Federal Law of 10.01.2002 № 1-FZ

On electronic digital signature

pravo.gov.ru

Abolished - Federal Law
from 06.04.2011, N 63-FZ

RUSSIAN FEDERATION

THE FEDERAL LAW

On electronic digital signature

Adopted by the State Duma on December 13, 2001
Approved by the Federation Council 26 December 2001

(As amended by Federal Law of 08.11.2007 N 258-FZ)

CHAPTER I. GENERAL PROVISIONS

Article 1. Purpose and scope of the present Federal law

1. The purpose of this Federal Law is to ensure legal conditions for the use of electronic digital signature electronic documents, under which the electronic digital signature in the electronic document is recognized equivalent handwritten signature on a paper document.

2. This Federal Law shall apply to relations arising from the commission of civil transactions and in other legislation of the Russian Federation cases.

This Federal Law does not apply to relations arising from the use of other analogues handwritten signature.

Article 2. Legal regulation of relations in the field of use of digital signature

Legal regulation of relations in the field of

digital signature is carried out in accordance with
the present Federal Law, the Civil Code of the Russian
Federation, the Federal law "On information, informatization and
Data Protection ", Federal Law" On Communications ", in other
federal laws and in accordance with these other
normative legal acts of the Russian Federation, as well as
It carried out the parties' agreement.

Article 3. The basic concepts used in the present
Federal law

For the purposes of this Federal Law
The following basic concepts:
electronic document - the document in which information
represented in digital form;
electronic digital signature - electronic props
document, intended for protection of the electronic
the document from forgery, the resulting cryptographic
converting the information using a private key
digital signature and allowing to identify
the signature key certificate holder, as well as to establish the absence of
distortion of information in the electronic document;
the owner of the signature key certificate - an individual, in the name of
which certification authority issued the certificate of the signature key and
which owns the corresponding private key e

digital signature, allowing by means of electronic
digital signature to create a digital signature in
electronic documents (to sign electronic documents);

means of electronic digital signature - hardware and (or)
software means for implementing at least one of
the following functions - creation of an electronic digital signature
an electronic document using a private electronic key
digital signature verification using the public key
electronic digital signature authenticity of the electronic digital
signatures in the electronic document, creating closed and open
electronic digital signature keys;

certificate of digital signature - a document on
paper, issued in accordance with the rules of the system
certification to confirm compliance of electronic
digital signature requirements;

the private key of electronic digital signature - a unique
sequence of characters known to the owner of the certificate key
signatures and for creating electronic documents
electronic digital signature by means of electronic
digital signature;

public key digital signature - a unique
a sequence of characters corresponding to the private key
electronic digital signature available to any user
information system and is designed to accept a
the use of electronic digital signatures

electronic digital signature in the electronic document;

signature key certificate - a document on paper or
electronic document with a digital signature
authorized person certifying center, which include
public key digital signature and which are issued
party certification center information system
authentication and digital signature
identification of the signature key certificate holder;

authentication of electronic digital signature
electronic document - a positive test result
appropriately certified means of electronic digital
signature using a signature key certificate Accessories
electronic digital signature in an electronic document owner
the signature key certificate and the absence of distortions in the signed
This digital signature electronic document;

the user signature key certificate - a natural person,
using information obtained in the certification center
signature key certificate to verify the electronic accessories
digital signature owner signature key certificate;

public information systems - information
a system that is open for use by all individuals and
legal entities and the services which these persons can not be
denied;

corporate information system - information system
which the participants may be limited circle of persons defined

its owner or agreement of the participants of this information system.

CHAPTER II. TERMS OF USE OF ELECTRONIC SIGNATURE

Article 4. Conditions of recognition of equivalence of electronic digital signature and a handwritten signature

1. The digital signature in an electronic document equivalent to a handwritten signature in the document on paper media, while respecting the following conditions:

signature key certificate belonging to this email digital signature, has not lost the power (force) at the time of verification or at the time of signing an electronic document if evidence, determining the time of signing;

confirmed the authenticity of the electronic digital signature electronic document;

digital signature is used in accordance with information specified in the certificate of the signature key.

2. Member of an information system can be simultaneously the owner of any number of signature key certificates. Wherein electronic document with a digital signature is legal significance in the implementation of the relations specified in signature key certificate.

Article 5. Use of digital signatures

1. Creation of electronic digital signature keys
implemented for use in:
information system, its public member or by
his treatment Certification Authority;
corporate information system in the manner prescribed
in this system.
2. When you create the keys of electronic digital signatures for
use in the public information system must
apply only certified means of electronic digital
signatures. Compensation for damages caused in connection with the creation of keys
electronic signatures uncertified means
digital signature can be the responsibility of the creators and
distributors of these funds in accordance with the law
Russian Federation.
3. The use of uncertified means of electronic
Digital signatures and keys they create electronic digital
signature in corporate information systems of the federal
public authorities, public authorities
The Russian Federation and local self-government
It allowed.
4. Certification of digital signatures
carried out in accordance with the legislation of the Russian
Federation on certification of products and services.

Article 6. Signature Key Certificate

1. The signature key certificate shall contain the following intelligence:

a unique signature key certificate registration number, date of commencement and expiry of the certificate of the signature key, located in the registry certification center;

surname, name and patronymic of the signature key certificate owner or a nickname of the owner. In the case of using a pseudonym certification authority an entry to this key certificate signature;

public key digital signature;

Name of electronic digital signature, which using the public key of the electronic digital signature;

name and address of the certification center, issued the certificate signature key;

information about relationships, which in the implementation of the electronic a document with a digital signature will be legal value.

2. If necessary, the certificate signature key on based on the supporting documents indicated position (with specifying the name and location of the organization in which established the post) and the qualification certificate holder key signature, and at his request in writing - other

information confirmed by relevant documents.

3. The signature key certificate shall be submitted certifying center signature key certificates registry not later than the date Commencement of the signature key certificate.

4. To check the accessories of digital signature respective owner signature key certificate is issued users with the date and time of issue, the information the signature key certificate (valid action suspended terms of its suspension, revoked, date and time of revocation of the certificate signature key) and information on register of signature key certificates. In the case of issuance of the certificate key signature in the form of a document on paper that Certificate issued on the letterhead and certification center certified by the personal signature of the authorized person and seal certifying center. In the case of issuance of the certificate of the signature key and said additional data in the form of electronic document the certificate must be signed by electronic signature authorized person certifying center.

Article 7. Term, and how key certificate signature certification center

1. The term of the certificate signature key storage in the form of electronic document certifying center determined the contract between the Certification Authority and the certificate holder

signature key. This provides access members
information system for certifying center
the signature key certificate.

2. The shelf life of the signature key certificate in the form of
electronic document certification center after revocation
the signature key certificate must be at least set
the federal law of the limitation period for the relations of these
in the signature key certificate.

After this storage period key certificate
the signature is removed from the registry key certificates and signatures
translated in archival mode. Term Archiving
is not less than five years. The procedure for issuing certificates of copies
signature key during this period is set in accordance with
Russian legislation.

3. The signature key certificate in the form of a document on paper
Keep media in the manner prescribed by law
Russian Federation on archives and archiving.

CHAPTER III. Certifying Center

Article 8. The status of the certification center

1. Certification Authority issuing key certificates
signatures for use in general information systems
Spaces must be a legal entity, performing functions

contemplated hereby. Wherein
certification authority must have the necessary material and
financial capacity to enable it to carry civil
responsibility to the signature key certificates users
for any losses that may be incurred by them as a result of
the unreliability of the information contained in the certificates of keys
signatures.

Requirements for material and financial
the possibilities of certification authorities, determined by the Government
The Russian Federation on the recommendation of the authorized federal
executive authority.

Status Certification Authority providing
the functioning of the corporate information system is determined
its owner or agreement of the participants of the system.

2. (repealed - Federal Law of 08.11.2007 N 258-FZ)

Article 9. Activities of the certification center

1. Certification Authority:

produces the signature key certificate;

creates keys of electronic digital signatures for handling
Participants information system with a guarantee of secrecy
the private key of electronic digital signature;

It suspends and resumes action key certificates
signatures and cancels them;

conducts signature key certificates registry, it provides the urgency and the possibility of free access to it members information systems;

checks the uniqueness of public keys of electronic digital signatures in the register of signature key certificates and archive Certification Authority;

It provides the signature key certificate in the form of documents paper and (or) in the form of electronic documents with information about their effects;

carries on the appeals key certificates of users Signature authentication of electronic digital signature electronic document in respect of the certificates issued to them keys signatures;

can provide participants with information systems of other associated with the use of digital signatures services.

2. Production of signature key certificates is carried out on based on the application of information system participant that It contains the information specified in Article 6 of the present Federal law and necessary to identify key certificate owner signatures and send messages to it. The application is signed the owner of his own signature key certificate. contained in a statement confirmed by the presentation of relevant information documents.

3. In the manufacture of signature key certificates Certification Authority issued in the form of documents on paper

media, two copies of the signature key certificate, which
handwritten signatures certified key certificate owner
signature of the authorized person and certification center, as well as
stamp certifying center. A copy of the public key certificate
signatures issued to the owner of the signature key certificate and the second -
It remains in the certification center.

4. Services in distribution of participants in information systems
signature key certificates registered certifying
center, together with information about their effects in the form of
Electronic documents are free of charge.

Article 10. Relationship between the Certification Authority and authorized federal executive power

1. Certification Authority prior to the use of electronic
signature of the authorized person certifying center for
assurances on behalf of the Certification Authority key certificates
signatures required to submit to the authorized federal body
executive certificate key signature of a person authorized
Certification Authority in the form of an electronic document, as well as the
in the form of a certificate paper document with
the handwritten signature of the authorized person said,
certified by signature and seal of the certifying center.

2. The authorized federal executive body

is the single state register of signature key certificates,
which is certified centers working with the participants
public information systems, assure issued by them
signature key certificates, allows free
Access to this registry and issues certificates of signature key
the relevant authorized persons certifying centers.

3. The electronic digital signatures of authorized persons
certification authorities can be used only after the
them in a single state register of signature key certificates.
Using these digital signatures for purposes not
related to the certification of signature key certificates and information about
their action is not allowed.

4. The authorized federal body of executive power:

It carries on the appeals of individuals, organizations,
federal government agencies, state
the authorities of the Russian Federation and local
self-authentication of digital
signatures of authorized persons certifying centers issued by them
the signature key certificate;

It takes place in accordance with the regulations of the authorized
federal executive body for the other powers
provision of this Federal Law.

Article 11. Obligations of the certification center for
with respect to the owner of the signature key certificate

Certification Authority certificate with key manufacturing signature assumes the following obligations in relation to the owner of the signature key certificate:

make the certificate signature key in the registry key certificates signatures;

to ensure the issuance of signature key certificate who applies to it participants of informational systems;

pause key certificate valid signature on treatment of its owner;

notify the facts of the signature key certificate owner, which came to be known, and that certification center can significantly affect the possibility of further the use of the signature key certificate;

other established regulations or agreement of the parties obligations.

Article 12. Obligations of the signature key certificate owner

1. The owner of the signature key certificate shall:

do not use open and for digital signature private keys of digital signature, if he knows that These keys are used or have been used previously;

keep secret private key of electronic digital signature;

require immediate suspension of the certificate

key signature if there are grounds to believe that the mystery of the closed key digital signature is broken.

2. Failure to comply with the requirements set out in this Article, compensation for damages caused as a result of this the responsibility of the

See the next page of the document