ST RK 1073-2007

Means of cryptographic information protection

General technical requirements

Committee for Technical Regulation and Metrology of the Ministry of Industry and Trade Republic of Kazakhstan
(Gosstandart)

Content

1 area of use
2 Normative references
3 Terms and definitions
4 General provisions
5 General technical requirements
5.1 General requirements for CIPF
5.2 Requirements for technical documentation of CIPF
5.3 Requirements for CIPF of the first security level
5.4 Requirements for CIPF of the second security level
5.5 Requirements for CIPF of the third security level
5.6 Requirements for CIPF of the fourth security level

1 area of use

This standard applies to cryptographic information protection tools of domestic and foreign production and establishes general technical requirements for them.

The standard is suitable for conformity assessment purposes.

This standard does not apply to cryptographic information protection tools, which are state encryption tools of the Republic of Kazakhstan.

2 Normative references

This standard uses references to the following standards:

GOST 28147-89Information processing system. Cryptographic protection. Cryptographic transformation algorithm.

GOST 34.310-2004Information technology. Cryptographic protection of information. Processes of formation and verification of electronic digital signature.

3 Terms and definitions

For the purposes of this International Standard, the following terms and definitions apply:

3.1 Cryptographic transformation algorithm: A set of a finite number of simple and uniquely defined rules that depend on the variable parameter (key) and specify the sequence of operations for solving the cryptographic transformation problem.

3.2 asymmetric cryptographic transformation algorithm: A cryptographic transformation algorithm in which forward and backward transformations use a public and a secret key that are related in such a way that it is computationally difficult to determine the secret key from the public key.

3.3 Authentication: Establishing the identity of one or more aspects of the communication: the session, its time, the communicating parties, the messages being sent, the origin of the data, the time the data was created, the content of the data.

3.4 State cryptographic means: means of cryptographic protection of information, intended as the main protection measure for maintaining the confidentiality of information constituting the state secrets of the Republic of Kazakhstan.

3.5 spoofing: A fixed-length string of bits, obtained according to a certain rule from the data and a key, added to the data to provide spoofing protection.

3.6 Imitation protection: Protection of a communication system from the imposition of false messages.

3.7 Key: A specific secret or public (if specifically indicated) state of some parameters of the cryptographic data transformation algorithm, which ensures the choice of one transformation from the set of transformations possible for this algorithm.

3.8 Cryptographic strength of the means of cryptographic protection of information: the computational complexity of the method (algorithm) for breaking cryptographic protection, which is the best for this means of cryptographic protection of information.

3.9 Cryptographic transformation: Transformation of data by means of encryption, generation (verification) of imitation insertion or formation (verification) of an electronic digital signature.

3.10 Pre-encryption: Encryption that is technically implemented separately from the transmission of encrypted data over communication channels.

3.11 symmetric cryptographic transformation algorithm: A cryptographic transformation algorithm in which the forward and reverse transformations use the same key or two keys, each of which is easily computed from the other.

3.12 Means of cryptographic information protection; CIPF: A tool that implements algorithms for cryptographic transformations, generation, formation, distribution or management of keys.

3.13 Electronic digital signature scheme: A cryptographic transformation algorithm that generates an electronic digital signature, and a corresponding cryptographic transformation algorithm that checks it.

4 General provisions

4.1 CIPF are intended for:

a) maintaining the confidentiality of data using a cipher;

b) authentication, including data integrity control, using an imitation insert and (or) digital signature;

c) generation, formation, distribution and (or) key management.

4.2 CIPF that meets the requirements of this standard are considered as technologically completed (operable) hardware, software or firmware.

4.3 Depending on the cryptographic strength for CIPF, 4 security levels are set:

4.3.1 CIPF of the first security level is designed to protect information, the damage from disclosure, imposition, or unauthorized change of which in the amount protected using the same key (same keys) does not exceed 100 minimum calculated indicators;

4.3.2 CIPF of the second security level is designed to protect information, the damage from changing which in the amount protected using the same key (same keys) does not exceed 10,000 minimum calculated indicators;

4.3.3 CIPF of the third security level is designed to protect information, the damage from changing which in the amount protected using the same key (same keys) does not exceed 1,000,000 minimum calculated indicators;

4.3.4 CIPF of the fourth security level is designed to protect information, the damage from changing which in the amount protected using the same key (same keys) does not exceed 100,000,000 minimum calculated indicators.

4.4 CIPF cannot be recognized as corresponding to the first, second, third or fourth security level if the computational complexity of the existing algorithms for opening the cryptographic protection provided by them is less than 250, 280, 2120 or 2160, respectively.

5 General technical requirements

Means of cryptographic protection of information must comply with the requirements of this standard and technical documentation approved in the prescribed manner.

5.1 General requirements for CIPF

5.1.1 The keys generated by the CIPF (except for public keys) must be sequences of random numbers generated using physical noise generators (for example, thermal, diode, radiation, impulse), or sequences of pseudo-random numbers generated using random events (for example, system computer parameters, mouse movements, keyboard clicks, timer status).

5.1.2 CIPF that uses the distribution of keys over insecure communication channels must provide cryptographic protection of keys in order to prevent the disclosure and unauthorized change of these keys (except for the disclosure of public keys), as well as the imposition of false keys.

5.1.3 Any key used by the CIPF should be used by only one cryptographic transformation algorithm, for example, only for encryption or only for the formation of an electronic digital signature.

5.1.4 Protection against unauthorized modification of the CIPF, including modification or substitution of their elements and modules, should be provided in order to exclude the impact on the cryptographic strength of the CIPF.

5.2 Requirements for technical documentation of CIPF

5.2.1 Technical documentation (design, technological and software documentation, depending on the type of CIPF) must contain a complete description of the cryptographic transformation algorithms implemented in the CIPF, generation, formation, distribution and management of keys.

5.2.2 If the CIPF implements cryptographic transformation algorithms defined by state and interstate standards or other regulatory documents on standardization that are in force or applied in the Republic of Kazakhstan in the prescribed manner, then in the technical documentation, instead of their full description, it is allowed to make references to these documents.

5.2.3 CIPF must implement cryptographic transformation algorithms in strict accordance with their description given in the technical documentation.

5.2.4 Each set of cryptographic information protection tools should include operational documentation that fully and adequately describes all possible modes of their use and contains a list of all organizational and technical measures necessary to ensure the security of the processed information, including the procedure and frequency of changing keys, the procedure for maintaining cryptographic information protection and actions to be taken to eliminate operator errors and other abnormal situations that may occur during operation, as well as their consequences.

5.3 Requirements for CIPF of the first security level

5.3.1 The key length of the symmetric cryptographic transformation algorithms implemented by the CIPF must be at least 60 bits.

5.3.2 The key length of asymmetric cryptographic transformation algorithms implemented by the CIPF must be at least 120 bits.

5.3.3 The key length of asymmetric cryptographic transformation algorithms implemented by the CIPF, the cryptographic strength of which is based on the computational complexity of the problem of factoring a composite number into factors or the problem of discrete logarithm in a finite field, must be at least 500 bits.

5.3.4 The length of the calculated CIPF hash code must be at least 120 bits.

5.3.5 The length of the generated CIPF EDS must be at least 120 bits.

5.3.6 The principle of generation and formation of keys implemented by the CIPF should ensure that each bit of the key takes a single value with a probability from the interval (0.50 ± 0.03).

5.4 Requirements for CIPF of the second security level

5.4.1 The key length of the symmetric cryptographic transformation algorithms implemented by the CIPF must be at least 100 bits.

5.4.2 The key length of asymmetric cryptographic transformation algorithms implemented by the CIPF must be at least 160 bits.

5.4.3 The key length of asymmetric cryptographic transformation algorithms implemented by the CIPF, the cryptographic strength of which is based on the computational complexity of the problem of factoring a composite number into factors or the problem of discrete logarithm in a finite field, must be at least 1500 bits.

5.4.4 The length of the calculated CIPF hash code must be at least 160 bits.

5.4.5 The length of the generated CIPF EDS must be at least 200 bits.

5.4.6 The principle of generation and formation of keys implemented by the CIPF should ensure that each bit of the key takes a single value with a probability from the interval (0.50 ± 0.01).

5.4.7 CIPF should implement procedures for calculating and verifying control information about keys in order to prevent the use of keys accidentally distorted at the stage of distribution and loading with a probability of at least 0.9999.

5.4.8 During preliminary encryption, CIPF should implement procedures for calculating and verifying control information about encrypted data in order to detect randomly distorted encrypted data with a probability of at least 0.9999.

5.4.9 CIPF should inform the operator about the establishment, reset, and also about the impossibility of establishing the encryption mode.

5.5 Requirements for CIPF of the third security level

5.5.1 The key length of the symmetric cryptographic transformation algorithms implemented by the CIPF must be at least 150 bits.

5.5.2 The key length of asymmetric cryptographic transformation algorithms implemented by the CIPF must be at least 250 bits.

5.5.3 The key length of the asymmetric cryptographic transformation algorithms implemented by the CIPF, the cryptographic strength of which is based on the computational complexity of the problem of factoring a composite number into factors or the problem of discrete logarithm in a finite field, must be at least 4000 bits.

5.5.4 The length of the calculated CIPF hash code must be at least 250 bits.

5.5.5 The length of the generated CIPF EDS must be at least 300 bits.

5.5.6 The principle of generation and generation of keys implemented by the CIPF should ensure that each bit of the key takes a single value with a probability from the interval (0.500 ± 0.003), while the keys should be sequences of random numbers and be formed using physical noise generators.

5.5.7 CIPF should implement procedures for generating and verifying imitation inserts or EDS for keys in order to prevent the use of keys accidentally or deliberately distorted at the stage of distribution and loading with a probability of at least 0.999999.

5.5.8 During preliminary encryption, CIPF should implement procedures for generating and verifying imitation inserts or EDS for encrypted data in order to detect accidentally or deliberately distorted encrypted data with a probability of at least 0.999999.

5.5.9 CIPF should inform the operator about the establishment, reset, as well as the impossibility of establishing the encryption mode and other abnormal situations.

5.5.10 CIPF should provide hierarchical cryptographic protection of keys at the stage of their distribution and management in order to prevent the disclosure and unauthorized change of these keys (except for the disclosure of public keys), as well as the imposition of false keys, or the operational documentation of the CIPF should contain organizational and technical measures to ensure protection against these threats.

5.5.11 Regular procedures for deleting (destroying) keys implemented by the CIPF should guarantee the impossibility of their recovery.

5.6 Requirements for CIPF of the fourth security level

5.6.1 The key length of the symmetric cryptographic transformation algorithms implemented by the CIPF must be at least 200 bits.

5.6.2 The key length of asymmetric cryptographic transformation algorithms implemented by the CIPF must be at least 400 bits.

5.6.3 The key length of asymmetric cryptographic transformation algorithms implemented by the CIPF, the cryptographic strength of which is based on the computational complexity of the problem of factoring a composite number or the problem of discrete logarithm in a finite field, must be at least 8000 bits.

5.6.4 The length of the calculated CIPF hash code must be at least 400 bits.

5.6.5 The length of the generated CIPF EDS must be at least 400 bits.

5.6.6 The principle of generation and formation of keys implemented by the CIPF should ensure that each bit of the key takes a single value with a probability from the interval (0.500 ± 0.001), while the keys should be sequences of random numbers and be formed using physical noise generators.

5.6.7 CIPF should implement procedures for generating and verifying imitation inserts or EDS for keys in order to prevent the use of keys accidentally or deliberately distorted at the stage of distribution and loading, with a probability of at least 0.999999999.

5.6.8 CIPF should implement procedures for generating and verifying imitation inserts or EDS for encrypted data in order to detect accidentally or deliberately distorted encrypted data with a probability of at least 0.999999999.

5.6.9 CIPF should inform the operator about the establishment, reset, as well as the impossibility of establishing the encryption mode and other emergency situations, prevent the transit of open data through itself into the area of storage, distribution and subsequent processing of encrypted data.

5.6.10 CIPF should provide hierarchical cryptographic protection of keys at the stage of their distribution and management in order to prevent the disclosure and unauthorized change of these keys (except for the disclosure of public keys), as well as the imposition of false keys.

5.6.11 The standard procedures for deleting (destroying) keys implemented by the CIPF should guarantee the impossibility of their recovery. If the CIPF does not implement the specified procedures, then these procedures for guaranteed deletion (destruction) of keys (except for public keys) must be implemented by the technical means supplied with the CIPF.

KeywordsKeywords: information security, cryptography, encryption, authentication, electronic digital signature, hash code, security level, compliance confirmation