On the approval of some of the normative legal acts for electronic signature and electronic document in the Republic of Azerbaijan

CABINET OF MINISTERS OF AZERBAIJAN REPUBLIC

"Electronic signature and electronic document" On the application of the Law of the Republic of Azerbaijan on the "President of Azerbaijan Republic Decree No. 65 dated May 26, 2004 in 1.4-, 1.5-second, at 1.6, 1.7 and 1.8 ensure the implementation of the provisions in to the Cabinet of Ministers of the Republic of Azerbaijan decides:
1. "Electronic signature validation rules", "State power and local self-management authorities to use electronic signature", " Rules of the registration and accreditation of the Center for the certificate (certificate services center) on services giving certificates for electronic signature and the use signatures", "Rules providing certificate services and carrying the certificate registry" Rule for exchange of electronic documents "shall be approved (attached).
2. This decision shall enter into force on the date of signing.

Prime Minister of the Republic of Azerbaijan A. Rasizade
Baku, January 28, 2006
№ 27

Cabinet of Ministers of the Republic of Azerbaijan
January 28, 2006 by Decree No. 27
Approved

Rules for electronic signature validation

1. GENERAL PROVISIONS

1.1. This rule has been prepared on the application of the Law of Azerbaijan Republic "Electronic signature and electronic document" on May 26, 2004, Decree No. 65 of the President of Azerbaijan the Republic in accordance with paragraph 1.4 and define the rule of validation of the electronic signature in electronic document.

1.2. Electronic signature verification is carried out in order to identify the validity of electronic documents and electronic signature and to confirm the authenticity of the owner's identity.

2. E-SIGNATURE VERIFICATION

2.1. Control, carried out by the person received electronic document or third person by using the signature

tools, on the basis of the inspection of signature.
2.2. During verification of electronic signature the certificates, time indicators, revoked certificates or cancelled certificates and other additional information can be used.

2.3. Electronic signature verification is carried out in 3 stages:
2.3.1. Checking the information of the electronic signature of the certificate of conformity;
2.3.2. a reliable determination of the certificate;
2.3.3. implementation of electronic signature verification procedure.
2.4. Electronic signature verification certificate of conformity of data to determine the identity of the certificate with the signature verification data, as well as the electronic signature creation data and information belonging to the owner of the signature verified.
2.5. During the checking the reliability of certificate it must be valid on the time of signing of electronic document, the authenticity of strengthened signature of the certificate provided by the Certificate Services Center, suspension, or cancellation of the force of the certificate, the use of the certificate in shown relations is checked.
When using the time indicator, the qualified certificate of the certificates center provided the indicator for an electronic document, restrictions on use of time indicators to be checked.
2.6. Electronic signature verification has been delegated to a third person, that person must be fulfilled verification.

3. PROCEDURE FOR CHECKING E-SIGNATURE

3.1. Electronic signature verification procedure consists of associated review of relations of signature with the signature verification data of the owner of an electronic document. Electronic signature creation and verification of specific procedures are defined by used technologies and standards.
3.2. Verification procedure for strengthened electronic signature consist of inspection of strengthened electronic signature, the hash-function (hash function is binary sequence of a arbitrary block of data to be converted mathematically or algorithmically) of the signature of the owner and checking the relations with the signature verification data. Strengthened electronic signature creation and verification procedures, as well as the procedure of calculation the value of hash-function are defined according the standards accepted by the Ministry of Communications and Information Technology of the Republic of Azerbaijan.

4. THE REQUIREMENTS FOR RELIABLE VERIFICATION OF E-SIGNATURE

4.1. Reliable verification of the electronic signature for this process will be carried out in accordance with the standards and other requirements and obtained results for verification the signature will provide the electronic document to be submitted to the user without distortion.
4.2. Electronic signature means that are used in the process of reliably verifying an electronic signature must ensure the following conditions:
4.2.1. The data used for checking the electronic signature of the person viewing the same

information must be indicated on the display of the computer;
4.2.2. electronic signature verification be conducted and its results should be provided directly on the display of the computer;
4.2.3. The contents of the signed electronic document shall be indicated on the display of the computer;
4.2.4. During verification the validity of the certificate should be checked at the same time;
4.2.5. The name of the person signing the electronic document (surname) must be indicated on the display;
4.2.6. When pseudonym is used in certificate, this fact must be indicated;
4.2.7. Detection of any changes in the electronic document must be provided.
4.3. During verification of strengthened electronic signature the electronic signature means must be certified.

5. RESULTS OF VERIFICATION OF E-SIGNATURE

5.1. The results of checking the electronic signature should be precious and cannot change.
5.2. The result is positive, negative, or may be incomplete.
5.3. If a positive result, the electronic signature is considered to be true. The positive result of verification of strengthened electronic signature used in the electronic document at the same time confirm the authenticity.
5.4. If the results of verification the electronic signature in electronic document are negative, this document is not valid.
5.5. If the results of verification the electronic signature are incomplete, additional data set to determine the authenticity of the electronic signature is required and the procedure can be repeated.
5.6. If the document has more than one electronic signature, for each electronic signature the inspection shall be conducted separately.

