Regulations on Real –Time Gross Settlement System (RTGS)

Approved by the Order
of the President
of National Bank No. 135 of June 12, 2003

Article 1. General Provision

1. Purpose of this document is to regulate electronic communications (relations occurring in the process of exchanging documents certified with electronic-digital signatures) between the participants in real-time gross settlement system in the banking system of Georgia, securing terms and rules on applying electronic-digital signatures in the electronic document, in case of protection of which electronic-digital signature is deemed equal to personal signature affixed to the hard copy;

2. Relations are regulated based on this document as well as under agreements signed between the participants of the real-time gross settlement system (hereinafter system), and normative acts associated with payment systems and the current legislation;

3. Sphere of application of this regulation encompasses on the entities of settlement system participants who use electronic documents and electronic-digital signatures;

4. Protection of rights of consumers that are not regulated by this regulation is granted by Georgian legislation.
Article 2. Definition of Terms

System organizer – owner of electronic-technological system (National Bank of Georgia).

Participant (consumer) of the settlement system (RTGS) – any financial-crediting establishment which has correspondence, settlement and other accounts at bank institutions of Georgia (its branch), is the settlement subject in the territory of the country and meets the requirements of current electronic-technological system;

Real-time Gross Settlement System (RTGS) – entire arrangement of organizational forms of funds circulation, procedures, technological-functional and software-hardware means;

Electronic document – electronic version of the hard copy, is the basis of carrying out operations between subjects of payment relation, has the legal power equivalent of the hard copy of payment documents certified with the seal and signatures;

Electronic-digital signature – is the sequence of symbols developed by the computer technique as a result of processing the electronic document by cryptographic algorithm using special system (replicated by the organizer), which authenticates validity and integrity of electronic document and identity of the signatory;

Holder of the electronic-digital signature – an individual, who is registered by the system organizer according to the stated rule;

Open key of electronic signature – commonly acknowledged (known) sequence of symbols of electronic-digital signature to be checked;

Close key of electronic signature – sequence of symbols elaborating for electronic-digital signature is known only to the authorized person;
Unauthorized access – access to information or system functions by unauthorized persons;
Compromising the key – loss, theft, unsanctioned duplication of keys, also other circumstances when it is truly unknown as to what happened to the key;

Means of electronic-digital signature – software-hardware means, by which electronic-digital signature is affixed to the electronic document;

Authenticity of electronic document – electronic document is original if it successfully undergo through the checkup procedures existing in the system and the electronic-digital signature is authentic;

Authenticity of electronic-digital signature of the electronic document - electronic-digital signature of the electronic document is authentic if the system gives notification that the latter is authentic and the signatory of the electronic document used uncompromised key of signature.

Article 3. Terms of Acknowledging Equivalence of Personal Signature and Electronic-Digital Signature

1. Electronic document has the equal legal force of a hard copy if its compilation, transferring, processing and storing is consistent with the requirements of this regulations, agreement entered between system organizer and participant, normative documents related to payment systems;

2. Electronic-digital signature in the electronic document is deemed as identical to the personal signature affixed on the hard copy in case of simultaneous adherence to those conditions, when:
   a. electronic-digital signature and passport of ciphering keys are active as of the moment of signing (or checking) the electronic document;
   b. there are exist evidencing the moment of signature;
c. electronic signature is checked by open key (by a receiver) and the authenticity of electronic-digital signature is certified;
d. electronic-digital signature is used consistent with the data indicated in the passport of key signature.

**Article 4. Passports of Ciphering Key and Electronic-digital Signature**

1. System organizer gives passport of keys of electronic-digital signature and ciphering to the legal entities who are participants of the system;
2. Passport of electronic-digital signature and ciphering keys should include the following data:
   a. unique registration number of the passport;
   b. organization which holds passports, its address;
   c. name, surname, position, telephone, email of responsible person in the passport holder organization;
   d. passport validity period;
   e. data on passport conditions (valid, suspended, terminated);
   f. date, time of passport issuance;
   g. organization issuing the passport;
   h. person issuing passport, telephone, email;
   i. serial number of electronic-digital signature and ciphering keys;
   j. software module of designing electronic-digital signature means;
   k. personal signature of a person issuing a passport;

3. Issuance of electronic-digital signature passport and ciphering keys can be made in an electronic format certified by the electronic signature of the system organizer;

4. Passport of electronic-digital signature and ciphering keys is registered with the registry for passports which is maintained by the system organizer;
5. Term of storing of passport of electronic-digital signature and ciphering keys is 10 years from the moment of changing any requisites in the passport (both hard copy and soft copy);
6. After expiration of the term of storing passport of signature keys the entry of the registry is transferred to the archive storing regime.

