEX No. 6 to the technical and methodological norms

Domain	Electronic signature	Domain code	SMEL
Document title	MINIMAL INFORMATIONAL CONTENT OF THE CERTIFICATES REGISTRY	Document code	06
		Page	2

A. Client identification data

No.	Data category	
1	Natural/legal person	
2	Name of the natural/legal person	

a. Data about the individual or on the legal representative of the legal person

3	First and last name	
4	Pseudonym	
5	Client identification code	
6	Date of birth DD/MM/YYYY	
7	Place of birth	

b. Address of the individual or of the legal representative of the legal person

8	Country	
9	City	
10	Sector	
11	Street	
12	No.	
13	Block	
14	Apart.	
15	Postal code	
16	Phone	
17	Fax	
18	E-mail	

c. Address of the legal person's headquarters

19	Country	
20	City	
21	Sector	
22	Street	
23	No.	
24	Block	
25	Apart.	
26	Postal code	
27	Phone	
28	Fax	
29	E-mail	

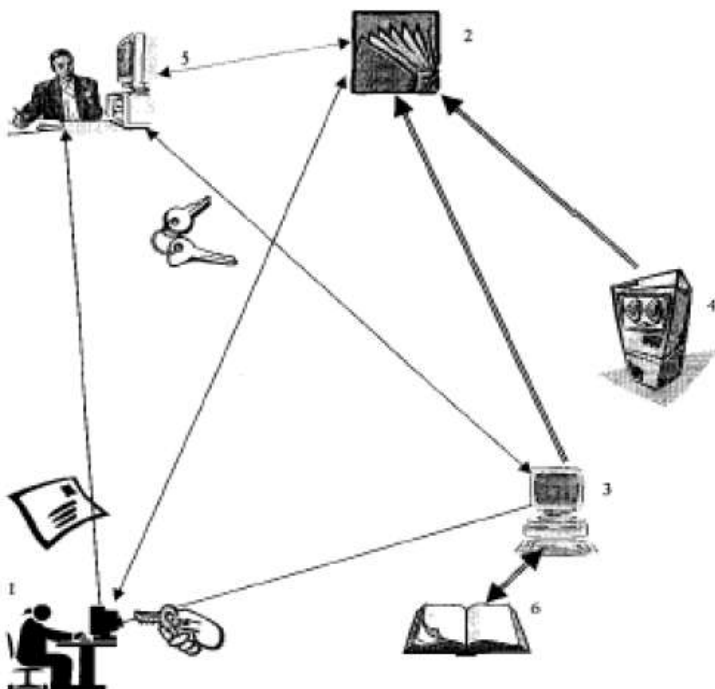
Domain	Electronic signature	Domain code	SMEL
Document title	MINIMAL INFORMATIONAL CONTENT OF THE CERTIFICATES REGISTRY	Document code	06
		Page	2

B. Certificate data

30	Certificate code	
31	Certificate category (simple / qualified)	
32	Certificate issue date	
33	Certificate expiry of the validity date	
34	Certificate notification on the expiry of the validity date	
35	Certificate expiry date	
36	FSC taking over the certificate management	
37	If there is the client's agreement (YES/NO)	
38	Certificate revocation date	

C. Certificate proper (in accordance with the annex 3)

ANNEX No. 7 to the technical and methodological norms



Management and use of the public and private keys for certification services

1 - Client, Certificate owner; 2 – Certification Services Providers' Registry (RFSC) kept by the ARS; 3, 4 - Certification Services Providers (there may be more of them, the example shows only two providers: FSC1 and FSC2); 5 – Recipient of an electronically signed document; 6- RC1- Electronic log registry of the certificates issued by the FSC I.

Phase I: Establishment of ARS and RFSC

Phase II: The client consults the RFSC, chooses (following the analysis of the information made available by the providers in accordance with the Art. 14 of the Law) a FSC among the existing ones (in our case chooses FSC1) and concludes the contract with the latter. The client is issued the certificate (created based on the data included in the certificate request form) and the electronic signature creation device; The certificate is included in RC1.

Phase III: The client sends the document bearing his electronic signature. The receiver verifies the signature using the client's public key (from his certificate). Additionally, for an increased safety, he may consult the to obtain the public key of the FSC1 (necessary for verifying the FSC1 signature on the client's certificate).