Cabinet of Ministers of the Republic of Azerbaijan
January 28, 2006 by Decree No. 27
Approved

State authorities and local government bodies to use the electronic signature

RULE

1. GENERAL PROVISIONS

1.1. This rule has been prepared on the application of Law of Azerbaijan Republic "Electronic signature and electronic document" in accordance with the Decree No. 65 paragraph 1.5 of the President of the Republic of Azerbaijan on May 26, 2004, and regulates the use of electronic signatures by the organs of state power and local government bodies.
1.2. In accordance with the Law of the Republic of Azerbaijan (hereinafter - the Law) "Electronic signature and electronic document" Article 6.1 the information systems of state power and local government bodies for exchange of electronic documents must use only strengthened electronic signature and certified signature tools.
1.3. In accordance with Article 6.2 of the Law the state power and local government bodies must only use the services of the center has been accredited in the field (hereinafter - the Center). The electronic signature creation data and certificates of any other center cannot be used.
1.4. Using the electronic signature creation data the signature is created by means of the electronic signature tools belongs to its owner. The owner of the signature creation data may have a few signatures which are used in the relations shown in their certificates.
1.5. In accordance with Article 6.3 notifications submitted to the state power and local government bodies by other physical or legal entity must be approved by its strengthened electronic signature.

2. E-SIGNATURE APPLICATION

2.1. Except as provided by the legislation of the Azerbaijan Republic, the state power and local government bodies can use the strengthened electronic signature.
2.2. For organization the use of strengthened signature by the state power and local government bodies the authority of this organization is responsible.
2.3. Division of Information Technologies of state authority and local government bodies shall organize the application of strengthened signature. In the absence of such division execution of these tasks can be delegated to any other division or person by the head of the body.
2.4. The structural section shall carry out the following services:
preparing the information required for creation the qualified certificates and submission them to the Center;
giving advice for the creation of the signature creation and verification tools to the owners of signatures;
suspension of certificates, renewal and applying to the center for revocation of qualified certificate;

in the absence of telecommunications network with the Centre of the owner of signature create them such opportunity on their own places of work;
carry out register of the signatures tools in the body;
carry out register of carriers of the signature creation data of the owner of signature;
storing the main documents to provide qualified certificate to the holder of signature;
control the use of the signature and signature creation data by the owners of signature.
2.5. The right to use strengthened signature by governing body and employees of state power, as well as request to the Center for suspension of certificates, renewal and cancellation of the certificate shall be carried out by the decision of head the body.

3. USE OF E-SIGNATURE

3.1. Creation of the signature creation and verification data by the owner of the signature may be carried out within the body or in the Center.
3.2. The name and position of the owner of signature in the body also must be indicated in the qualified certificate.
3.3. If the legislation requires the approval of the document with a seal, complete information on the competence of the owner of the signature in qualified certificate is used. This signature is equal to person's hand signature on the paper approved by the seal.
3.4. In addition a special assignment of signature, the field of its use and the text on the seal shall be indicated in the qualified certificate of strengthened signature used as a seal.
3.5. The right to use strengthened signature as a seal is given to the authorized owner of that signature in the body.
3.6. When the owner of the signature relieves his position the body is apply to the Center for cancellation the certificate belonging to him. The signature creation data of the owner of signature shall be destroyed in way without possibility for their restoration.
3.7. The owner of the signature for the execution of official duties is using signature creation data prepared only for this purpose. The signature creation data cannot be used for the purposes out of scope of his work.
3.8. In accordance with the responsibilities the owner of the signature can use only one signature creation data.

4. PROTECTION OF ELECTRONIC SIGNATURE CREATION DATA

4.1. The owner of the signature must ensure the protection of the signature creation data.
4.2. In case of breach of confidentiality of information the owner of signature shall immediately provide the information to the corresponding division of body (authority) and shall not use the signature creation data. In this case the division (authority) is carrying out urgent measures to stop the force of the certificate and to inform about that the Center. Structural division (authority) within a day officially requests the Center for cancellation of the certificate.
4.3. The following are considered as violations of the confidentiality of signature creation data:
Loss of the signature creation data carrier;
Loss of carrier the signature creation data and the subsequent finding;

Leakage of confidential information or suspicion of a serious distortion in the information system of the body;
signs of intervention to the storage facilities of carriers of the signature creation data;
signature creation data and the activation code are known to other persons;
dismissal of employees who participated in the creation of the signature creation data.
4.4. The owner of the signature is responsible for use of the signature creation data according requirements and copying them or giving to another person is prohibited.
4.5. The validity period of signature creation and verification data conventionally is 1 (one) year and shall be determined by the Center. When this time period expire the signature creation and verification data shall be replaced. Change may be conducted according plan or in a manner outside of plan. Signature creation and verification data exchange is carried out in accordance with the rules of their establishment.

Cabinet of Ministers of the Republic of Azerbaijan
January 28, 2006 by Decree No. 27
Approved

Registration and accreditation of the Center (certificate services center) providing the certificates for electronic signatures and services on the use of signatures

RULES

1. GENERAL PROVISIONS

1.1. These Rules have been prepared on the application of the Law of Azerbaijan Republic "Electronic signature and electronic document" in accordance with the Decree No. 65 paragraph 1.6 of the President of the Republic of Azerbaijan on May 26, 2004 and define the rules of registration and accreditation of the Center (hereinafter - the center) providing the certificates for electronic signatures and services on the use of signatures.
1.2. The registration data of the Center after including into the registry of certificates held by Ministry of Communications and Information Technologies of the Republic of Azerbaijan (hereinafter - MCIT) is

considered to be registered.
1.3. These Rules shall apply to foreign Centers for registration in the Republic of Azerbaijan.

2. REGISTRATION OF THE CENTER

2.1. A person who wants to act as the Center in the Republic of Azerbaijan must apply for registration to the Ministry of Communications and Information Technologies. For this purpose, a person submit an application form provided in the Appendix to these Regulations to MCIT within 30 (thirty) days before starting the activities.
2.2. "Electronic signature and electronic document" on the Law of the Republic of Azerbaijan (hereinafter - the Law) with the exception of paragraph 10.1.6, the following documents shall be attached to the application for the provision of other services:
2.2.1. certificate of state registration of the applicant and a copy of the regulations;
2.2.2. letter on the commitment on requirements specified in paragraph 8 of the Law;
2.2.3. certificates in terms of services, including a description of the procedure to determine the owner of the signature ("Certificate Policy", "Rules on the application of a certificate");
2.2.4. security measures during creation and use of electronic signature, including document about protection possibilities of the signature creation data;
2.2.5. document about services, as well as the prices on a temporary suspension of these services;
2.2.6. document about the results of the audit in accordance with Paragraph 18.3 of the Law;
2.2.7. certificates of compliance of tools used in the electronic signature and electronic document circulation.
2.3. If the Center provides services for registration of time indicators, the related documents ("Rules for registration of time indicators") shall be submitted. If the Center will provide the only registration of time indicators then during the registration shall not submit the documents specified in clause 2.2.3 and 2.2.4 of these Regulations.
2.4. The information submitted shall be approved by the hand signature and seal of authorized official of the legal person, for the individual person by his hand signature.
2.5. Documents shown in paragraphs 2.2.3 and 2.2.4 of these Regulations shall be made in accordance with the requirements of the "providing certificate services, giving the certificate and rules for carrying out the registry".
2.6. The submitted documents shall be compiled in Azerbaijan language and have 2 copies.
2.7. If deficiencies are found in the information or in documents submitted to the MCIT, the applicant shall be informed in writing about it within 3 (three) working days after receiving the documents. After elimination of shortcomings the documents can be resubmitted to the MCIT.
2.8. Consideration of the documents and decision on the registration of the center shall be carried out in 30 (thirty) days.
2.9. According to paragraph 9.7 of the Law the registration of Center may be refused in the following cases:
2.9.1. If the applicant does not comply with the requirements of the law;
2.9.2. information and documents submitted does not comply with the requirements of the law;
2.9.3. if the applicant submitted false information;
2.9.4. If according to the results of the security audit of information system of the Center the applicant cannot function as a possible bidder;

2.9.5. certification of applicant or registration of time indicators does not comply with the requirements of the law and other normative legal acts;
2.9.6. If an applicant has debt to the state;
2.9.7. In other cases envisaged by the legislation of the Azerbaijan Republic.
2.10. The rejection of registration must be justified and the applicant should be informed in 3 (three) working days after receiving these documents.
2.11. Applicant may appeal against the decision on refusal of registration of the Center in administrative order and (or) to the court. [1]
2.12. In 1 (one) working day after the date of registration of a resolution the information about an applicant includes in the MCIT " Register of certificate services centers" and includes in the certificate issued to the applicant.
2.13. In the following cases the registered Centers should report in 7 (seven) working days to the MCIT on the changes made:
2.13.1. Legal persons and physical persons carrying out business activity without establishment of legal entity when state registration data has changed;
2.13.2. Change of address for a physical person.
2.14. Center should submit to the MCIT the relevant document in 15 (fifteen) working days if any changes of information and documents submitted during registration are happened.

3. ACCREDITATION OF THE CENTER

3.1. The documents specified in item 2.2 of these Regulations Accredited in the Center shall include the following for accreditation of the Center:
3.1.1. Qualified and trained staff for specific information;
3.1.2. Provision of services and procedures related with the certificates;
3.1.3. Certificate of Compliance of information protection tools.
3.2. Accredited Center provides services for state power and local government bodies. The document on the results of examination of the information system is added to the documents referred in paragraph 2.2 of these Regulations at the time of registration of the Center.
3.3. Time period are indicated in terms of Rules 2.7, 2.12, and the relevant requirements shall also apply during accreditation.
3.4. If necessary, the MCIT can be acquainted directly with the Center's facilities.

4. TERMINATION OF REGISTRATION AND ACCREDITATION OF THE CENTER AND CANCELLATION OF OPERATION

4.1. Termination of the Center's activities is carried out in accordance with the civil legislation of the Azerbaijan Republic.
4.2. Termination of registration and accreditation and claiming of cancellation of the activities of the Center are possible in the following cases:

4.2.1. Submitted for registration and accreditation of the Center the information and documents are not correct or invalidated;
4.2.2. The Center violates the requirements of Law and other related legislative acts for more than two times.
4.3. The Center announces via the mass media and other means the owners of the certificates, guarantee certificates, the certificate services centers with concluded agreements and MCIT for at least 30 (thirty) days prior to the termination of the activity.
4.4. After passing 30 (thirty) days after the issuance of announcement the cancellation of certificates is carrying out in the Center.
4.5. The accredited center in 30 (thirty) days after the announcement of the termination of activities with the permission of holders of signature the qualified certificates and the users information shall handed over to another center or to the MCIT. Not returned certificates shall be canceled or given to the MCIT for storage in accordance with paragraph 15 of Law.

Appendix to the regulations for registration and accreditation of the Center (certificate services center) providing the certificates for electronic signature and services on their use

Ministry of Communications and Information Technologies of the Republic of Azerbaijan

APPLICATION

1. Name of applicant Center _____

name of center

2. Legal address _____

3. Internet address _____

4. Legal status _____

5. Phone number fax _____

6. VAT _____

7. Types of service

_____

_____

_____

_____

The registration of the center (accreditation) is requested.

_____

(signature)

Seal

Cabinet of Ministers of the Republic of Azerbaijan
January 28, 2006 by Decree No. 27
Approved

Providing the certificate services, giving the certificates and carry out registry of certificate

RULES

1. GENERAL PROVISIONS

1.1. These Rules "Electronic signature and electronic document" on the application of the Law of the Republic of Azerbaijan of the President of the Republic of Azerbaijan on May 26, 2004, in accordance with paragraph 1.7 of the Decree 65 regulates organization of the work of certified service centers (hereinafter - the Center), including certification services, providing certificates and their registration.
1.2. These Rules have been apply to the activities of certificate services centers operating in the Republic of Azerbaijan and accredited certificate services centers (hereinafter - the accredited center). The activities of centers that serve corporative information systems taking into account the requirements of the "Electronic signature and electronic document" Law of Azerbaijan Republic (hereinafter - the Law) are governed by internal regulations.

2. CERTIFICATE SERVICES AND RESPONSIBILITIES OF PARTIES

2.1. The registered center may provide the following services for use of electronic signatures:
issuance of the certificate;
suspension of the certificate, renewal and revocation of the certificate;
provide information on certificates according to requests;
registration of time indicators;
creation of an electronic signature;
provide advice on the use of signature.
2.2. The accredited Center carrying out services specified in the paragraph 2.1 of these Regulations for qualified and strengthened electronic signature.
2.3. The accredited Center should provide the following for reliable services:
a) shows directory and protect it, provides services of reliable and immediate implementation of the revocation of the certificate;
b) issuance of the certificate, revocation date and display the exact time;
c) inspect the information about the owner of the signature according the law;
d) has well-educated, experienced, skilled staff using administration and management methods (especially management, electronic signature technologies and ability to implement security measures) in accordance with the requirements accepted in the field of certificate services;
d) uses reliable systems and software tools providing technical and cryptographic security;

e) takes measures against the falsification of certificates, when creating the electronic signature data in the Center ensures confidentiality during the process of creation;
g) for protection of the information implements techniques, cryptographic and organizational measures established by the requirements and standards;

f) carry out the activity as well as has financial resources to pay for damage;
g) in accordance with the legislation on the protection during the rendering of services of all collected information about qualified certificates;
j) do not keep and copy illegally the electronic signature creation data of the owner of the signature;
h) before conclusion of agreement with the owner of the signature of the certificate inform him in clear writing about his certificate and use of the signature tools, including limitations on the use of the certificate, the Center's legal status and accreditation status, investigation of claims and settlement of disputes;
x) to storage certificates use the systems that meet the following requirements:
- Only authorized persons have access and correction possibilities;
- Verification of information authenticity;
- General public search of certificates and the information about certificates is opened only with the permission of the owner's signature;
- The technical changes that contradict to the security requirements is known to the operator;
- Security of programs and technical tools of certificate services, keeping tools in the protected rooms and disallow outsiders to enter these rooms.

2.4. Signature creation data of the center's can be used only for confirmation of the information about certificates and time indicators.
2.5. Centers must provide reliable, secure services in accordance with the terms of the agreement with the owner of the signature for all days of the week, a full 24 hours.
2.6. The owner of the signature must comply with the following:
a) to provide the center with complete and accurate information;
b) use the signature creation and verification data only in the relations specified in the certificate;
c) protect the signature creation data and signature tools, prevent them from the use by other persons;
d) when loosing the control of the signature creation data or presence a threat, immediately notify the Center to block the certificate;
d) to comply with other requirements specified in the "Certificate Policy".

3. ISSUANCE THE CERTIFICATE

3.1. Certificate has been issued to the applicant on the basis of their written agreement signed between a person and Centre. The owner of the signature or a person authorized to act on behalf should apply to the Center with defined application form.
3.2. The following documents shall be attached:
- A copy of the identity of the owner of the signature;
- The signature of the person authorized to act on behalf of the owner;
- A legal entity authorized to act on behalf of the person;
- The signature of the owner of the data of electronic signature verification.

3.3. If the owner of the signature created the signature verification data requests the issuance of the certificate, then issued in paper and electronic copies of the text should be submitted.
Signature creation and verification data of the owner of the signature must meet the requirements established by the Center.
3.4. If necessary, the Center may give to the applicant for use own equipment for signature verification data.
3.5. The center shall check the accuracy of the documents submitted by the owner of the signature.
3.6. Verification and certification of documents is carried out from the date of submission within two (2) working days.
3.7. If the documents submitted correctly a person who applied signing written agreement with the Centre and receive the certificate, otherwise the Center should refuse to provide the certificate.
3.8. For search of all related information about type and description of services provided in the contract, duration, prices, special conditions, and other information included in the certificate, as well as the qualified certificates should be a permission of the owner of the signature. Prices are determined by taking into account the requirements of current legislation.
3.9. The Center before signing a contract for issuance of the certificate should inform the owner of the signature about regulations for use of certificates and signature tools, the legal and accreditation status of the Center.
3.10. Signature of the owner of the certificate should be submitted in paper and electronic form. Two (2) copies of certificate shall be prepared on official letterhead paper of the Center and approved the signature of the authorized person and sealed. After signing by the owner of the signature a copy of paper certificate will be returned to the Center. Electronic form of certificate shall be approved by the strengthened signature of the Center.
3.11. After determination the personality of the owner of signature in the Center, the signature creation and verification data written on carrier, certificate on the paper, as well as obtaining information provided by the Center he is signing in the relevant journals.
3.12. The Center includes issued certificate to the "Register of issued certificates" and from that moment it considered as published.
3.13. Period of validity of issued certificates shall not be less than three (3) years, signature creation and verification data conditionally is 1 (one) year.

4. SUSPENSIION OF A CERTIFICATE, CERTIFICATE RENEWAL AND REVOCATION

4.1. After issuance of certificate the Center can suspend, renew and revoke it in the cases specified in paragraph 13 and 14 of law. In this case, the Center makes registration of the changes in the "Register of Certificates".
4.2. The owner of the signature must apply to the Center for suspension or renewal of the certificate. Center immediately takes appropriate action in accordance with the application, informs the owner of the signature and makes registration of the changes in the "Register of Certificates".
4.3. The owner of the signature shall provide the relevant information within 3 (three) hours to the Center in the following cases of violation of confidentiality of signature creation data:
loss of the carrier for signature creation data;
loss of the carrier for signature creation data and its subsequent finding;

leakage of confidential information in the information system or in case of serious doubts;
signs of interference with the signature creation data carriers or storage facilities or in case of doubts;
signature creation data and the activation code are known to other persons;
employees who participated in the creation of the signature creation data are leaved their job.
4.4. If the confidentiality of signature creation data of the Center is violated, the Center is carry out urgent measures to revoke the qualified certificate and change the signature creation data.
In this case, the Center informs serviced owners of the signature and provides free of charge replacement of certificates with the signature creation data.
4.5. Suspension, renewal and revocation of certificate in cases of violation of confidentiality the procedures of changing the signature creation data are kept by documents regulating the activities of Centers.

5. REQUESTS ABOUT CERTIFICATES

5.1. The users of the Certificate services may apply to the Center to present them the information about issued certificates, validation of the signature verification data belonging to the owner of the signature on the certificate.
5.2. Except for cases with no permission of the owner of the signature, the Center may provide other information about the status and certificate on request about the certificate.
5.3. Services about certificates provided by the Center on the request are free of charge.
5.4. The Centers can carry out a review of certificates in the real-time.

6. REGISTRATION OF TIME INDICATORS

6.1. During the registration of time indicators, creation of time indicators, presentation to user, registration and storing them shall be carried out.
6.2. If the Center provides the service of registration of time indicators, beside the general requirements it must follow the relevant requirements related with the registration of time indicators and carry out the activities on the basis of relevant regulatory document. If the Center provides services only on registration of the time indicators the activities related with the certificates should be regulated by the governing documents.
6.3. In the time indicators the Baku time with precision of a second synchronized with the world time is used and at the moment of creation is registered with strengthened electronic signature.
6.4. Verification of the time indicator is based on the user's signature information.
6.5. If the registration of time indicators is carry out in violation of existing requirements, in particular, the accuracy of time is not precise or signed with not valid qualified certificate, the time indicator is not considered to be a true.

7. CREATION OF ELECTRONIC SIGNATURE

7.1. Centers providing technical tools to owners of the signature give service for creation the electronic signature.
7.2. The owner of the signature freely using the signature creation data creates an electronic signature.

7.3. The Centers are responsible for the security of technical tools and the signature creation data of the owner of the signature.

8. ADVISE ON THE USE OF A SIGNATURE

8.1. The Centers carry out consultation service for proper and effective use of electronic signature by the owner of the signature.
8.2. In accordance with Paragraph 17.2 of the Law, before signing the contract notification of the owner of the signature about certificate and the rules for using of signature tools do not belong to this service.

9. CARRYING OUT THE REGISTRY

9.1. Registry is the list carried out by the Centers and approved by their strengthened signature. The Center creates "Certificates registry" and "The list of revoked certificates" and other lists (for example, the "delta" list).
9.2. The following information shall be included in the registry:
- The certificate serial number;
- The signature of the owner of the information;
- The certificate validity period (start and end time of the period, date);
- Suspension or revocation of the certificate, date and reason.