**Article 5. Commitments of the Holder of the Passport of Signature Key**

1. Holder of signature key passport must:
   store electronic-digital signature keys confidentially;
   a. not use open and close keys for electronic-digital signing, provided that he/she is conversant that these keys are compromised;
   b. immediately require termination of the validity of the passport signature keys, in case of existence of violation on the confidentiality of electronic-digital signature close key;

2. Signature key passport holder is not authorized to give electronic-digital signature means, electronic-digital keys, information on electronic documents format, technology of information processing and other data on safety issues to the third person;

3. Passport holder is obliged to promptly inform system organizer in writing on loss of keys or their compromising and terminate their application;

4. Compensation of damage incurred as a result of negligence of these requirements (to be proved by the commission made up of the parties) is borne by the holder of signature key passport holder;

5. System organizer, after receiving information on compromising of the keys is obliged to suspend further service to the participant before rectification of the situation. As of this moment, operations of the participant will be held only on the basis of produced hard copy documents;
6. The damage caused by processing the electronic document prior to informing system organizer on compromising keys will be assigned to the system participant, however, regardless of informing the system organizer, damage incurred as a result of processing electronic document is borne by the system organizer;

7. System organizer is authorized to exercise control of safety measures in the process of activities organized by the participant.

**Article 6. Application of Electronic-Digital Signature Means**

1. Creation of electronic-digital signature keys is exercised solely by using cryptographic devise provided by the system organizer;

2. Compensation of damage incurred by keys created by software-hardware means of electronic-digital signature which were not provided by the system organizer, is borne by the consumer of these means;

3. Person, who illegally acquired closed key of other’s electronic-digital signature and made use of such electronic-digital signature, will bear responsibility consistent with the effective legislation;

**Article 7. General Principles of Exchanging Electronic Documents**

1. System organizer compiles electronic document adhering to defined safety procedure;

2. System participant, after compiling the electronic document, it should be certified and ciphered with his/her electronic-digital signature;

3. Electronic document is deemed as sent by the system organizer (or participant) from the moment the document exits its control area and relevant confirmation is
received. Exit of control area is construed as impossibility of return of the document, making amendments or cancellation without consent of the receiver;

4. Electronic document is considered as received by the system organizer (or participant) from the moment the latter is given access to the document;

5. Confirmation on receive-sending of the document is sent immediately (by the system through software-hardware means);

6. Confirmation of the receipt of electronic document implies that the fact of authenticity of the document is identified;

7. By the time of sending (or receiving) electronic documents, both sender and receiver should keep confirmation of sending (or receiving) the electronic document which may exist in a hard or electronic copy;

8. Charge off of the amount from the corresponding account in the system and its reflection on the relevant corresponding account occurs in one and the same moment (of real time), thus, transfer acquires the status of completed as of the same moment (bank of a payer loses and a bank of a receiver receives the right of ownership of financial sources).

**Article 8. Registration Electronic Documents in a Hard Copy**

1. Electronic document or the result of operation exercised with its application may be presented in a form of printed paper. Printed hard copy of the electronic document should be processed and certified by the appropriate responsible person;

2. Printed hard copy of the electronic document is the ground for operation implementation solely in terms of authenticity of electronic document;
Article 9. Electronic Document Storing

1. Storing of completed electronic documents is exercised consistent with the terms provided in the agreement entered between the system organizer and a participant and respective normative documents;

2. It is necessary to protect the system and information from unsanctioned access;

3. While storing electronic documents, it is necessary to ensure their:
   a. protection from damage caused intentionally or for the reason of negligence, from counterfeiting and unsanctioned devastation;
   b. invariability and availability, application and duplication;

4. Electronic documents are stored on electronic (optical) information storage medium;

5. Print of electronic documents to the paper for storing purposes is not required.

Article 10. Receiving, Modification and Storing of Keys by the System Participant

1. System participant is obliged to appoint a person authorized to make electronic-digital signature – administrator. System organizer must be immediately informed on change of administrator;

2. Administrator is obliged to personally visit system organizer – system security administrator, undergo relevant instructions, independently generate electronic key set (open and close);

3. set of keys will be transferred to the system security administrator in a ciphered form;
4. System security administrator draws up and transfers passports of electronic-digital signature keys;

5. System administrator gives to and receives from administrator of the participant open keys set;

6. After checkup, administrators bilaterally sign two copies of signature key passports, each is stored for ten years with each party;

7. In case of change of keys, party initiating change of the key is obliged to notify the other party in a timely manner on necessity of undergoing this procedure;

8. Under the initiative of one of the parties, key must be changed when the effective term of key set expires, keys are compromised or the administrator of the participant has changed;

9. Effective term of keys is identified upon consent of the parties. In case the term expires, change of keys is a must. Under the initiative of one of the parties, keys may be changed prior to expiration of their effective term any time;

10. After changing of the keys, participant must store the set of invalidated keys together with electronic documents with relevant ciphering-deciphering program application versions for not less than 10 years;

11. Participant is obliged to ensure independently storage of keys and their protection from promulgation and disclosure;
Article 11. Submitting a Claim and Dispute Discussion in the Course of Operations

1. In case of dispute arises in the period of electronic service provided by system organizer to the settlement participant, interested party sends relevantly draw up claim to the other party;

2. Claim is deemed as duly processed if it reflects the name of the claimant organization, detailed description of the claim, signature of the authorized person, date, hard copy of the disputed electronic document;

3. In case it appears that the claim is not duly processed under the relevant rule, the party against which the claim was made must notify disclosed inaccuracy to the claimant;

4. For resolution of the disputes, parties are entitled to create an ad hoc expert commission (hereafter commission) for consideration of a claim which will be one time type created only for particular case;

5. Commission should ensure achievement of possible consensus between the parties, unless the parties apply the decision through a rule of law (private arbitration, court);

6. Composition of the commission will be agreed by the parties and will be approved by bilateral acts;

7. Commission will be composed of party representatives with equal number, in case of necessity – independent experts will also be included. Commission also should be composed with the specialist(s) from the information security department of National Bank of Georgia;

8. Party representatives may also be appointed persons other than their employees, whose authority is confirmed by relevant proxy;
9. In such case, commission in no later than three weeks:
   a. should ensure assignment of functions between the members and define timelines for their implementation;
   b. ensure overcoming divergences;
   c. disclose the guilty party;
   d. identify the issues of material compensation by parties;
   e. draw up an expert conclusion of rendered activities;

10. Commission should make decision by two third of votes of the members;

11. If any of the parties disagrees or does not enforce an expert conclusion of the commission, or if the agreement was not reached between commission members, parties should apply to court.

**Article 12. Checking Authenticity of Disputed Electronic Document, Electronic-Digital Signature Keys or Electronic Signature**

1. Authenticity of current (stored at archived) disputed electronic document, electronic-digital signature key or electronic signature must be checked in the building of the system organizer, using its software-hardware means;

2. Procedure of checking free (clear) technical means is held after relevant system and software applications are installed and their readiness for operations is identified;

3. For dispute resolution purposes the commission should request from the responsible person of the disputed electronic document holder party the electronic document subject to dispute and sample of control key set to (electronic or optical information storage medium) which was used for signing;

4. In case of necessity commission may require both from claimant and defender to submit additional documents evidencing exchange of disputed electronic document (notifications, confirmations, communication protocols etc.)
5. Disputed electronic document must be submitted in a form of file and in a format used in the system;

6. In case any of the parties refuses to produce mentioned materials, his/her claim will be deemed as groundless and the dispute will be resolved in favor of the other party;

7. Commission, first of all, defines the identity of the keys submitted by the parties (by means of signature key passports). In case of their inconsistency, the responsibility is borne by the party where the inconsistency was detected;

8. In case the dispute is not resolved by means of the initial checking of keys, the authenticity of the electronic-digital signature of disputed electronic document will be checked by means of disputed electronic document and key set;

9. Signature of disputed electronic document should be checked by means of protection used in the system;

10. If the result of checking is negative, signature of electronic document should not be deemed as authentic;

11. If the document is created by the system participant, the receipt of which is not denied by the system organizer and the result of checking confirms authenticity of electronic-digital signature, the responsibility on authenticity of electronic document is borne by the system participant;

12. If the document was created by the system organizer, receipt of which is not denied by the system participant and the result of checking confirms authenticity of electronic-digital signature, responsibility for authenticity of the electronic document is borne by the system organizer;
13. In case the participant refuses electronic document, i.e. the participant argues that electronic document received by the system organizer was not sent by him/her, and the system organizer argues otherwise, commission shall:

a. check transmission of this electronic document in the system. If the electronic document was not transmitted through the system, dispute consideration will be terminated due to absence of grounds;

b. receive disputed electronic document from the system organizer (his responsible person) on the basis of which the document was processed. On behalf of the system organizer, refusal to produce disputed electronic document the dispute will be resolved in favor of the participant;

c. check the authenticity of the signature of the user on the electronic document produced by the system organizer. If the signature is not authentic, dispute will be resolved in favor of the participant;

14. In case the system organizer (or participant) refuses to receive electronic document, i.e. the participant (or organizer) argues that the electronic document sent by him is received by the system organizer (or participant), and the system organizer (or participant) refuses to receive, the commission shall:

a. require disputed electronic document from the participant (or organizer) and the confirmation of the system organizer (or participant) on its receipt. In case system participant (organizer) refuses to produce disputed electronic document, or relevant confirmation, the dispute will be resolved in favor of the system organizer (participant);

b. compare electronic document and relevant confirmation (among them of unique numbers – which should coincide). If confirmation data does not correspond to the data of disputed electronic document, dispute will be resolved in favor of system organizer (participant);

c. check the authenticity of signature of the system organizer (participant) of the confirmation. If the signature is not authentic, dispute will be resolved in favor of system organizer (participant);
15. For resolution of the dispute arising in case of discrepancy between the electronic document sent by the participant and the document received by the system organizer, i.e. when the participant argues that the electronic document sent by him does not correspond with the document processed by the system organizer and the system organizer does not acknowledge this, the commission shall:

a. request from the system organizer (or his responsible person) an electronic document, which was received for processing. In case the system organizer refuses to produce disputed electronic document, dispute will be resolved in favor of the participant;

b. compare contents of the electronic document received by the system organizer with the document transferred by the user. In case of identity, dispute will be resolved in favor of the participant, in the adverse case dispute will be resolved in favor of the organizer;

c. check the authenticity of signature of the participant on the electronic document received by the system organizer. If the signature is not authentic, dispute will be resolved in favor of the participant.