

Approved Under Decree N 145/01 of
November 24 of 2010 of
Governor of National Bank of Georgia

Regulation on Usage of Electronic Document and Digital Signature in Payment and Securities System

Article 1. General Provisions

1. Purpose of this Regulation is to regulate electronic relation (relation arising from exchanging electronic document certificated by digital signature) between subjects of payment and securities system (GPSS) (hereinafter – system), to ensure terms of use and conditions of electronic signature in electronic document, fulfillment of which digital signature has the same legal force as of signature on material document.
2. Regulation of relation is carried out by this Regulation, rules of payment and securities system (hereinafter – system rules), contract concluded between participants, normative acts related to payment systems and present legislation.
3. This Regulation applies to subjects of system.
4. Rights of participants, not covered by this Regulation, are regulated by Georgian legislation.

Article 2. Definition of Terms

For the purpose of this Regulation terms used in this document have following meaning:

- a) payment and securities system (GPSS) – payment and settlement system of National Bank of Georgia, which includes Real Time Gross Settlement (RTGS) and Central Securities Depository (CSD) Systems;
- b) GPSS System rules (system rules) – RTGS and CSD system rules;
- c) electronic document (electronic message) - information created, transferred, received or stored through electronic, optical or other similar means, which confirms legally significant fact or fact, that has no legal significant;
- d) owner of electronic signature – a person, who has a certificate of electronic signature and pursuant to requirements of this Regulation and system rules signs electronic document electronically;
- e) digital signature – type of electronic signature, which is result of cryptographic transformation of electronic data, which logically connects with electronic document by

using private key of digital signature and satisfies following requirements: it is connected only with signatory, via it identification of signatory is possible, it is created by private key, which is under complete control of the signatory, it is connected with data in such way, that it gives possibility to detect whether or not there were changes in these data;

f) cryptographic transformation – encryption and decryption of electronic data by using logical and mathematical transformations;

g) key pair – public key, which locked and mathematically connected with asymmetric cryptosystem. Key pair is created by signatory or/and upon request of signatory issuer of certificate of digital signature;

h) private key – unique combination of electronic data, which is generated automatically, is known only by signatory and is used for creation of digital signature on electronic document;

i) public key - unique combination of electronic data, to which any person has an access and is used for verification of authenticity of digital signature on electronic document;

j) compromise private key of digital signature – any case or/and action, which has caused or may cause unauthorized use of private key;

k) issuer of certificate of digital signature – National Bank of Georgia;

l) certificate of digital signature – electronic document, issued by issuer of certificate and which contains public key of digital signature, allows to verify authenticity of digital signature and identify signatory;

m) means of digital signature – combination of electronic (software) means and cryptographic methods, which is used for created of key pair or/and digital signature and to verify authenticity of digital signature;

n) authenticity of electronic document – electronic document is authentic, if it successfully passed verification procedures in system and its digital signature is authentic;

o) verification of authenticity of digital signature on electronic document - precise determination of:

o.a) digital signature is created using private key relevant to the public key contained in signatory's certificate;

o.b) document has not changed since signing it with digital signature;

Article 3. Legal Force of Electronic Document

Electronic document has the same legal force as a material document, if its creation, transmission, processing and preservation is carried out pursuant to requirements prescribed by this Regulation, system rules, contracts concluded between system operator and system participant, normative acts related to payment systems.

Article 4. Certificate of Digital Signature

1. National Bank of Georgia (system operator) issues certificate of digital signature to system participants.
2. Certificate of digital signature shall contain:
 - a) unique registration number of certificate;
 - b) owner of digital signature;
 - c) data on used cryptographic algorithms and means of digital signature;
 - d) public key of digital signature;
 - e) expiration date of certificate;
 - f) date and time of issue of certificate;
 - g) issuer of certificate.
3. Certificate of digital signature is issued electronically, which is confirmed by digital signature of system operator.
4. Certificate of digital signature is registered in the registry, which is maintained by system operator.

Article 5. Obligations of the Owner of Digital Signature

1. Owner of digital signature shall:
 - a) keep secret private keys of digital signature;
 - b) not use private keys for digital signature, if it knows, that private keys have been compromised;
 - c) immediately demand suspension of certificate of digital signature's keys, in case of there is ground for compromising secrecy of private keys.
2. Owner of digital signature has no right to pass digital keys to the third person, information on processing technologies and other information on securities issues.
3. Owner of digital signature shall immediately notify in writing system operator on compromising private keys and shall terminate their usage.
4. Compensation of loss incurred by non-fulfillment of these requirements is imposed on owner of digital signature.
5. After receiving information on compromise of keys, system operator shall suspend further service of participant's relevant client until the situation won't improve.
6. Loss incurred as a result of processing of electronic document before notifying system operator on compromise of keys, shall bear system participant.

Article 6. Creation of Digital Signature

1. Keys of digital signature are created pursuant to rules and procedures established by system operator/system participant.
2. Loss incurred from keys created by system participant without compliance with the rules described in Paragraph 1st of this Article, shall be borne by the mentioned system participant.
3. Person, who has unlawfully obtained private key of other's digital signature and has used it, shall be held liable pursuant to Georgian legislation.

Article 7. Drawing Up Electronic Document on Paper

1. Electronic document or the result of the operation carried out by it can be printed out on the paper. Electronic document printed on paper shall be drawn up and certified by relevant responsible person.
2. Printed electronic document can serve as a ground for execution of operation only if, electronic document is authentic.

Article 8. Keeping Electronic Documents

1. Executed electronic document is kept pursuant to legislation.
2. It is necessary to secure system and information from unauthorized access.
3. While keeping electronic documents:
 - a) security from intentional or negligent distortion, falsification and unauthorized destruction shall be ensured;
 - b) invariability and availability, usage or creation of copies shall be ensured.