ANNEXA No. 8 to the technical and methodological norms

Domain	Electronic signature	Domain code	SMEL
Document title	INFORMATION MADE AVAILABLE BY CLIENTS FOR THE CERTIFICATION OF APPLICATIONS - SIMPLE CERTIFICATE	Document code	08
		Page	3

Mandatory data on the applicant

First and last name		Pseudonym		E-mail	
---------------------	--	-----------	--	--------	--

Optional data on the applicant

Address	Residence country		City		County/Sector		
	Street		No.		Block		Wing
	Floor		Apert.		Postal code		
	Phone		Fax				
Date of birth (dd/mm/yyyy)		I.C.series			I.C. No.		
Issued by		Valid until (dd/mm/yyyy)			Issue date (dd/mm/yyyy)		
Passport no.		Issued by			Valid until (dd/mm/yyyy)		

Driver's licence no.		Issued by		Valid until			
Card type		Issuing bank		Card no.		Card expiry date	

Optional data about the husband/wife

First and last name		Date of birth (dd/mm/yyyy)	
---------------------	--	----------------------------	--

Data about the applications

Applications type (electronic mail, web navigation, small and low risk transactions, web subscription to certain services)	
--	--

provided by third parties, etc.)	
Other information required by the above mentioned applications	

Domain	Electronic signature	Domain code	SMEL
Document title	INFORMATION MADE AVAILABLE BY CLIENTS FOR THE CERTIFICATION OF APPLICATIONS - QUALIFIED CERTIFICATE – LEGAL PERSONS	Document code	08
		Page	3

Mandatory data on the applicant

First and last name		Pseudonym		Date of birth (dd/mm/yyyy)		
Address	Residence country		County/Sector		City	
	Street		No.		Block	
	Wing	Apart.		Postal code		
	Phone		Fax	E-mail		
I.C. Series		I.C. No.		Issue date (dd/mm/yyyy)		
Issued by		Valid until (dd/mm/yyyy)				
Passport no.		Issued by		Valid until	DD/MM/YYYY	
Driver's licence no.		Issued by		Valid until	DD/MM/YYYY	
Card type		Issuing bank				
Card no.		Card expiry date	DD/MM/YYYY			
Optional data about the husband/wife						
First and last name				Date of birth (dd/mm/yyyy)		
Data about the applications						
Application type. Electronic mail, web navigation, any type of transactions, file						

transfer, software validation, web subscription to various services provided by third parties, etc.	
Other information required by the above mentioned applications	

Domain	Electronic signature	Domain code	SMEL
Document title	INFORMATION MADE AVAILABLE BY CLIENTS FOR THE CERTIFICATION OF APPLICATIONS - QUALIFIED CERTIFICATE – LEGAL PERSONS*	Document code	08
		Page	3

Mandatory data about the legal person (filled in in front of the legal representative)**

Domain name		Legal person name				
Address	Country		City			
	Street		No.		Block	
	Wing		Apart.		Postal code	
	Phone		Fax		E-mail	
Legal decision no. and establishment data of the legal person		Registration number in the Trade Registry				
Fiscal code no.		Bank through which the current operations are developed	Bank account no.			

Mandatory data about the contact person designated by the legal person (filled in in the presence of the contact person)**

First and last name		Position within the company		Date of birth	DD/MM/YYYY
I.C. Series		I.C. no.		Issue date	DD/MM/YYYY
Issued by		Valid until	DD/MM/YYYY		
Passport no.		Issued by		Valid until	DD/MM/YYYY
Driver's licence no.		Issued by		Valid until	DD/MM/YYYY
Card type		Issuing bank		Card no.	

Card expiry date	DD/MM/YYYY					
Address	Country		City			
	Sector/County		Street		No.	
	Block		Wing		Apart.	
Telephone		Fax		E-mail		
Optional data about the husband/wife						
First and last name			Date of birth	DD/MM/YYYY		
Data about the applications						
Application type: electronic mail, web navigation, any type of transactions, file transfer, software validation, web subscription to certain services provided by third parties, etc.						
Other information required by the above mentioned applications						

* In case the modification of the legal person's form or status, the legal person is bound to renew the contract with the FSC.

