**DECISION**

**NO. 69, dated 27.1.2016**

**ON THE APPROVAL OF THE REGULATION**

**"ON ELECTRONIC IDENTIFICATION AND TRUSTED SERVICES"**

Pursuant to Article 100 of the Constitution, Articles 14, 19, 28, 52 and 54 of Law no. 9880, dated 25.2.2008, "On Electronic Signature", and Articles 5, 17 and 35 of Law no. 107/2015, "On electronic identification and trusted services", upon the proposal of the Minister of State for Innovation and Public Administration, the Council of Ministers

DECIDED:

1. Adoption of the Regulation "On Electronic Identification and Trusted Services", according to the text of Regulation and Annex 1, attached to this decision.

2. All subjects that have started the activity before the entry into force of this regulation, within 30 (thirty) days from the date of its approval, should start the registration procedures provided for in law no. 107/2015, dated 1.10.2015, "On electronic identification and trusted services", and in this regulation. Those entities registered with the Authority for the provision of electronic signatures, according to Law no. 9880, dated 25.2.2008, "On Electronic Signature".

3. Decision no. 525, dated 13.5.2009, of the Council of Ministers, "On the adoption of the regulation on electronic signature", is abrogated.

4. The National Authority for Electronic Certification is charged with the implementation of this decision. This decision enters into force after its publication in the Official Notebook.
PRIME MINISTER

**Edi Rama**

**REGULATION**

ON ELECTRONIC IDENTIFICATION AND TRUSTED SERVICES

I. GENERAL PROVISIONS

1. Scope of the Regulation Pursuant to the law no. 9880, dated 25.2.2008, "On Electronic Signature", and Law no. 107/2015, dated 1.10.2015, "On electronic identification and trusted services", this regulation determines:

a) the method of registration for qualified service providers with the National Authority for Electronic Certification (Authority);

b) the necessary functional, technical and legal requirements to be owned and implemented by qualified service providers, pursuant to Articles 19 and 28 of Law no. 9880, dated 25.2.2008, "On Electronic Signature", and Article 17 of Law no. 107/2015, "On electronic identification and trusted services";

c) procedures for the abrogation and derecognition of qualified certificates and ways of informing, pursuant to Article 14 of Law no. 9880, dated 25.2.2008, "On Electronic Signature", and Article 15 of Law no. 107/2015, "On electronic identification and trusted services";

d) conformity and assessment bodies, pursuant to article 52, of law no. 9880, dated 25.2.2008, "On Electronic Signature", and Article 33, of Law no. 107/2015, "On electronic identification and trusted services";
e) recognition and acceptance of electronic identification of trusted and foreign products, pursuant to Article 54 of Law no. 9880, dated 25.2.2008, "On Electronic Signature", and Article 34, of Law no. 107/2015, "On electronic identification and trusted services".

2. Definitions

The terms used in this regulation have the same meaning as those provided in Law no. 107/2015, "On electronic identification and trusted services".

II. REGISTRATION

3. Registration in the Authority

a) The Trustee is registered with the Authority within 30 (thirty) days from the date of commencement of the activity and submits the necessary documentation confirming that the entity meets all the conditions set forth in the law and this regulation;

b) The Authority has the right to request additional information or to prepare detailed technical guidance regarding the technical, professional and legal requirements set forth in the law and this regulation and related to the exercise of the activity by qualified trust service providers or a conformity and assessment bodies;
c) Registration in the authority must, at a minimum, be accompanied by the following data and documents:

i) the name and address of the qualified service provider;

ii) relevant evidence of commencement of the activity;

iii) documents proving that it meets the legal, professional, technical and financial requirements set forth in the law and this regulation;

iv) any other document relating to the activity to be carried out, according to the list of documents approved by the Authority.

d) The formulation of all documentation submitted to the Authority shall be in accordance with the legislation in force in the Republic of Albania.

III. LEGAL, TECHNICAL, PROFESSIONAL AND FINANCIAL CONDITIONS

4. Legal Reliability Qualified service provider that commences the activity must prove that it meets the following requirements:

a) To be a legal or natural person registered in the Republic of Albania, according to the legislation in force ;

b) Not to be sentenced by a final court decision for any of the following offenses:

i) theft;

ii) fraud;

iii) corruption;

iv) Money laundering;

v) Participation in criminal organizations;

c) Have paid all tax liabilities, as evidenced by the relevant documentation for these obligations.

d) Not be in the process of bankruptcy and its capital is in the process of confiscation, and when its business activity is suspended or is under way for any of the matters referred to in point “b”, point 4, this regulation.

