GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80
File No.: 44629-2014

GM/T 0028-2014

Security requirements for cryptographic modules

密码模块安全技术要求

Issued on: February 13, 2014 **Implemented on: February 13, 2014**

Issued by: State Cryptography Administration

Table of Contents

Foreword

This Standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This Standard uses Redraft Law to modify ISO 19790:2012 Information technology - Security techniques - Security requirements for cryptographic modules.

The technical differences between this Standard and ISO 19790: 2012 and the reasons are as follows:

- With regard to Appendix C - E, this Standard makes adjustments with technical differences, to suit our country's technical conditions; specifically adjusts the documents listed in Appendix C - E; replaces the list of standards listed in ISO 19790:2012 with the list of standards approved by the State Cryptography Administration.

Attention is drawn to the possibility that some of the elements of this Standard may be the subject of patent rights. The issuing authority of this document shall not be held responsible for identifying any or all such patent rights.

This Standard was proposed by and shall be under the jurisdiction of Standardization Technical Committee of Cryptography Industry.

Main drafting organizations of this Standard: DCS Center, Beijing Watchdata Technologies Co., Ltd., Beijing Certificate Authority, Zanjia Electronic Technology (Beijing) Co., Ltd., Feitian Technologies Co., Ltd., Beijing Haitai Fangyuan Technologies Co., Ltd., Beijing HuaDa ZhiBao Electronic System Co., Ltd., Commercial Cryptography Testing Center of State Cryptography Administration, Shanghai KOAL Software Co., Ltd., Beijing Creative Century Technologies Co., Ltd.

Main drafters of this Standard: Gao Neng, Jing Jiwu, Wang Juan, Tu Chenyang, Wang Xuelin, Chen Guo, Zhan Banghua, Zhang Jiachun, Zhu Pengfei, Jiang Hongning, Chen Yue, Luo Peng, Tan Wuzheng, Zhang Wantao, Liu Limin, Wang Yuewu, Xiang Ji, Wang Qiongxiao, Lin Zhangqiang, Xia Luning.

Security requirements for cryptographic modules

1 Scope

This Standard, for the cryptographic modules which are used to protect the security system of sensitive information in computer and telecommunications systems, specifies security requirements. The Standard defines 4 security levels for cryptographic modules, to meet the security requirements of different degrees of sensitive information and many application fields. For the 11 security domains of cryptographic modules, this Standard gives the corresponding requirements of the four security levels. The high security level, on the basis of the low security level, further improves security.

2 Normative references

The following documents are essential to the application of this document. For the dated references, only the versions with the dates indicated are applicable to this document. For the undated references, the latest version (including all the amendments) are applicable to this document.

The documents listed in Appendix C, D, and E of this Standard.

3 Terms and definitions

The following terms and definitions are applicable to this document.

3.1 Access control list

A list of permissions which allows access to an object.

3.2 Administrator guidance

Written data used by cryptographic officer and/or other management roles to correctly configure, maintain, and manage cryptographic modules.

3.3 Approval authority

An authority which is authorized to approve and/or evaluate security functions. The function of approval authority is to evaluate and approve security functions, not to test the compliance of cryptographic modules with this Standard.

3.4 Approved data authentication technique

Approved data authentication technique based on digital signature, message authentication code, or hash with cryptographic keys (such as HMAC), and other methods.

3.5 Approved integrity technique

Approved integrity technique based on hash, massage authentication code, or digital signature algorithm.

3.6 Approved mode of operation

A mode of operation of cryptographic modules. Under this mode, only approved security functions can be used. It shall not be confused with the mode of operation of cryptographic algorithm, such as AES CCM mode.

3.7 Approved security function

Security functions given in Appendix C, such as cryptographic algorithm.

3.8 Asymmetric cryptographic technique

USE two correlation-transform cryptographic techniques: a public transformation defined by public key and a private transformation defined by private key. The two transformations have the following nature: Within the given finite time, and under the given computational resources, it is not computationally feasible to deduce the private transformation from the given public transformation.

3.9 Bypass capability

The capability of a service to partly or totally bypass cryptographic functions.

3.10 Certificate

Entity data which cannot be forged, and which are produced based on the private key or secret key of authentication authority.

3.11 Compromise

Unauthorizedly DISCLOSE, modify, replace, or use critical sensitive data; or unauthorizedly MODIFY or replace public security parameters.

3.12 Conditional self-test

When the specified test condition occurs, a test performed by cryptographic modules.

3.13 Confidentiality

key of the signer, to confirm the integrity of the data to be signed, the authenticity of the signer's identity, and the nonrepudiation of the signature behavior.

3.29 Electromagnetic emanations

The signal which contains useful information. Once it is intercepted and analyzed, the information transmitted, received, processed, or operated by an information processing device may be divulged.

3.30 Electronic key entry

The operation where SSP or cryptographic key component, by electronic means, is input into cryptographic modules.

3.31 Encrypted key

The key which is encrypted by approved security function; it is considered protected.

3.32 Entity

Person, block, device, or process.

3.33 Entropy

A measure of disorder, randomness, or variability of closed systems. The entropy of random variable X is the mathematical measure of the amount of information obtained by observing X.

3.34 Environmental failure protection

The characteristics implemented on a cryptographic module to prevent the damage to the security of cryptographic module caused by environmental conditions beyond the normal operational range of the module.

3.35 Environmental failure testing

USE a specific test method to ensure the security of cryptographic module; so that it will not be damaged by the environment conditions beyond the normal operational range of the module.

3.36 Error detection code

The value formed by redundant bits which are calculated from the data to be tested, which is used to detect whether the data are unintentionally altered; but not to correct.

PSP: Public Security Parameters

RBG: Random Bit Generator

SFMI: Software (Firmware) Module Interface

SSP: Sensitive Security Parameter

5 Security levels of cryptographic module

5.1 Overview

Cryptographic modules are a series of hardware, software, and/or firmware, which are included in cryptographic boundary and perform approved or accepted security functions (including cryptographic algorithms and key generation). To protect the cryptographic module itself and the SSP contained and controlled in cryptographic module, this Standard specifies 4 security levels with incremental security requirements. Some common examples given in this Standard are used to illustrate how to meet the security requirements of this Standard, not to constrain or enumerate all situations. For the purpose of this Standard, the term “module” shall be understood as “cryptographic module”. The following subclauses provide an overview of the 4 security levels. The 4 security levels involve the same cryptographic technique.

This Standard uses “shall [xx.yy]” to identify and sequence all security requirements in the Standard; where xx represents the clause, and yy is the numeric index in the clause. If “shall [xx.yy]” appears in a sentence in this Standard, it means that the sentence is a security requirement of this Standard and is numbered [xx.yy]. There is a total of 12 clauses in this Standard, corresponding to the security domains of cryptographic module. 1~12 represent: general requirements; specifications of cryptographic modules; interfaces of cryptographic modules; roles, services, and authentication; software/firmware security; operational environment; physical security; non-invasive security; management of sensitive security parameters; self-tests; life cycle guarantee; mitigation of other attacks, respectively. Each clause contains specific security requirements. Each security requirement is numbered in sequence from [xx.01].

Any sentence below which contains “shall [xx.yy]” is considered to be a security requirement of cryptographic module. This identification method can be directly referenced by the subsequent test standards corresponding to this Standard, or be referenced by the document submitted by the vendor of cryptographic module.

shall prevent unauthorizedly executing, modifying, and reading the software which realizes cryptographic function.

5.4 Security level 3

In addition to the physical security mechanism of tamper trace required in security level 2, security level 3 requires a stronger physical security mechanism, to prevent unauthorized access to the SSP in cryptographic module. These physical security mechanisms shall be able to detect and respond to the following behaviors with a high probability. These behaviors include: direct physical access, use or modification of cryptographic modules, and detection of modules through vents or seams. The physical security mechanisms described above may include a solid shell, a tamper detection device, and a zeroization response circuit. When the removable cover/door of cryptographic module is opened, the zeroization response circuit shall set-to-zero all CSPs.

Security level 3 requires identity-based authentication mechanism, to improve the security of the role-based authentication mechanism in security level 2. The cryptographic module needs to authenticate the identity of the operator, and verify that whether the authenticated operator is authorized to play a specific role and can perform the corresponding services.

Security level 3 requires that the manually-created plaintext CSP is encrypted; and by trusted channel or split knowledge, is input or output.

The cryptographic module of security level 3 shall effectively prevent environmental factors, or voltage, temperature beyond the normal operational range of the module destroying the security of cryptographic module. Intentional deviations from the normal operational range can be exploited by an attacker, thereby circumventing the protective measures of cryptographic module. The cryptographic module shall be designed with special environmental protection characteristics, to detect environmental anomalies and set-to-zero CSP; or through environmental failure testing, to provide a reasonable guarantee; so as to ensure that the module's security will not be destroyed due to environmental anomalies.

For the test index of security level 3, TEST the mitigation methods for non-invasive attacks which are realized in cryptographic module and stipulated in 7.8.

For software cryptographic module, there is no requirement for security level 3 in all clauses of this Standard. Therefore, the maximum overall security level which the software cryptographic module can achieve is limited to security level 2.

defined cryptographic boundary, but explicitly bound to the firmware module.

- **Hybrid software module:** The cryptographic boundary delimits the collection of software components and disjoint hardware components (That is, the software components are not in the hardware module boundary). The computing platform and operating system included in the software operational environment are outside the defined hybrid software module boundary.

- **Hybrid firmware module:** The cryptographic boundary delimits the synthesis of firmware components and disjoint hardware components (That is, the firmware components are not in the hardware module boundary). The computing platform and operating system included in the firmware operational environment are outside the defined hybrid firmware module boundary, but explicitly bound to the hybrid firmware module.

For software modules which run in a modifiable environment, the physical security specified in 7.7 and the non-invasive security requirements specified in 7.8 are optional.

For hardware and firmware modules, the physical security specified in 7.7 and the non-invasive security requirements specified in 7.8 “shall [02.04]” be applicable.

For hybrid modules, the software and firmware components “shall [02.05]” meet all the applicable requirements of the software/firmware security specified in 7.5 and the operational environment specified in 7.6. Hardware components “shall [02.06]” meet all the applicable requirements of the physical security specified in 7.7 and the non-invasive security specified in 7.8.

7.2.3 Cryptographic boundary

7.2.3.1 General requirements for cryptographic boundary

The cryptographic boundary “shall [02.07]” be made up of well-defined side boundaries (for example, the collection of hardware, software, or firmware components), which establish the boundary of all components of a cryptographic module. The requirements of this Standard “shall [02.08]” apply to all algorithms, security functions, processes, and components within the cryptographic module boundary. The cryptographic boundary “shall [02.09]” contain at least all security-relevant algorithms, security functions, processes, and components within the cryptographic module (that is, security-relevant within the scope of this Standard). Non-security relevant algorithms, security functions, processes, and components can also be included within cryptographic boundary. The implementation of non-security relevant

- Data output interface: Except for the state data output from the “state output” interface and the control data output through the “control output” interface, all output data from cryptographic module, including plaintext, ciphertext, SSP, etc., “shall [03.06]” be output through the “data output” interface. In the process of executing manual input, pre-operational self-test, software/firmware load, and zeroization, or when the cryptographic module is in an error state, it “shall [03.07]” prohibit data output through the “data output” interface.

- Control input interface: All input commands, signals (for example, clock input), and control data (including manual controls such as switches, buttons, and keyboards; and function calls) used to control the operation of cryptographic module “shall [03.08]” be input through the “control input” interface.

- Control output interface: All output commands, signals, and control data (for example, the control command for another module) used to control the operation of cryptographic module “shall [03.09]” be output through the “control output” interface. When the cryptographic module is in an error state, it “shall [03.10]” prohibit the control output through the “control output” interface, unless some exceptions are specified and documented in the security policy.

- State output interface: All output signals, indicators (such as error indicators), and state data [including return codes and physical indicators, such as visual (displays, indicator lights), sonic (buzzer, warning tone, bell), and mechanical (vibrator)] used to indicate the state of cryptographic module, “shall [03.11]” be output through the “state output” interface. State output can be explicit or implicit.

In addition to the software cryptographic modules, all modules “shall [03.12]” also have the following interface:

- Power interface: All external electrical energy which is input into cryptographic module “shall [03.13]” be input through the power interface. The power interface is not necessary. When all energy is supplied or maintained from within the cryptographic boundary of the cryptographic module (for example, through an internal battery), there is no need for the power interface.

The cryptographic module “shall [03.14]” distinguish between the input of data, control information, and energy; and the output of data, control information, and status information. The specifications of cryptographic modules “shall [03.15]” specify the format of input data and control information, including the length limitation for all variable-length inputs.

the module “shall [04.38]” authenticate whether the operator can assume the new role.

Identity-based authentication: If a cryptographic module supports identity-based authentication mechanism, the module “shall [04.39]” require a separate and unique-identification operator; “shall [04.40]” require the operator to implicitly or explicitly select one or more roles; and “shall [04.41]” authenticate the identity of operator, and whether the operator is authorized to play the selected role (or collection of roles). To authenticate the identity of operator, select roles, and to authenticate whether the operator can be authorized to play the selected roles can be combined. If the cryptographic module allows an operator to change its role, and if the requested new role has not been authorized before, the module “shall [04.42]” authenticate whether the identified operator is authorized to assume this new role.

The cryptographic module can allow an authenticated operator to perform all the services allowed by the authorized role; or it can separately authenticate each service or a set of services. When a cryptographic module is reset, restarted, closed, and then opened again, the module “shall [04.43]” require to re-authenticate the operator.

A cryptographic module may require multiple types of authentication data to implement the authentication mechanism supported by the module, including (but not limited to) knowing or owning a password, PIN, cryptographic key, etc.; owning a physical key, password token, etc.; or validating personal characteristics (for example, biological characteristics). It “shall [04.44]” protect the authentication data in the cryptographic module to prevent unauthorized leakage, modification, and replacement. Approved security functions can be used for authentication mechanisms.

It shall allow the initialization of authentication mechanism to be specially processed. If a cryptographic module does not contain the authentication data required to authenticate the operator when it is first accessed, it “shall [04.45]” use other authorized methods (for example, program control, USE exit-factory settings or default authentication data) to execute access control and initialization authentication on the module. If the default authentication data are used to control access to the module, after the first authentication, the default authentication data “shall [04.46]” be replaced. The default authentication data do not need to meet the requirements for zeroization specified in 7.9.7.

The authentication mechanism can be a set of mechanisms with different authentication attributes, which can be combined to satisfy the requirements of this clause. If a cryptographic module uses security functions to authenticate operators, then, those security functions “shall [04.47]” be approved security

For security level 3 and 4, in addition to the requirements for security level 1 and 2, the following requirements “shall [05.17]” be applicable to the software or firmware components within the cryptographic module:

- All software or firmware within a cryptographic boundary “shall [05.18]” be protected by approved digital signature. If the calculation result is not equal to the result generated before, the test fails; and the module “shall [05.19]” enter the error state.

- The digital signature technique can include a single signature, or multiple partial signatures. The authentication failure of any signature among the partial signatures “shall [05.20]” cause the module to enter an error state. The private key of signature “shall [05.21]” be stored outside the module.

7.6 Operational environment

7.6.1 General requirements for operational environment

The operational environment of cryptographic environment refers to the management of software, firmware, and/or hardware required for the operation of module. The operational environment of software, firmware, or hybrid module includes at least module components, computing platform, and an operating system which controls or allows software or firmware to run on the computing platform. The operational environment within the hardware module can include an operating system which supports the operation of the internal software or firmware. The operating system can include virtual machine [system and/or process] and runtime environment (for example, Java runtime environment - JRE).

The general operational environment is the use of a commercial general operating system (i.e., a resource manager) to manage software and firmware components, as well as management systems and operator processes (threads), which include general applications software, such as word processor, etc.

The operational environment can be non-modifiable, limited, or modifiable.

The following clauses illustrate three specific operational environments:

a) A non-modifiable environment is designed or configured to prevent the operator or process from modifying module components, computing platform, or operating system. That is, the module components, computing platform, or operating system in the environment are not allowed to be modified. The environment may contain the firmware modules which run on non-programmable computing platform, or the

hardware modules with the capability to prevent any other software or firmware from being loaded.

b) A limited operational environment is designed or configured in a way where the operator or process is allowed, in a controlled manner, to modify module components, computing platform, or operating system. That is, the modifications to the module components, computing platform, or operating system in this environment must meet relevant requirements. In limited operational environment, if the firmware which run on programmable hardware module is contained, then, in this module, to load other firmware needs to meet the firmware load requirements specified in 7.4.3.4.

c) A modifiable operational environment is an environment which can be reconfigured by adding/deleting/modifying certain functions, and/or one which contains the functions of general operating system (For example, it can choose to use computer operating system, configure smart card operating system, or to load programmable software). If an operator or process can modify software components, and/or load and execute certain software (for example, word processor); and the software is not part of existing software, firmware, or hybrid modules; then, the operational system is considered as a modifiable operational environment. A modifiable operational environment has the following characteristics:

In the operational environment, functions can be added or modified. These added or modified functions may interfere with the operation of cryptographic module unless the operational environment prohibits such interference. In such an environment, it requires that, the functions which run under the same operational environment and are not trusted parts of the operational environment, except for the interfaces which have been defined through the cryptographic module, cannot access SSP by other means. Therefore, when the operational environment is running, it is required to have the capability to isolate the functions of cryptographic module from other functions in the operational environment; so that from the cryptographic module, the other functions which are isolated cannot obtain the information related to CSP. And except for the interfaces provided by the cryptographic module itself, by other means, the other functions cannot modify the CSP, PSP, or execution stream of the cryptographic module. Specific configuration of the operational environment may be required, to adequately protect the code and data of cryptographic module (For example, PROHIBIT cryptographic module from implementing internal process communication of specific type; or ASSIGN restricted access permission to the documents which contain the SSP or code of cryptographic module).

covers on passivation layer) to cover the cryptographic module; or install the module in a shell of tamper trace, to prevent direct observation, detection, or control of the module, and to leave evidence after attempting to tamper or move the module.

c) Security level 3:

In addition to the requirements for security level 1 and 2, the single-chip cryptographic module of security level 3 “shall [07.36]” also meet the following requirements:

- It “shall [07.37]” use a hard and opaque coating of tamper trace (for example, hard opaque epoxy resin coated on passivation layer) to cover the cryptographic module.

- It “shall [07.38]” reasonably implement the shell of module. The attempt to tamper or penetrate the shell “shall [07.39]” most likely cause serious damage to the cryptographic module; that is, the module will not work.

d) Security level 4:

In addition to the requirements for security level 1, 2, and 3, the single-chip cryptographic module of security level 4 “shall [07.40]” also meet the following requirements:

- It “shall [07.41]” use an anti-erasure hard and opaque coating to cover the cryptographic module. The coating has hardness and viscosity characteristics. So that the attempt to flake or pry the coating is likely to cause serious damage to the module; that is, the module will not work.

- The anti-erasure coating “shall [07.42]” have dissolution characteristic. So that the attempt to dissolve the coating will most likely dissolve or seriously damage the module; that is, the module will not work.

7.7.3.2 Multiple-chip embedded cryptographic module

In addition to the general security requirements specified in 7.7.2, for multiple-chip embedded cryptographic module, the following requirements are set:

a) Security level 1:

If the cryptographic module is installed in a shell or removable cover, it “shall [07.43]” use the production grade shell or removable cover.

b) Security level 2:

trace (for example, flexible polyester film printed circuit, serpentine wire, or winding pack, or inelastic fragile circuit, or solid shell), the shell “shall [07.54]” be encapsulated. The envelope “shall [07.55]” be able to detect the tamper attempts to access SSP, including cutting, drilling, grinding, milling, burning, melting, dissolving the encapsulation material or shell, etc.

- The cryptographic module “shall [07.56]” contain tamper response and zeroization circuit. The tamper response and zeroization circuit “shall [07.57]” be able to continuously monitor the tamper detection envelope. Once the tamper behavior is detected, they “shall [07.58]” immediately set-to-zero all unprotected SSPs. When the cryptographic module contains unprotected SSP, the tamper response circuit “shall [07.59]” remain available.

7.7.3.3 Multiple-chip standalone cryptographic module

In addition to the general security requirements specified in 7.7.2, for multiple-chip standalone cryptographic module, the following requirements are set:

a) Security level 1:

The cryptographic module “shall [07.60]” be entirely encapsulated in a production grade shell of metal or rigid plastics. The shell can have door or removable cover.

b) Security level 2:

In addition to the requirements for security level 1, the multiple-chip standalone cryptographic module of security level 2 “shall [07.61]” also meet the following requirements:

- If the shell of cryptographic module contains any door or removable cover, the door or removable cover “shall [07.62]” be installed with a pick-resistant mechanical lock with physical or logical keys; or “shall [07.63]” be protected by the seal of tamper trace (for example, trace tape or holographic seal).

c) Security level 3:

In addition to the requirements for security level 1 and 2, the multiple-chip standalone cryptographic module of security level 3 “shall [07.64]” also meet the following requirements:

"shall [09.12]" be via the defined HMI, SFMI, HFMI, or HSMI interface specified in 7.3.2.

All SSPs protected by cryptographic technique, whether input into or output from a module, "shall [09.13]" be encrypted by approved security function.

For the SSP which is directly input, the input value can be displayed temporarily, to allow visual verification and improve accuracy. If an encrypted SSP is input directly into the module, the plaintext value of the SSP "shall not [09.14]" be displayed. The (plaintext or encrypted) SSP which is directly input "shall [09.15]", in the process of inputting into the module, use the conditions specified in 7.10.3.5 to manually input the test for verification, to ensure accuracy.

To prevent inadvertent output of sensitive information, it "shall [09.16]" require two separate internal operations to perform the output of any plaintext CSP. These two separate internal operations "shall [09.17]" be specially designed to jointly control the output of CSP.

For electronic input or output via wireless connection, CSP, cryptographic key components, and authentication data "shall [09.18]" be encrypted.

Manually-input PSP does not need to be authenticated by cryptographic technique.

a) Security level 1 and 2:

   Through physical ports and logical interfaces, plaintext CSP, cryptographic key components, and authentication data can be input and output. These ports and interfaces can be shared with other ports and interfaces of cryptographic module.

   For the software components of software module or hybrid software module, in encrypted or plaintext form, CSP, cryptographic key components, and authentication data can be input or output; provided that the CSP, cryptographic key components, and authentication data "shall [09.19]" remain in the operational environment only and meet the requirements specified in 7.6.3.

b) Security level 3:

   For security level 3, in addition to the requirements for security level 1 and 2, CSP, cryptographic key components, and authentication data "shall [09.20]", in encrypted form or through trusted channel, be input into or output from module.

software/firmware integrity test “shall [10.18]” fail. For any software/firmware which is not subject to the security requirements of this Standard, or for any executable code stored in non-reconfigurable memory, the pre-operational software/firmware integrity test is not required.

If a hardware module does not contain software or firmware, the module “shall [10.19]” implement at least one of the cryptographic algorithm self-test specified in 7.10.3.2 as pre-operational self-test.

The cryptographic algorithm used for the approved integrity technique for pre-operational software/firmware test “shall [10.20]” first pass the cryptographic algorithm self-test specified in 7.10.3.2.

7.10.2.3 Pre-operational bypass test

If a cryptographic module realizes bypass capability, then the module “shall [10.21]” ensure that the logic for managing bypass capability is correct. Through the following methods, the module “shall [10.22]” authenticate the data path:

- SET the bypass switch in an encrypted position; VERIFY that the data transmitted by bypass mechanism are encrypted.

- SET the bypass switch in a non-encrypted position; VERIFY that the data transmitted by bypass mechanism are non-encrypted.

7.10.2.4 Pre-operational critical function testing

Other critical security functions related to the secure operation of cryptographic module “shall [10.23]” be tested before running. The document “shall [10.24]” specify the critical functions which need to be tested before running.

7.10.3 Conditional self-tests

7.10.3.1 General requirements for conditional self-tests

When the conditions specified by the following tests occur, the cryptographic module “shall [10.25]” perform corresponding tests: cryptographic algorithm self-test, pairing consistency test, soft/firmware load test, manual key entry test, conditional bypass test, and conditional critical function testing.

7.10.3.2 Cryptographic algorithm self-test

Cryptographic algorithm self-test: For all cryptographic functions (for example, security function, SSP establishment method, authentication) of each approved cryptographic algorithm, it “shall [10.26]” perform cryptographic algorithm tests. Before the cryptographic algorithm runs for the first time, it “shall [10.27]” perform this conditional test.

Error state: the state in which the cryptographic module encounters an error condition (for example, self-test failure). A single module error state can be caused by one error condition, or by multiple error conditions. The error state can include: “hard” error which indicates a device failure; such errors may require upkeep, maintenance, or repair of cryptographic module. Or recoverable “soft” error, such errors may require initialization or restart of the module. To restore from an error state “shall [11.11]” be possible, except for those error states caused by “hard” errors which require upkeep, maintenance, or repair of cryptographic module.

Each different cryptographic module service, security function use, error state, self-test, or operator authentication “shall [11.12]” be described as a separate state.

Any role other than the cryptographic officer “shall [11.13]” be prohibited from being converted to the cryptographic officer state.

The cryptographic module may contain other states, including, but not limited to, the following two states:

Bypass state: a state of module; in which, due to module configuration or operator intervention, the service, in plaintext form, outputs the specific data or state item which shall normally be output in encrypted form.

Inactive state: the state in which cryptographic module is at rest (for example, low power consumption, standby, or sleep).

7.11.5 Development

The cryptographic module shall have a strict and compliant development process, to ensure that: The realization of cryptographic module is consistent with the function definition and security policy of the module. The cryptographic module is maintainable. The validated cryptographic module is reproducible. This clause sets out the security requirements of cryptographic module at all levels of abstraction, from functional specification to concrete realization:

a) Security level 1:

The cryptographic module of security level 1 “shall [11.14]” meet the following security requirements:

- If the cryptographic module contains software or firmware, then, source code, programming language, compiler, compiler version and compiler options, linker and linker options, runtime library and runtime library settings, configuration settings, generation process and methods, generation options, environment variables, and all other resources used

- The design and realization of software cryptographic module “shall [11.26]” avoid using the codes, parameters, or symbols which are unnecessary for module function and operation.

c) Security level 4:

In addition to the requirements for security level 1, 2, and 3, the cryptographic module of security level 4 “shall [11.27]” also meet the following security requirements:

- For the hardware and software components of each cryptographic module, the document “shall [11.28]” have comments, to illustrate: when entering a module component, function, or program, the pre-conditions required to ensure correct execution; when the execution of the module component, function, or program is completed, the post-conditions of which the expected value is true. The pre- and post-conditions can be described in any sufficiently detailed representation, to completely and clearly explain the behavior of cryptographic module components, functions, or programs.

7.11.6 Vendor test

This clause sets out requirements for the vendor test of cryptographic module, including the test of security functions realized in cryptographic module, thus ensuring that the actual behavior of cryptographic module is consistent with the module security policy and functional specification:

a) Security level 1 and 2:

For security level 1 and 2, the document “shall [11.29]” clarify the function testing performed on the cryptographic module.

For software or firmware components in software or firmware cryptographic modules and in hybrid modules, the vendor “shall [11.30]” use a common automatic security diagnostic tool (for example, CHECK buffer overflow, etc.).

b) Security level 3 and 4:

In addition to the requirements in security level 1 and 2, the document “shall [11.31]” explain the process and results of the low-level testing performed on the cryptographic module.

7.11.7 Distribution and operation

other SSPs used by cryptographic module. (Security level 1, 2, 3, and 4)

- Description of all REGs used by the cryptographic module and the usage. (Security level 1, 2, 3, and 4)

- Description of the minimum entropy value of the entropy source which is output by cryptographic module to the outside. (Security level 1, 2, 3, and 4)

- Description of each REG (approved REG, non-approved REG, and entropy source) used by cryptographic module. (Security level 1, 2, 3, and 4)

- If the entropy is collected within the cryptographic boundary of cryptographic module, description of the minimum entropy and its generation method. (Security level 1, 2, 3, and 4)

- Description of each method of using REG to generate SSP. (Security level 1, 2, 3, and 4)

- Description of all SSP establishment methods used by cryptographic module. (Security level 1, 2, 3, and 4)

- Description of each SSP generation method used by cryptographic module. (Security level 1, 2, 3, and 4)

- Description of each approved key generation method used by cryptographic module. (Security level 1, 2, 3, and 4)

- Description of SSP establishment methods used by cryptographic module. (Security level 1, 2, 3, and 4)

- Description of SSP input and output methods used by cryptographic module. (Security level 1, 2, 3, and 4)

- Description of key input and output methods used by cryptographic module. (Security level 1, 2, 3, and 4)

- If the split knowledge process is used, and if it proves that n cryptographic key components are needed to reconstruct the original CSP; then, any n-1 components do not provide any information about the original CSP except the length. (Security level 3 and 4)

- Description of the split knowledge process used by cryptographic module. (Security level 3 and 4)

- Description of the SSP storage method used by cryptographic module. (Security level 1, 2, 3, and 4)

state, including data input and control input;

- Output event which results from the transition from one state to another state, including internal module state, data output, and state output.

- Description of the source code of software or firmware. (Security level 1, 2, 3, and 4)

- For the hardware and software components of each cryptographic module, the comments annotated in the source code shall specify: when calling a module component, function, or program, the pre-conditions required to ensure correct execution; when the execution of the module component, function, or program is completed, the post-conditions of which the expected value is true. (Security level 4)

- The administrator guidance shall make the following descriptions: (Security level 1, 2, 3, and 4)

  - The cryptographic module's management functions, security events, security parameters (and appropriate parameter values), physical ports, and logical interfaces available to cryptographic officer;

  - Steps on how to securely manage cryptographic module;

  - Assumptions of user behavior associated with the secure operation of cryptographic module.

- The non-administrator guidance shall make the following descriptions: (Security level 1, 2, 3, and 4)

  - Approved security functions, physical ports, and logical interfaces available to the user of cryptographic module;

  - Necessary responsibilities assumed by the user to ensure the secure operation of module.

A.2.12 Mitigation of other attacks

The document requirements for mitigation of other attacks include:

- If cryptographic module is designed to be able to mitigate one or more specific attacks which are not defined in this Standard, in the module's document, LIST the cryptographic module's security mechanisms for mitigating the attacks. (Security 1, 2, and 3)

- If cryptographic module is designed to be able to mitigate one or more

Appendix B

(Normative)

Cryptographic module's security policy

B.1 Purpose

This appendix summarizes the requirements which "shall [B.01]" be provided in non-private security policy. The format of security policy "shall [B.02]" be presented in the order indicated in this appendix. In the absence of a statement allowing copying or distribution, it "shall not [B.03]" mark the security policy as a private or copyrighted document.

B.2 Clauses

B.2.1 General

- GIVE a table, SHOW the level of cryptographic module in 11 security domains and the overall security level achieved.

B.2.2 Specifications of cryptographic module

- