

**Resolution of
The Supreme Council of Information &
Communication Technology (ictQATAR)
Regarding the Bylaw regulating the work of
certification service providers**

**The Supreme Council of Information & Communication Technology
(ictQATAR)
Board of Directors' resolution No. () of 2011
Promulgating the Bylaw regulating the work of certification service
providers pursuant to the Electronic Commerce and Transactions Law**

The Board of Directors,

Having perused the Electronic Commerce and Transactions Law promulgated by Decree Law No. (16) of 2010; particularly Article No. (3) of the promulgation law, and

The proposal by the Secretary General of The Supreme Council of Information and Communication Technology,

Has decided the following:

Article (1):

The Bylaw regulating the work of certification service providers, its tables of fees and its appendices enclosed therewith, shall be effective.

Article (2):

The concerned authorities, each within its competence, shall implement this resolution. This resolution shall be published in the Official Gazette.

Tamim Bin Hamad Al-Thani

Chairman

The Supreme Council of Information and Communication Technology

Issued on: / /1433 A.H.

Corresponding to: / /2012

The Bylaw Regulating the Work of Certification Service Providers

Chapter (1) Definitions

Article (1)

In the application of the provisions hereof, the following terms and expressions shall have the meanings assigned to each of them, unless the context otherwise requires:

State	:	State of Qatar.
The Supreme Council	:	The Supreme Council of Information and Communication Technology.
Board	:	Board of directors of the Supreme Council.
General Secretariat	:	The General Secretariat of the Supreme Council.
Concerned Department	:	Concerned administrative unit of the General Secretariat.
Committee	:	Grievance and Disputes Resolution Committee set out in Article No. (64) of the Law.
The Law	:	The Electronic Commerce and Transactions Law promulgated pursuant to Decree Law No. (16) of 2010.
Person	:	Natural or legal person.
Electronic signature	:	Inscription affixed on the data message in the form of letters, numbers, symbols, tokens, or otherwise with a distinctive feature, used to identify the signatory and distinguish them from others; for the purpose of expressing the signatory's approval of the data message.
Signature creation information	:	Information, symbols or special encryption keys used by the signatory in creating the electronic signature.
Signatory	:	The person having the legal right to access signature creation information, acting either for himself or on behalf of a person they represent to use this information for creating the electronic signature.
Certification service provider	:	A person licensed to maintain an infrastructure of the public keys, to issue certification certificates and to provide services in relation to electronic signatures.
Certification certificate	:	A document issued by a certification service provider confirming the valid link between a signatory and the signature creation information.

Encryption	:	Using uncommon symbols or signs thereby making information intended to be passed or sent incomprehensible by others, or using symbols or signs without which information is not accessible.
Certifying person	:	The person acting on the basis of a certification certificate or electronic signature.
Place of business	:	A non-transitory facility or installation used to carry out the business of certification services.
Entrusted employee	:	Any employee working for the certification service provider, and entrusted to undertake or assist in undertaking any of the duties, competences or responsibilities of the certification service provider pursuant to the provisions of the Law and this Bylaw.
Reliable	:	Means those systems, procedures, operations, human resources, products and services carry out their functions properly, consistently and reliably.
Consumer:	:	A person acting for purposes other than those of his trade, business or profession.

Chapter (2)

Licensing certification service providers

Article (2)

Pursuant to the provisions of the Law and this Bylaw, none of the following businesses may be practiced without a license from the Secretariat General.

- 1- Maintaining an infrastructure for public keys.
- 2- Providing services related to electronic signatures.
- 3- Issuing electronic certification certificates.

Article (3)

Any person wishing to provide the services and businesses set out in the above article shall submit a request to such effect to the concerned department on the application form prepared for this purpose; and shall enclose the following documents therewith, as the case may be:

1. Memorandum and articles of association pursuant to the legislations applicable in the State.
2. The commercial registration or the commercial license.

3. The organization structure of the company.
4. Title of deeds or lease contract.
5. Accredited auditors' report on the company's financial position for the last two years, or for the period since its establishment until the date of submitting the application, whichever is more recent.
6. Proof of payment of due fees.
7. A written declaration that the place of business conforms to all technical standards required by the Law and this Bylaw.
8. A written declaration to the effect that all entrusted employees fulfil all pertinent requirements pursuant to the Law and this Bylaw, in addition to a detailed statement of their qualifications and experience in the field of certification services; with supporting documents.
9. Technical features or specifications of certification equipment and the systems accredited for providing the certification service; accompanied with an approved chart therefor.
10. A graph drawing for of the service provider's place of business and a precise description of the approved safety measures to secure it.
11. A comprehensive economic feasibility study for the project to be established.