9.3. Application to registry and to the lists should be provided within 7 days, 24 hours a day.
9.4. The lists of active, suspended and revoked certificates must be automatically implemented at not later than 3 hours.
9.5. The time period between of request for issuance of a certificate and entering data into a register in the Center should not exceed 72 hours and in accredited Center 24 hours.
9.6. Center should remove invalid certificates from the register and archives them.
9.7. During carrying out register the following should provide:
Only authorized employees should enter the information into the registry;
Unauthorized change of information should be prevented;
Measures should be taken to prevent unauthorized intrusion.
9.8. The procedure to carry out register should be considered in the documents regulating the activities of Centers.

10. REQUIREMENTS RELATED TO THE OPERATION OF CENTER

10.1. The establishment of the Center's activities in accordance with the requirements of the law and the implementation of 1, its reliability and ensuring the security, as well as for the purpose of disclosure to users, each Center should prepare regulatory documents and must follow them.
10.2. Each Center must carry out its activities according to the regulatory documents such as "Certificate Policy" and "Rules of the certificate practice".

10.3. "Certificate Policy" is the basis of the Center’s activity and "Rules of the certificate practice" determine the procedure of its implementation.
10.4. "Certificate Policy" is a document containing the information about issuance and publication of certificates, as well as the services of the Center's.
10.5. " Rules of the certificate practice" cover security measures during services, issuance of certificates, the suspension, renew and revocation information, contain the possibility to request certificates.
10.6. If the Center provides services of registration of the time indicator, "Rule for registration of time indicators" should be prepared and followed him.
10.7. The Centers during their activity must have a technical, personnel and financial resources, as well as the financial capabilities to pay for losses of the users and should provide a reliable and continuous service.

11. REQUIREMENTS FOR SAFETY MEASURES

11.1. The Centers must provide security of activities and protection of the information about the owners of the signature on the basis of the procedures in accordance with international standards on information security.
11.2. Security procedures should include the following:
information security (management and procedural levels) activities;
financial resources and mechanisms for payment of damages;
requirements relating to staff;
protection of the equipment, as well as the of places where they are located and ensure they are used by persons with permission;
measures to prevent unauthorized access into the information systems;
measures on the prevention of unauthorized changes.
11.3. The Center should determine compliance with the security requirements and at the same time in order to establish confidence in reliability for users of services from the start of activities, taking into account every year the security audit of the information system. The results of the audit shall be submitted within 30 (thirty) days to the Ministry of Communications and Information Technology of the Republic of Azerbaijan (hereinafter - the Ministry).
11.4. Security procedures are not available to the public, the only Ministry and its authorized representatives should be introduced during implementing control functions.
11.5. Protection of security activities of the accredited Center will be provided by appointed a competent person participating in designing of information protection system, giving technical services and controlling the status of the information protection and by the information security services.

12. REQUIREMENTS FOR FINANCIAL RESOURCES

12.1. In order to carry out the activities in full accordance with the law the Center should has sufficient financial resources. Financial resources should provide the following:
- The implementation of activities;
- The acquisition of necessary equipment and facilities, and application;

- The maintenance of professional level staff;
- Conduct an audit every year to provide information system;
- Pay to users for the damage.

12.2. Depending on the size and characteristics of services the Center should have funds on the bank account to provide the activities in accordance with the requirements of the legislation.

12.3 The Centers shall determine the procedures for payment damage caused to the owner of the signature as a result of own activities. For this purpose the insurance may also provide the opportunity.

13. REQUIREMENTS FOR PERSONNEL

13.1. Centers are expected to have sufficient number of well-educated, experienced and competent staff to ensure commitments and activities.

13.2. The technical staff should have experience in at least the following areas:

security technology, cryptography, electronic signature control infrastructure;

evaluation of the technical standards for safety;

an information systems.

13.3. In the accredited Center the registration, certification, security and system administrator positions must be considered.

Registration administrator carries out creation and cancellation of certificates, determination of their respective owners of the signature at suspension and restoration of certificates.

Certification administrator is responsible for the preparation of certificates, registration of certificates and storage and use of the signature creation data of the Center.

Security administrator works in the information security services and is responsible for the information protection system of the Center.

The System administrator is responsible for the information system, software and technical complex of the Centre's.

It is not allowed to share the Security administrator position with the duties of other positions, this rule should be applied as soon as possible to other positions.

14. TECHNICAL REQUIREMENTS FOR EQUIPMENT AND TECHNOLOGIES

14.1. The Center should use certified tools for certificates and provision of electronic signature creation and verification data.

14.2. The Center should apply for audit of the information system prior to and each year after the registration and use the techniques and technologies to ensure reliable usage of the system.

14.3. If the Center provides services for creation of electronic signatures, the signature tools with the relevant technical and procedural methods must satisfy to the following conditions:

enter only once the electronic signature creation data and protect their confidentiality;

do not make a copy of the electronic signature creation data without a necessity and protect the signature from falsification with the current available technologies;

avoid using by others the electronic signature creation data of the owner of the signature.
14.4. Signature tools must not alter the data to be signed or transfer of this information to the person before the signing process should be prevented.
14.5. The Center for the purpose of information system security management and safety should use the procedures and methods recognized in the international practice in accordance with information security standards.
14.6. Signature tools used by the Center should fulfill the following functions:
controlling of the sources of information related to the issuance of certificates and their management;
checking completeness of the information exchange;
signing of the submitted information;
archiving of worked information and signing them with the e-signature;
expectation of completeness of the data stored and exchanged, as well as used cryptographic keys;
protection of the carriers of the signature creation data used by the Center;
management of request to the information resources (signature creation data of the Center, qualified certificates, the list of revoked certificates, the data stored in the other official documents;
creation and storage of information on internal audit in relation with the information security.
14.7. The Center also can use the signature tools for the following purposes:
verification of electronic signatures;
support of protocol for verification of the certificate status in the real-time;
verification of the existence of a unique identification name for qualified certificate;
use of smart cards with safety passwords, personal identification number or the of biometric identification tools for storage and utilization of signature creation data.

15. REQUIREMENTS FOR STORAGE OF INFORMATION AT PROVIDING THE CERTIFICATION SERVICES

15.1. The Centers must provide storage of the documents for the certificate services in accordance with paragraph 15 of the Law.
15.2. The valid, suspended and revoked certificates with shown usage fields, as well as other related with them documents and information should be kept in the Center within the period specified in the legislation of the Republic of Azerbaijan.
15.3. The Center provides a storage of the following documents:
15.3.1. Documents relating to the provision of services in the security certificate;
15.3.2. Signed contracts with owners of signature;
15.3.3. Copies of documents issued by the certificate of the Center;
15.3.4. Documents confirming the training of the owner of signature;
15.3.5. Documents about suspension, revocation and renewal of the certificate;
15.4. The Centers should keep documents of the current state of used technical equipment and technology.

16. STANDARDS AND TECHNICAL DOCUMENTS

16.1. The Centers must comply with the following standards and technical documents in their activities:

1	2
The overall organization of the activities of the accredited Center	ETSI TS 101 456, CEN/ISSS CWA 14167-1
Qualified certificates	ETSI TS 101 862, ITU-T Rec.X-509 v.3.
Format for the request of certificate issuance	PKCS#10
"Certificate Policy" və "Rules for certificate practice"	RFC 3647
Information system security audit and standard for expertise	ISO 15408 or similar appropriate national standard
Creation, storage or usage of signature creation data	General requirements (Common Criteria), security level EAL3 or above in accordance with ISO 15408
1	**2**
Strengthened electronic signature creation data	Complained to CWA 14169 standard and TS ISO/IEC 15408 (-1,-2,-3) or According to ISO/IEC 15408 (-1,-2,-3) at least EAL4+
Electronic signature verification	CEN/ISSS CWA 14167-1
Real-time certificate status verification protocol	RFC 2560
Algorithms and parameters	ETSI SR 002 176
The signature creation and verification of the owners of the signature	For RSA at least 1024 bit or For DSA at least 1024 bit or For DSA elliptic curve at least 160 bit Hash function: RIPEMD - 160; or SHA – 1
Signature creation and verification data of accredited Center	RSA – at least 2048 bit or DSA – at least 2048 bit or DSA elliptic curve at least 256 bit Hash function: RIPEMD - 160; or SHA - 1
Security criteria	CEN/ISSS CWA 14167-1

	ETSI TS 101 456 TS ISO/IEC 17799 or ISO/IEC 17799
Time indicators and services	ETSI TS 101 861 CEN/ISSS CWA 14167-1
"Procedure for registration of time indicators"	ETSI TS 102 023
Procedure for signature creation and verification	ГОСТ 34.310-95 Information technology. Cryptographic protection of information. Procedures for the development and validation of digital signatures based on asymmetric cryptographic algorithm.
Hash function	ГОСТ 34.311-95 Information technology. Cryptographic protection of information. Hash function.

16.2. International definitions are used

S. №	**Definitions used**	**In English**	**Abbreviations**
1	**2**	**3**	**4**
1.	Avropa Sertifikatlar Təşkilatı İnformasiya Cəmiyyətinin Standartlaşdırma Sistemi	European Committee for Standardization Information Society Standardization System	CEN/ISSS
2.	Beynəlxalq Standartlar Təşkilatı	International Standardization Organization	ISO
3.	Ləğv edilmiş sertifikatların reyestri	Certificate Revocation List	CRL
4.	"Sertifikat siyasəti"	Certificate Policy	CP
5.	Sertifikatın tətbiqi qaydaları	Certificate Practice Statement	CPS
6.	Sertifikatın vəziyyətinin real vaxtı rejimində yoxlanılması protokolu	On-line certificate status protocol	OCSP
7.	Unikal identifikasiya adı	Unique identification name	Dname
8.	Əlaqələndirilmiş ümumdünya vaxtı	Coordinated Universal Time	UTC
9.	Ümumi tələblər	Common Criteria	CC

Cabinet of Ministers of the Republic of Azerbaijan
January 28, 2006 by Decree No. 27
Approved

EXCHANGE OF ELECTRONIC DOCUMENTS

RULE

1. GENERAL PROVISIONS

1.1. This rule is prepared in accordance with paragraph 1.8 on the application of the Law of the Republic of Azerbaijan "Electronic signature and electronic document" of Decree No. 65 dated May 26, 2004 of the President of Azerbaijan Republic and determine the procedure of the exchange of electronic documents.
1.2. This rule shall not apply to electronic documents, which contain the state secret information.
1.3. Government authorities, agencies, organizations and enterprises are carrying out the exchange of the electronic documents according the directive “Clerical work in the state authorities, agencies, organizations and institutions” approved by Decree No. 935 dated 27 September 2003 of the President of the Azerbaijan Republic.

2. ORGANIZATION OF EXCHANGE OF THE ELECTRONIC DOCUMENT

2.1. Exchange of electronic documents includes:
- Formation of an electronic document;
- Adding properties and strengthened electronic signature;
- Submitting the electronic documents;
- Verification of the authenticity of electronic documents;
- Approval of receiving of an electronic document;
- Registration of received and submitted electronic document;
- Storage of an electronic document.

3. FORMATION OF ELECTRONIC DOCUMENT

3.1. The structure of electronic document should be formed as shown in the Law of the Republic of Azerbaijan (hereinafter - the Law) Paragraph 22 "Electronic signature and electronic document". The content and information about the person is addressed in the general part of electronic document.
In addition to electronic signature, as a rule, the registration number, date, address, the sender organization (person) requisites should be in the electronic document.
3.2. During the creation of electronic documents additional information on its use and submitting features (phone numbers, fax, e-mail address, name and surname of the applicant having the right to confirm the electronic document, etc.) may be provided.
3.3. The composition and design scheme of the placement of the requisites in the electronic documents must comply with the requirements of the clerical rules established for paper documents.

4. SENDING AND RECEIVING OF ELECTRONIC DOCUMENT

4.1. Before sending of an electronic document its proper design (has e-signature, the main and additional requisites) and the address are being checked.
4.2. Electronic document can be sent by sender (hereinafter - the Sender), by a person who is authorized to

act on his behalf or by information system programmed by the Sender to operate automatically.
4.3. Paragraph 27.3 of the electronic document law is accepted not to be sent by Sender in the following cases:
4.3.1. If received notification about not sending of electronic document;
4.3.2. If there is no confirmation about validity of the electronic document;
4.3.3. It became known or should have known to receiver of electronic document (hereinafter - the Receiver) as a result of checking the authenticity of electronic document that the electronic document is an automatic copy of another document.
4.4. Unless otherwise specified between the parties in the contract, the Receiver in a result of validation of the authenticity of the electronic document ensures that Sender submitted it and informs the Sender about unambiguously receiving with automatic tools.
4.5. The electronic documents can be approved in suitable manner in accordance with an agreement between the parties. The approval may be in the form of signing of electronic document with electronic signature of the Receiver or without an electronic signature with automatic notification.
4.6. If within the period specified by a Sender or shown in the contract between the parties confirmation is not received then Sender shall notify a Receiver and define a period for submission of confirmation. If in shown period confirmation is not received by the Sender, the electronic document is counted as not sent. In this case Sender can submit to Receiver the content of electronic document by other communication means.

5. VERIFICATION THE AUTHENTICITY OF ELECTRONIC DOCUMENT

5.1. The verification of electronic document using the electronic signature tools are carried out in the following steps:
5.1.1. Compliance of an electronic document to certain form and verification of the presence of necessary requisites;
5.1.2.Verification the validity of electronic signature in the electronic document.
5.2. Verification of validity of electronic signature carrying out in accordance with the "Rules of verification of electronic signature".
5.3. If verification of the electronic document gives a positive result its implementation will be accepted or it will be go for additional processing.
5.4. Verification of the electronic document with a negative result is a conflict case and shall be settled in accordance with procedures agreed between the parties.

6. REGISTRATION OF ELECTRONIC DOCUMENT

6.1.The registration of electronic documents is carried out in electronically or in paper journals.
6.2. During the registration of electronic documents by electronic journals the protection of data against unauthorized interventions should be provided to prevent accidental or false destruction.

7. STORAGE OF ELECTRONIC DOCUMENT

7.1. In accordance with Paragraph 29 of the Law at storage of an electronic document must be satisfied the following conditions:
7.1.1. Electronic document keeps the structure of creation, transfer or acceptance;
7.1.2. Electronic document gives an opportunity to identify the Sender, the Receiver and a time of delivery;
7.1.3. The information in the electronic document may be used to further reference;
7.1.4. The term of storage of an electronic document is intended to be not less the time of a paper document;
7.1.5. Determined in accordance with the legislation and with the consent of the parties let comply to other conditions.
7.2. Maintain the appropriate journals during storage of electronic documents, electronic signature verification data (their certificates) and store the programs providing verification of electronic signatures.
7.3. The appropriate connection between the electronic document and verification data (synchronization) must be provided for examination of conflict situations during storage of electronic documents.
7.4. Electronic archives should be protected from unauthorized interference, accidental destruction or distortion.

8. INFORMATION SECURITY IN THE EXCHANGE OF ELECTRONIC DOCUMENT

8.1. Software, technical, administrative and organizational measures must be taken into account to ensure the information security during the exchange of electronic documents.
8.2. The appropriate tools may be used to protect confidential and personal information contained in the electronic document.
8.3. In addition to electronic documents, the electronic signatures and their requisites should be protected.
8.4. The organization of electronic document circulation in state bodies during the implementation of information security requirements shall be carried out in accordance with the requirements specified by the legislation of the Republic of Azerbaijan with the application of certified programs, technical tools and organizational measures. Certified tools should be used with strict compliance with operational requirements and conditions established in the documents.

_____