5. Technical reliability

5.1 General technical requirements fulfilled by the qualified trust service provider

a) A qualified service provider for security management applies methods that are in accordance with internationally recognized standards for electronic identification and trusted services ;

b) The reliability of the system used and the technical and cryptographic security of the processes to be carried out shall be confirmed after passing the tests required by the a conformity and assessment bodies ;

c) The methods used for assessing the security of the system used shall be based on the methods provided by the standards ISO 15408 and ISO 27001 (International Standardization Organizations) or more advanced or equivalent methods that are capable of assessing security;

d) Any equipment or system used for certification by a qualified service provider for the creation, signature, storage and administration of certificates should be designed for this purpose only;

e) Any system and technical equipment used by a qualified service provider for the provision of a service for the creation, storage and administration of certificates shall be designed for use only for this purpose and for no other;

f) Testing to verify the reliability of systems and equipment used by trusted and requested service providers pursuant to letter "b" of point 5.1 of this regulation shall normally take place every 2 (two) years and whenever there are changes in the system, which require verification of confidentiality after each change;

g) The creation, storage and use of private keys of each qualified service provider must be carried out within the system, with a protection profile, in accordance with the safety requirements of the EAL level 3 (Assessment of the Level of Guarantee) safety or more advanced, in accordance with ISO 15408 or other specifications with equivalent security levels;

h) The certification service provider uses equipment and technology to enable the performance of basic functions as follows:

i) testing to prove the origin of the information received and exchanged;

ii) testing the integrity of the exchanged messages;

iii) archiving information on the work done with respect to issuing electronic certificates;

iv) ensuring the integrity of the stored and exchanged data, including the cryptographic keys used;

v) the storage of private keys used by the qualified service provider;

vi) administration of access to information sources related to electronic identification and trusted data creation, list of certificates that have been revoked / abolished and the official correspondence stored in the system;

vii) creation and archiving of internal audit reports;

i) Each qualified service provider shall carry out the following functions through the equipment and technology installed by him:

i) to test electronic identification and trusted services in accordance with the technical requirements provided by the European Telecommunication Standards Institute ( ETSI) and by the European Committee for Standardization (CEN / ISSS);

ii) be able to use the OCSP (Status Online Certificate Protocol on-line) protocol;

iii) the Certification Service Provider, for equipment and technology standards not specified in this Regulation, uses the international standards of specialized bodies such as the European Telecommunications Standards Institute (ETSI), the European Committee for Standardization (CEN / ISSS) .

5.2 Technical Documentation Required by Qualified Trusted Provider A. Statement of Practice and Certified Trustee Certification Policy

1. A qualified Trusted Provider will determine the certification policies and practices for trusted services that offers. These documents, after being approved by the Authority, are published and communicated to third parties.

2. A qualified service provider shall notify the Authority of any changes it intends to carry out in the practice statement and certification policy. Upon approval by the Authority, these documents shall be immediately available, in accordance with point 1.

3. A qualified service provider shall establish in its practices specific provisions which provide for termination of service.

B. Documentation on Terms and Conditions for Providing Electronic Identification and Trusted Services

A qualified Trusted Provider makes available to Applicants and Product Holders providing all necessary terms and conditions. These terms and conditions shall specify:

a) the policies to be applied for the provision of trusted service;

b) any restriction on the use of the service;

c) the obligations of the holder of the certificate;

d) restrictions on the use of services, including limitations on damages arising out of the use of services in excess of these limitations, if any;

e) Applicable legislation;

f) procedures for appeals and settlement of disputes;

g) Information on the ways of contacting a qualified service provider. Certificates holders will be immediately notified of the required changes to the terms and conditions.

C. Information Security Policy Document

A qualified service provider must have an information security policy document that sets out the approach of a qualified service provider to manage its information security. Especially:

1. The information security policy of a qualified service provider is documented, enforced and maintained, including security controls and operating procedures for systems and information support tools provided by a qualified service provider trusted.

2. The information security policy of the trusted provider of trusted services and inventory of information security assets under point 6.4 shall be revised at scheduled intervals and in any event when changes occur. Any change that will affect the security level should be reflected in the policy document. Configuring trusted service provider systems will be regularly checked for changes that violate security policies.

6. Professional Credibility

6.1 Reliability of the Provider

The qualified trust service provider guarantees that it operates legally and reliably by providing evidence that it meets the applicable legal and technical requirements under the applicable electronic identification and trusted legislation. The management and operation of a qualified service provider rely on credible policies, which consist in:

a) the organization in such a way that the creation and issuance of electronic certificates is separated from any other activity;

b) the forecast of performing the creation, storage, use and restoration of private codes, with the simultaneous participation of at least two authorized persons;

c) a clear definition of the protected physical area, where all control codes are kept and where the certificates issued are managed and the authorization of certain employees enjoying the right of access to the protected area;

d) the practice of providing a trusted service, which should be non-discriminatory;

e) service accessible to all applicants, as specified in the terms and conditions set by the qualified service provider;

f) sufficient financial resources to cover damages caused in accordance with law no. 9880, dated 25.2.2008, "On Electronic Signature", and Law no. 107/2015, "On electronic identification and trusted services";

g) policies and procedures for resolving with understanding the complaints and disputes with customers or other parties about the security of services or any other related matter.

6.2 Personnel Credibility

The management and operation of a trusted provider of trusted services relies on policies that determine the division of duties and areas of responsibility according to the following criteria:

a) Employ staff who possess the expertise, credibility, experience and qualifications required and who have received training regarding security and rules of personal data protection for services provided by job function;

b) Employs staff in accordance with letter "b" of point 4 of this regulation;

c) Establishes disciplinary sanctions for staff in case of violation of the policies or procedures established by it;

d) The roles and responsibilities of security, as specified in the trusted security service provider's management policy, shall be documented in job descriptions or other approved documents for dedicated personnel. Trusted roles, which depend on the reliability of the trusted service provider's operation, must be clearly identified. Responsibilities on these roles are:

i) security officers are responsible for administering the implementation of security practices;

ii) system administrators are responsible for the installation, configuration and maintenance of reliable systems of a qualified service provider trusted service provider;

iii) system operators are responsible for the operation of trusted systems on a daily basis and to perform support and recovery of the system;

iv) system auditors are responsible for controlling the archives and auditing the systems logs of the qualified service provider;

e) Determines in the description of the work of the employees the assignment of duties, access categorized according to the levels and privileges;

f) Ensures that trusted roles personnel are not in conflict of interest, in order to avoid the activity of a qualified service provider.

6.3 Asset Management

A qualified trusted provider provides an adequate level of asset protection, including asset information. It also keeps an inventory of all asset information and assigns a classification in accordance with the risk assessment. All assets must be identified and invented. A qualified service provider must document the importance of these assets. The asset inventory should contain all the information needed to restore disaster-led services. For the foregoing, the classification of information should be documented for each asset. Based on the importance, business value and security classification, the level of protection should be proportionate to the importance of the asset.

Assets can be of different types. Some examples are:

- Information: databases, electronic files, contracts and agreements, system documentation, user manuals, training materials, operational and support procedures, business continuity plans, audit trails, archived information etc .;

- Software assets: applications, system software, software development tools etc .;

- Physical assets: computer equipment, communication equipment, mobile media, etc .;

- Services: computer and communications services, support services such as heating / cooling, electricity etc.;

-Human resources: employees and their qualifications, skills and experience. Each asset must be owned by a designated structure of a qualified service provider. The asset owner should be responsible for the proper classification of assets as well as the periodic review of the restriction and rating of access, taking into account applicable control access policies.

6.4 Management of Information Storage Media

Each medium is handled securely, in accordance with the requirements of the information classification scheme. Media containing sensitive data is eliminated when it is no longer needed.

6.5 Access Control

Access to a qualified service provider system should be restricted to authorized individuals only. Levels and access schemes should be in compliance with the relevant specifications in the standards adopted by the European Telecommunications Standards Institute (ETSI) and the European Committee for Standardization (CEN / ISSS).

6.6 Cryptographic Controls

Security controls shall be implemented for the management of any cryptographic key and / or cryptographic device based on established standards and compliance with the security requirements that these devices provide throughout their life cycle.

6.7 Physical and environmental security

The qualified trust service provider controls physical access to system components whose reliability is critical to trusted services and minimizes the risk associated with physical security. System components and standards for physical and environmental safety are defined in policy documents in accordance with the relevant specifications in the standards adopted by the European Telecommunications Standards Institute (ETSI) and the European Committee for Standardization (CEN / ISSS).

6.8 Operations Security

A qualified service provider uses trusted systems and products protected by modifications and guarantees technical security and process reliability. The manner of their use and protection is set out in Annex no. 1, attached to this Regulation, in accordance with the relevant specifications in the standards approved by the European Telecommunications Standards Institute (ETSI) and the European Committee for Standardization (CEN / ISSS). 6.9 Network Security

Qualified trust service provider enforce relevant network and system protection legislation against possible attacks and defines protection policies in accordance with the relevant specifications in standards approved by the European Standards Institute Telecommunications (ETSI) and the European Committee for Standardization (CEN / ISSS).

6.10 Incident Management

A qualified trust service provider raises an information technology process monitoring system related to system access to incident management. The mode of operation of this system is set out in Annex no. 1, attached to this Regulation, in accordance with the relevant specifications in the standards adopted by the European Telecommunications Standards Institute (ETSI) and the European Committee for Standardization (CEN / ISSS).

6.11 Data retention and collection of evidence

The qualified trust service provider retains all information about the data generated

during the work processes, in particular for the purpose of obtaining evidence in legal proceedings and for the purpose of ensuring continuity of the service, in accordance with law no. 9887, dated 10 March 2008, "On the protection of personal data". The procedures for data retention and collection of evidence are set out in the policy document drafted and approved by the qualified trust service provider in accordance with Albanian legislation and with the relevant specifications in the standards approved by the European Telecommunications Standards Institute (ETSI) and by the European Committee for Standardization (CEN / ISSS) EC.

6.12 Continuity Management

The qualified trust service provider has the obligation to develop procedures to evaluate and ensure continuity of activity in emergencies arising from natural disasters, human error, intentional interventions. In the event of disasters, including the private key signing of the root key signature or access credentials on the systems which enable the provision of trusted services, the qualified trust service provider has the obligation to guarantee continuity of work and data retrieval.

6.13 Risk assessment
A qualified trust service provider, after identifing, analyzing and evaluating the risk of providing trusted services, including management and technical issues, applies appropriate risk treatment measures. Risk treatment measures should ensure that the level of safety is proportionate to the risk levels.
The trusted service qualified provider determines all the security requirements and operational procedures that are required to implement the selected risk treatment measures, which are documented in the information security policies and the trusted service statement. The assessment is reviewed and updated continuously.

6.14 Interruption of the trusted service provider services

a) In cases of the activity termination of a qualified service provider, the continued maintenance of the information must be continually ensured to verify the validity of the electronic identification or trusted services provided before termination of the activity. The procedures for termination of the activity are defined in an updated plan, which must contain:
i) procedures for ensuring continuity of the revocation status;
ii) logos archive of events for the period of time the activity is offered, OCSP
iii) informing all the holders(owners) of the products and services whose provision will be terminated by the qualified provider of the trusted service;
iv) obligations that are transferred to a qualified service provider in order to keep all the necessary information and provide functioning evidence of a qualified service provider who has ceased operations;
v) ways of destruction or revocation of private keys, including secondary copies, so that private keys are not accessed and used further;
b) A qualified trust service provider, sets out a plan to cover the expenditure necessary to fulfill these minimal demands;
c)A qualified service provider holds or transfers his or her public key or/and qualified certificates issued up to the fulfillment of the obligations matured during the activity, to a trusted party.

7. Financial Reliability

a) The qualified trust service provider, demonstrates that it has the necessary financial guarantees to cover the legal

responsibilities deriving from Article 41 of Law no. 9880, dated 25.2.2008, "On Electronic Signature", and Article 29 of Law no. 107/2015, "On electronic identification and trusted services". The minimum financial guarantee should be 100 (one hundred) million ALL;
b) The value of the security specified in letter "a", point 7 of this regulation is covered by a deposit or bank guarantee or unconditional insurance policy issued by a licensed insurance company and covering this service categories. Financial guarantees must be valid throughout the service provider's activity period and must cover all the secured events;
c) Notwithstanding the financial guarantee provided for in point (a) of point 7, a qualified trustee service provider must be insured against any damages that may result for any qualified certificate issued to the signature holder from any breach of contract,breaks of the law or malfunctioning of its product, as follows:

i) up to 5 (five) million ALL for any damage caused because of some financial limitations or other restrictions imposed by the parties to the Qualified Certificate ;
ii) up to 10 (ten) million ALL, when the qualified certificate is unlimited and universal. The requirements above do not prohibit a qualified service provider from voluntarily offering insurance policies of higher value than those provided for in this point.

8.The obligaton to provide information

The qualified trust service provider is obliged to inform the applicant of a qualified certificate in respect of:
a) secure means of creating electronic identification for the trusted service and measures taken in the event of loss or suspicion of appropriation of such means;
b) means of storage and clarification of the confidentiality of personal data used;
c) security measures applied by qualified trust service provider, of the trusted service for the protection against unauthorized access to electronic identification tools for the trusted service as well as the applicant's rights as a subject of personal data;
d) potential restrictions that will have a qualified certificate;
e) notifying that the use of a qualified certificate is voluntary;
f) the notification of the revocation procedure;

g) notification of ways to relosve disputes and appeals
The information provided under this letter must be comprehensible to the clients and be made known to any interested party.

## IV. CONFORMITY AND ASSESSMENT BODIES

9. Recognition as a conformity and assessment bodies
a) An organ (body) that complets the following conditions is known as an organism:
i) has all the necessary certificates or knowledge relating to the certification of a qualified service provider with the equipment and processes associated with a qualified certification service recognized by the best international practice or standardization organisms in this field;
ii) the a conformity and assessment bodies (organism) and all its personnel meet all the requirements provided for in point (b) of point 4 of this regulation;
iii) there is no conflict of interest and its staff is not involved in any activities that may affect their professional and independent evaluation;
iv) provides full transparency for the activity it performs and has detailed reports on each activity performed;
v) has in its possession all the necessary staff and tools related to the specific field or the specific activity that is going to be certified
vi) guarantees the confidentiality of the

information received from the duty and makes it available to the Authority whenever the activity is interrupted.

b) The Authority shall draw up a complete list of specific requirements for each condition specified in letter "a", point 9, and publish an updated list of test and confirmation organisms;
c) The Authority may recognize a conformity and assessment bodies for all or a part of the processes or components related to electronic identification and the trusted service;
d) The a conformity and assessment bodies before starting the testing and confirmation services,must make known the fees that will be applied to qualified service providers;
e) The a conformity and assessment bodies certifies in writing or refuses completely or partially the controlled entity. The conclusions became known to the Authority within the deadlines set by the Authority itself;
f) The conflicts between a conformity and assessment bodies and qualified service providers are solved with the Authority intervention and / or in court;
e) In cases when the Authority has no a conformity and assessment bodies , the activity of a qualified service provider is deemed to be valid by the Authority and not interrupted, but the deadlines for inspection are halved.

10. Exceptions

Foreign products that are accompanied with the manufacturer's declaration certifying compliance with international technical standards, as confirmed by the a conformity and assessment bodies in the country of origin are exceptioned by the evaluation.

**V. PROMOTION, REVOCATION AND INFORMATION OF THE PARTIES**

11. Abolition and revocation of certificates

The abolition and revocation of the certificates shall be made only in the cases provided by Law no. 9880, dated 25.2.2008, "On Electronic Signature", and Law no. 107/2015, "On electronic identification and trusted services".

12. Actions that accompany revocation / abolition

a) A revoked / abrogated certificate can no longer be used under any circumstances;

b) The qualified trust service provider of the trusted service enables the immediate suspension of the certificate until the release and verification or not of the reasons for the abolition or revocation of the certificate;

c) The qualified trust service provider immediately notifies the holder of the electronic certificate about the suspension / revocation of the relevant certificate and records the delivery of the notice in time;

d) The Qualified Provider of the trusted service, provides continuous certificate revocation service, 24 hours a day for the whole week, including holidays, so that the holder of the qualified certificate or legally authorized person may submit a certificate or a revocation request, or the Authority itself issues a abrogated order. In any case, before the revocation, the qualified trust service provider will verify whether the request is filed by a person who has the legal right to do so;
e) The request for the revocation of the Qualified Certificate is processed immediately. The service provider provides the appropriate means of electronic communication and informs the holders (owners) of the certificates for this, including telephone number , fax or other means; f) The

Qualified Service Provider, provides the information service about the status of certificates (valid / revoked / repealed), all the time, 24 hours a day, 7 days a week, including holidays. This information should:

i) reflect the status of each certificate;

ii)reflect at least the date, time and code of the identification of the revoked / abolished certificates;

iii) be open and free of charge for the beneficiaries of the certificates or third parties.

## VI. SIGNATURES AND FOREIGN PRODUCTS

13. Recognition of foreign certificates

Electronic signatures and foreign products for electronic signatures are recognized and enforced in accordance with the agreements entered into by the Republic of Albania with foreign states for their acceptance and exchange of data when they have (fulfill) the minimum of technical reliability and security provided by Law no. 9880, dated 25.2.2008, "On Electronic Signature", Law no. 107/2015, "For electronic identification and trusted services", and the regulation.

14) Procedures for unification of foreign certificates and products.

a) Products and qualified certificates issued by a qualified service provider operating in a foreign country with which the Republic of Albania has signed an agreement are recognized only after this provider submits to the Authority all the required documentation for the recognition of the qualified certificate according to the law and the regulation; b) The documentation pertaining to a qualified foreign trusted provider must be confirmed by the home country Authority that fulfills all safety and assessment requirements as defined by law and the regulation. In any case, the qualified trust service provider is responsible for the safety of products and foreign certificates issued in our country, as well as for the consequences that may arise from non-fulfillment of obligations by this provider;

c) The Authority publishes in the updated register of certificates public codes for the verification of the certificates issued by foreign service providers recognized in the Republic of Albania.

ANNEX I

1. Security of operations

A qualified service provider should use systems and products that are protected against modification and guarantee the technical security and reliability of processes based on them. Especially:

a) An analysis of security requirements should be made during design and specification phase of each system development project by a qualified service provider to ensure security of IT systems.

b) Integrity of systems and information should be protected against viruses, malicious and unauthorized programs.

c) Media used within the systems must be handled securely to protect them from damage, theft, and unauthorized access.

d) Media management procedures should protect them against aging and deterioration of the media within the time period in which data is needed to be maintained.

e) Procedures should be defined and implemented for all trusted and administrative roles that affect the security of systems and services.

f) A qualified service provider must specify and implement such procedures to

ensure that security patches are applied within a reasonable time as they become available. A security patch should not be applied if it would present further weakness or instability that would avoid the benefits of their application. The reason for not applying security patches should be documented.

2. Incident Management

General

System activities related to access to IT systems, users of IT systems, and service requirements will be monitored. Especially:

a) Monitoring activities should consider the sensitivity of any information collected or analyzed.

b) Abnormal system activities indicating potential security breaches, including interference with the Qualified Service Provider's network, shall be detected and reported as an emergency.

c) The Qualified IT Service Provider's IT system will monitor the following events:
i. Switching on and off logging functions;

ii. Validity and Usability of Essential Services and Services in the Network and the System. d) A qualified service provider will act promptly and in a coordinated way to respond to incidents and limit the impact of the security breach. A qualified service provider will assign trusted staff to follow all alarms of potentially critical security events and to ensure that relevant incidents are reported in accordance with its internal procedures.

e) A qualified service provider shall establish a procedure to notify interested parties in accordance with the rules of any security breach or loss of integrity that has a significant impact on trusted services and personal data stored in.

f ) In cases where the security breach or loss of integrity effects naturaly or legally the person to whom the service is provided, the qualified trust service provider of the trusted service will also notify the natural or legal person of the security breach or loss of integrity without delay.

g) Audit Reports will be regularly analyzed and reviewed to identify evidence of malicious activity and notify the staff of potential critical security events.

h) Upon detection of a vulnerability that has not been addressed beforehand, the Qualified Trust Service Provider shall take appropriate measures to remedy it within a reasonable time. If this is not possible, the Qualified Trust Service Provider will establish and implement a plan to reduce critical vulnerability or document the factual basis for determining that vulnerabilitys correction is not required (needed).
i) Incident reporting and responsible procedures will be used to minimize security damage by incidents and malfunctions.

3. Control access

Access to the Qualified Service Provider's system will only be possible for authorized persons. Especially:

a) Controls will protect the internal network domains from unauthorized access including access by third party owners and third parties. Firewalls should be configured in ways to prevent all

protocols and accesses that are not needed for the functions of a trusted service.

b) A qualified service provider will administer the access of users, operators, administrators and system auditors. The administration will include user account management, auditing, modification time to time, and access abolishment.
c) Information access and enforcement action of the system functions shall be restricted in accordance with the access control policies. The systems will provide sufficient security controls, trusted roles identified in trusted service provider qualified practices, including security management sharing and enforcement functions. In particular, the use of support programs will be limited and controlled.

d) The Qualified Service Provider's staff will be identified and verified before using critique service-related functions. Personnel will be responsible for the performed activity.

e) Sensitive data will be protected against detection through reused ways of data storage.