The concerned department may, within (30) thirty days from the date of submitting the application, request the license applicant to provide any information, data or documents it deems necessary, as the case may be, in the form and the manner and at the time as may be specified by the concerned department.

Article (4)

The license shall be valid for (5) five years effective from the date of it has been granted, and may be renewed for similar period(s) pursuant to the terms, conditions and controls set out in the Law and this Bylaw.

Article (5)

Subject to the provisions stipulated in Article No. (3) hereof, the certification service provider shall submit the application for license renewal at least (3) three months prior to the expiry date of the current valid license.

Article (6)

The applicant for license issuance or renewal shall pay the due fees. In case the application is rejected, withdrawn by the applicant before a decision on it is issued or if the license is cancelled or suspended after being issued, such fees shall not be refunded; unless the General Secretariat otherwise decides.

Article (7)

The concerned department shall receive and examine the application for license issuance or renewal as well as the documents enclosed therewith and shall ensure that it meets all related terms, controls, specifications and standards as set out in the Law and this Bylaw.

Article (8)

The General Secretariat shall, within (30) thirty days from the date of receiving the application, or from the date on which the data, information and documents required by the Secretariat General, have been submitted, issue a decision granting or renewing the license, or rejecting the application,. The applicant shall be advised of such decision in writing at its address indicated on the application. The rejection decision shall be reasoned.

The elapse of the aforesaid period without a response shall be construed as an implicit rejection of the application.

The concerned parties may lodge a grievance against such decision to the Committee within (30) thirty days from the date of being advised thereof.

Article (9)

If license is granted, the concerned department shall record and maintain the licensee's data in a special register (information/data repository) called "Approved Certification Service Providers" Register.

Article (10)

The license shall include the following data:

1. Certification service provider's name.
2. Address of certification service provider's place of business.
3. License number, issue date, validity period and expiry date.
4. Any terms, controls, provisions or restrictions imposed by the General Secretariat pursuant to the provisions of the Law and this Bylaw.

Article (11)

An applicant for license issue or renewal must meet the following conditions:

1. Have commercial registration or commercial license.

2. Resident in the State, including being a branch of a certification service provider whose head office is established outside the State.
3. Solvent by way of owning financial resources not less than QAR 5,000,000 (Qatari Riyal five millions).
4. Have insurance covering its work related to the provision of certification services, against any potential financial loss pursuant to the pertinent laws, systems and legislations applicable in the State.
5. Neither the license applicant, nor any of its entrusted employees, may be an owner of or a shareholder in any company that is considered by the General Secretariat as having a potential to mitigate or limit fair competition.
6. Have good reputation and conduct, and that no final judgment has been pronounced against him/her in a crime violating honor or trust; unless he/she has been rehabilitated.

Those terms shall continue to be met by any certification service provider throughout the validity period of the license.

In all cases, the applicant for license issue or renewal shall abide by all rules, terms, controls, standards, decisions, procedures, instructions and specifications be issued by the Supreme Council from time to time pursuant to the provisions of the Law and this Bylaw, as well as by all legislations pertinent to its work as a certification service provider.

Chapter (3) **Inspection and Audit Standards and Requirements**

Article (12)

The certification service provider shall be subject to all inspection and audit processes as required pursuant to the provisions of the Law and this Bylaw, according to the method, in the manner and at the time to be determined by the General Secretariat.

The certification service provider shall submit any documents, data, papers or information required for the inspection and audit processes, and shall respond to any questions or inquiries raised by inspectors or the auditors to enable them to accomplish their assigned duties.

Article (13)

Inspection and audit processes shall be carried out in the following cases:

1. Upon submitting the application for a license for the first time.
2. Every two years from the license issue date.
3. Upon submitting a license renewal application.
4. At any other time as may be determined by the General Secretariat at its sole discretion.

Article (14)

Inspectors or auditors shall verify the following issues:

1. Protection and planning policy.
2. Physical security (access perimeters, controls, data centre)
3. Information Communication Technology infrastructure (network and systems).
4. Electronic storage capacity./Information/Data Repositories
5. Certification services quality management system (certificates lifecycle management, delivery, issuance...),
6. Availability of electronic certification practice statement and compliance with the policies and regulations.
7. Compliance with the guidelines and technical requirements issued by the General Secretariat.
8. Agreements concluded with authorized signatories and other certification service providers.
9. Compliance with the license terms.
10. Compliance with the provisions of the Law and this Bylaw.
11. The certification service provider acts in accordance with the data it submits in relation to practicing its business.
12. Any other activities undertaken by the certification service provider.

Article (15)

The auditor or inspector shall prepare a report including the results/findings of their works and shall submit it to the concerned department within (15) fifteen days from the date of completing the inspection or audit process.

Article (16)

If it is proven, in the inspection or audit report, that a certification service provider has not met the terms and controls related to its business pursuant to the provisions of the Law and this Bylaw, the General Secretariat may reject the application for license issue or renewal, or suspend such license, as the case may be.

Article (17)

The technical audit entity must be registered in the State, and must not have any financial, legal or other relation with the certification service provider.

Article (18)

The General Secretariat shall ensure that the technical auditor meets the following requirements:

1. Sufficient familiarity with the provisions of the Law and this Bylaw as well as all guidelines, controls, standards and instructions issued by the Supreme Council in relation to certification services.
2. Accredited by an entity specialized in technical inspection.
3. holding a Certified Information Systems Auditor (CISA) certificate, Certified Information Technology Professional (CPA.CITP) certificate, Certified Internal Auditor (CIA) certificate or an accredited information security auditor certificate.
4. Be able to conduct technical audit in compliance with ISO 27000 standards, particularly ISO (27001:2005) regarding information systems – security technologies – information systems management, as well as ISO (272002) regarding codes of practicing information security management.
5. Must have sufficient experience in the fields of electronic signatures, electronic certification certificates, electronic programs, information security tools and technology, security and financial reviews rules and specialized audit technologies.

Chapter (4)

Certification service provider's obligations

Article (19)

In performing its work, the certification service provider shall abide by all terms, controls and conditions pertinent to such work as set out in the Law and this Bylaw; particularly the following:

1. Adhering to technical standards approved by the General Secretariat and enclosed with this decision, including procedures, systems and processes of encryption, and issuing electronic signatures and electronic certification certificates. These standards may be amended by the General Secretariat from time to time, provided that the certification service provider is advised of such amendments.

2. Taking all necessary action to ensure that all systems, processes, procedures, employees, apparatuses, equipment, products and services meet the approved controls, standards and requirements based on the ISO standards (27000) and the decisions, instructions and guidelines issued by the General Secretariat in this regard. In this respect, the certification service provider shall submit a report to the General Secretariat about such compliance upon submitting an application for issuing a new license or renewing a valid license.
3. Using approved and reliable systems and measures in all its activities and processes, and adopting the utmost degree of caution and diligence in performing all activities, to perform such activities efficiently, honestly and reliably.
4. Taking all the action necessary to ensure meeting all terms, requirements and standards required by any government or semi-governmental body to which the certification service provider provides services within the framework of its business.
5. Keeping reliable, complete and accurate registers for all processes of issuing, renewing, suspending or cancelling certification certificates.
6. Allowing registers to be continuously accessible for electronic review by the concerned parties by using regular precautionary backup, and taking all necessary action and employing all sufficient and appropriate means to protect data from any unauthorized alteration.
7. Meeting all safety and security standards, terms and requirements in the place of business and in the certification system in such a manner that guarantees continuity of business upon the occurrence of a failure or a disorder in any apparatuses, by using apparatuses, servers and storage units duplicity technology.
8. Using reliable means for issuing, delivering and storing certificates, and taking sufficient and appropriate measures to protect certificates against fraud, forgery, tampering, distortion, confidentiality violation or illegal or unauthorized access.
9. Providing physical protection for the place of business and the certification system against tampering or illegal or unauthorized access.
10. The compensation received by the certification service provider against the services and works it provides to the clients must be reasonable and appropriate to the nature and type of such services, and in consistency with the best international and regional practices. The Supreme Council shall have the right to review such compensation from time to time.

Article (20)

The certification service provider shall, in providing electronic signature support services, act according to the data it provides to the concerned department in respect of practicing its business, and shall particularly abide by the following:

1. Preparing, reviewing, auditing and updating the data on regular basis and maintain a copy thereof in its database and on its website in accordance with the related controls and standards set out in the Law and this Bylaw.
2. Presenting an updated copy of such data upon submitting an application for issuing or renewing the license.
3. Registering all changes which may occur to such data promptly upon their occurrence, and retaining a copy thereof in its database and on its website, in addition to advising the concerned department in writing of any changes which occur to such data within (15) fifteen days from the occurrence of such change.

Article (21)

The certification service provider shall use encryption, or any other technology, as a means for protecting electronic transactions for the purpose of maintaining confidentiality of information and data, identifying the creator's personality and preventing third parties from accessing information or messages, intercepting them or preventing the respective addressee from receiving, distorting them or modifying them by deletion or addition.

Certificate service provider shall have a well defined key management process which includes dedicated key ceremony

Article (22)

The certification service provider shall use one or more of the following methods, as the case may be, for protecting the certification system or the information systems:

1. Public key encryption.
2. Access control mechanisms.
3. Firewalls and network security filtering devices.
4. Information filters.
5. Blocking denial set.
6. Data encryption technologies.
7. Backup/recovery (procedures) protection measures.
8. Malware protection mechanisms (software, hardware)

9. Any reliable and trustworthy method or means of the technologies related to preventing security penetration attempts as required or allowed by the concerned Department.

Article (23)

The certification service provider shall keep all registers, related to performance of its work, in accordance with the standards and controls set out in the Law and this Bylaw, and shall particularly adhere to the following:

1. Keeping registers in hardcopy and electronic copy, or in any other appropriate form required by the concerned department, provided that the registers are accurate, complete, legible, accessible and usable by concerned parties.
2. Providing means that enable concerned parties to use the registers in a timely and appropriate manner.
3. Preparing an archive for the purpose of classifying, storing, keeping, copying and archiving all registers and files related to the certification service provider's work, as well as the data, information or certificates associated therewith. The certification service provider shall have available mechanisms for accessing such archives for a period not less than (7) seven years, and shall ensure compliance with all related requirements, controls and technical standards.
4. The archive shall, particularly, contain the data related to certification certificates, including the identification process used in the event a person requests a certification certificate from the certification service provider, the double symbols issuance process, the alternative technical processes used for the purpose of providing electronic certification, electronic information management, information systems, place of business and network facilities of the certification service provider.

Article (24)

The certification service provider shall have an electronic storage space on the internet to enable it to perform its work, and such storage space shall meet have the following features:

1. To be continuously accessible to the public, with disconnection of any service related to the storage space, whether scheduled or non-scheduled, not exceeding one hour at any time; and provided that the service availability percentage does not drop below 99.95% per annum.

2. The storage space must include sufficient, complete and accurate information about the following:
 - a. Certification certificates and all data, information, documents or papers related thereto.
 - b. Lists pertaining to suspending or cancelling certification certificates.
 - c. A complete archive of the certification certificates that have been stopped, cancelled, suspended, or which have expired, for a period not less than (7) seven years.
 - d. Any information, data, documents, clarifications, prerequisites, instructions, standards or requirements which the Supreme Council may require.

Article (25)

The certification service provider shall, in the event any violation of its place of business or certification system occurs, advise the concerned department, as well as the clients affected by such violation, in writing within (24) twenty four hours from the date of its certain or presumed knowledge of such violation; whether such violation is physical or electronic.

Article (26)

The certification service provider may not merge or have joint liability with any third party except after furnishing the concerned department of the consequences on the services and clients.

The General Secretariat shall have the right to take the action it deems appropriate in light of the content of such notice and the potential impact of such merger or of joint liability on the terms of granting the license or on the interests of related parties.

Article (27)

The certification service provider shall adhere to the following:

1. Suspend the certificate validity immediately upon a request by its holder, or in case it discovers or have grounds to believe that:
 - A. The certificate has been given on the basis of wrong or untrue information.
 - B. The signature tool has been violated.
 - C. The certificate has been used for fraudulent purposes.
 - D. The information contained in the certificate has changed

2. Notify the certificate holder immediately upon suspending the certificate validity and advising the reasons for such action.
3. Remove the certificate suspension immediately if the certificate holder withdraws the suspension request, or when correctness of the information included in the certificate and the legality of using it are proven.