** In case the legal representative or the contact person is changed, the newly assigned persons in these positions are bound to attend to the FSC to fill in the data required by the FSC

ANNEX No. 9 to the technical and methodological norms

Domain	Electronic signature	Domain code	SMEL
Document title	MAP OF THE INFORMATIONAL FORM REGARDING THE CEASE OF ACTIVITY OF A CERTIFICATION SERVICES PROVIDER	Document code	09
		Page	3

FISC name			FISC Registry code		
Address	Country		County/Sector		City
	Street		No.		Block
	Wing		Apart.		Phone
	E-mail		Fax		Postal code
Trade Registry Code		Fiscal code		Starting date of the activity	DD/MM/YYYY Y

				cease	
Date when notified the ARS	DD/MM/YY YY	Reasons for the cease of activity (existence and nature of the circumstance which justifies the cease of activity, in acc. with the art. 24, paragraph 1 of the Law)			
The name of the FSC taking over the activity		Code from the Registry of the Services Providers			
Registration number in the Trade Registry		Fiscal code			
Address of the FSC taking over the activity	Street		No.		Wing
	Floor		Apart.		
	City		Sector/County		Country
	Phone		Fax		E-mail
Measures taken with reference to the clients	<p>Revocation of the certificates issued to the clients (List of revoked certificates) – the data from Table 1 will be filled in</p> <p>Taking over of the certificates issued to the clients (List of taken over certificates) – the data from Table 2 will be filled in</p> <p>Measures taken to ensure the archives referring to clients and issued certificates, as well as ensuring the processing of the personal data in accordance with the Law (acc, to the art. 24 paragraph 4 of the Law)</p>				

Domain	Electronic signature	Domain code	SMEL
Document title	MAP OF THE INFORMATIONAL FORM REGARDING THE CEASE OF ACTIVITY OF A CERTIFICATION SERVICES PROVIDER	Document code	09
		Page	3

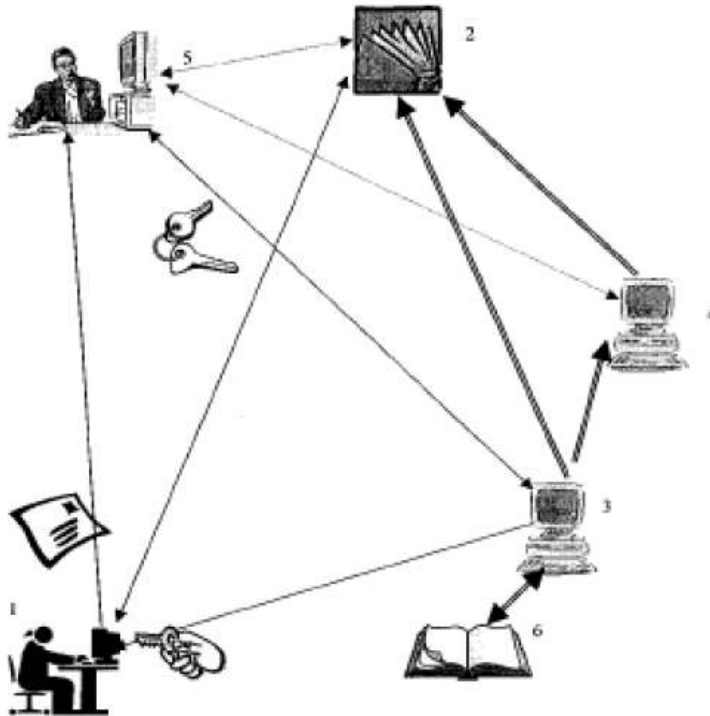
TABLE 1 – List of revoked certificates

Certificate series	Issue date and hour	Signature algorithm	Version
	DD/MM/YYYY		

TABLE 2 – List of valid certificates taken over

Certificate series	Issue date and hour	Signature algorithm	Version	Expiry date of the certificate validity
	DD/MM/YYYY hh/mm			

ANNEXA No. 10 to the technical and methodological norms



Hierarchical structure of the FSC

1 - Client, Certificate owner; 2 – Registry of the Certification Services Providers (RFSC) kept by the ARS; 3, 4 – Certification Services Providers (FSC2 manages the public key of FSC1); 5 – Recipient of an electronically signed document; 6 - RC1- Electronic registry of the certificates issued by FSC 1.

Phase I: FSC1 requires to FSC2 the issuance of a certificate. FSC2 manages the public key of FSC 1.

Phase II: The client sends the document bearing his electronic signature. The recipient verifies the signature using the client’s public key (from his certificate) Additionally, for an increased safety, he may consult the RFSC to obtain the public key of FSC1 (necessary to verify the signature of FSC 1 from the client’s certificate). Alternatively, the client may verify the signature of the FSCI from the client’s certificate accessing the

FSC1 certificate issued by FSC2 (located on a superior hierarchical level). In its turn, the signature of FSC2 from the FSC1 certificate can be verified turning to RFSC or to a FSC who manages the FSC2 key and so on.

Published in the Official Gazette number 847 / 28. 12. 2001