The certificate holder or any interested third party may object to the suspension decision issued by the certification service provider before the concerned department.

Article (28)

The certification service provider shall cancel the certificate immediately upon the occurrence of any of the following cases:

- A. If the certificate holder requests cancelling it.
- B. If the certification service provider knows of the demise of the natural person or the dissolution or liquidation of the legal person holding the certificate.
- C. If the certification service provider, after conducting detailed verification, is confident of the correctness of the reasons on which it has relied for suspending the certificate validity.

Article (29)

The certification service provider shall be liable for the damages resulting from its negligence in taking the necessary action to suspend or cancel certificates, pursuant to the provisions set out in the above two articles.

Article (30)

The certification service provider shall ensure the following:

1. Fulfilment on the part of its entrusted employees of all requirements of qualification, experience and all other standards and prerequisites stipulated in the Law and this Bylaw.
2. No entrusted employee shall have any interests or relations that conflict with his work.

The certification service provider shall maintain a register showing complete data of all employees.

Chapter (5) Consumer Protection

Article (31)

The certification service provider shall take all the necessary action to ensure fulfilment of all terms, controls and standards related to protecting privacy, personal information and data security in accordance with the provisions of the Law and this Bylaw.

Article (32)

The certification service provider shall provide adequate information to consumers regarding the reporting of any grievance in respect of any of the activities and services it renders, in terms of the form of grievance, the data it should contain, as well as the method, the time and the place for lodging it, through a clear and transparent mechanism and according to predefined procedures.

Article (33)

A service provider wishing to obtain an explicit consent from a consumer to send commercial electronic messages shall specify the following issues when requesting such consent:

- A. The purpose of requesting the consumer's consent.
- B. Sufficient information about the service provider's identity.

The consumer who receives commercial electronic communications from a service provider may withdraw such consent by sending a notice to the service provider mentioning its wish not to receive further electronic communications; and the service provider shall immediately stop sending any electronic messages to such consumer.

The electronic communication should include precise information about the manner in which the consumer can contact the service provider.

Article (34)

The certification service provider shall keep a special register to record consumers' grievances in a serialized manner in order of receipt of such grievances, and shall deal with such grievances in an effective and transparent manner.

Article (35)

The certification service provider shall decide on grievances within (30) thirty days from the date of receiving them, and shall advise the concerned department and the consumer of the result of examining the grievance and the action taken in respect thereof.

Article (36)

If the (30) thirty-day period mentioned in the above article elapses without action being taken by the certification service provider, the consumer may submit a written request in this regard to the concerned department.

The concerned department may take any action or issue any instructions to the certification service provider regarding the grievance, in accordance with the authorities and competences assigned thereto in this respect by the provisions of the Law and this Bylaw.

Chapter (5)

Suspending and cancelling the certification service provider's license

Article (37)

The General Secretariat may suspend the certification service provider's license if the certification service provider breaches any of the provisions stipulated in the Law or this Bylaw. The certification service provider shall, in compliance with a decision to stop its business, carry out the following:

1. Retain all registers and electronic data related to its business as a certification service provider, and those related to certification certificates in particular, and not to modify their content until they are disposed of in accordance with the decisions, instructions, guidelines or circulars issued by the Secretariat General.
2. Provide the General Secretariat with all technical details related to the data and its specifications.
3. Transfer the data, either wholly or partially, according to the technical controls to be set by the Secretariat General, in such a manner that preserves consumers' rights.

Article (38)

The General Secretariat may revoke the certification service provider's license in any of the following cases:

1. If the certification service provider becomes non-compliant with the terms, controls and standards set out in the Law and this Bylaw.

2. If (6) six months elapse from the date the General Secretariat issues a decision to suspend the license and the certification service provider does not remedy the reasons of suspension.
3. Upon a written request from the certification service provider to stop its business as a certification service provider.
4. If the certification service provider stops its business without notifying the Secretariat General.

Article (39)

The General Secretariat shall notify the certification service provider in writing, or by any other legal means, of the decision to suspend or to cancel the license.

The decision to suspend or to cancel a license of a certification service provider shall be published on the Supreme Council's website. By no means shall any certification service provider whose license has been cancelled obtain a certification service provider's license for a period of (5) five years subsequent to the date of cancelling its license, unless the General Secretariat otherwise decides.

Article (40)

The certification service provider, whose license has been suspended or cancelled, shall coordinate with the General Secretariat and implement any decisions, instructions or guidelines issued thereby until the certification service provider completes the liquidation of its business as a certification service provider.

Article (41)

The certification service provider shall follow the following procedures if it intends to terminate its business as a certification service provider:

1. Advise the General Secretariat at least (3) three months prior to terminating its business.
2. Advise concerned parties in writing of its intention to terminate its business at least two months in advance.
3. After giving the notice mentioned in clause No. (2) above, the certification service provider shall allow subscribers appropriate opportunity to switch to other certification service providers.

Article (42)

After terminating its business, the certification service provider shall take all the necessary measures to maintain its registers and the certified certificates it had issued, for at least (7) seven years from the date of closing down its business, in accordance with the controls and terms to be determined by the Secretariat General.

In all cases, the certification service provider may not keep any copies of the registers and electronic data resulting from practicing its business as a certification service provider, for any reason in relation to its terminated business, after the aforementioned (7) seven-year period.

Chapter (6)

Secretariat General's Management of Certification Service Providers' Activities

Article (43)

Without prejudice to the provisions set out in Article No. 64 of the Law, the General Secretariat may, either independently or in cooperation with any competent authority, examine any grievance or claim that may be lodged against any of the certification service providers, their officers, representatives or entrusted employees, pursuant to the provisions of the Law and this Bylaw.

Article (44)

The General Secretariat shall have the right, if it is the opinion that a grievance or a claim filed against any certification service provider is serious or valid, to take all the necessary action, decisions and measures in light of the provisions of the Law and this Bylaw if.

Article (45)

The General Secretariat shall create a general register for certification service providers in the State, and shall maintain it in a hardcopy and an electronic copy, and such register shall include all data, papers and documents related to certification service providers.

Article (46)

The certification service provider shall advise the General Secretariat in writing of any modification in the data pertinent to its work as a certification service

provider within (15) fifteen days from the date on which such modification has occurred.

Chapter (7) **Approving foreign Certification Certificates**

Article (47)

The General Secretariat may approve certification certificates issued by foreign entities that have competence to issue electronic certification certificates provided any of the following conditions is met:

1. The foreign entity issuing the certificate must basically meet the rules and requirements set out in this Bylaw for licensing the practice of certification service provider's activity.
2. The foreign entity issuing the certificate must have an agent in the State licensed by the General Secretariat to issue electronic certification certificates and must have the necessary requirements and prerequisites to deal with electronic certification certificates.
3. The foreign entity must be among those entities which have been approved by the Secretariat General, pursuant to an effective agreement, as a competent foreign authority authorized to issue electronic certification certificates.
4. The foreign entity must be one of the approved or licensed entities authorized to issue electronic certification certificates by the certification authority in its native country; provided that there is an agreement to this effect between the foreign licensing authority and the Secretariat General.

Article (48)

Approving a foreign authority shall be granted upon a request submitted thereby, or by concerned parties, on the forms prepared by the Secretariat General. Moreover, the General Secretariat may approve a foreign authority, on its own initiative, in the cases mentioned in items (1, 2, and 3) of the previous article.

Article (49)

In the event a foreign authority applies for accreditation, the General Secretariat shall decide on the accreditation request, after receiving and verifying the correctness of the required documents and data, within a period not exceeding (90) ninety days from the date on which the foreign authority fulfils all requirements of the Secretariat General.

If the aforementioned period elapses without issuing the accreditation, the request shall be deemed to have been rejected; unless the General Secretariat advises the requesting authority in writing of extending the said period.

A decision to accredit a foreign authority shall be issued by the Secretariat General, and such decision shall determine the period of accreditation and the conditions for renewal thereof. The General Secretariat may, by a reasoned decision, revoke or suspend the accreditation.

Article (50)

Accredited foreign authorities may request the General Secretariat to approve the types of electronic certification certificates issued by them in accordance with the rules and controls set by the General Secretariat in this respect.
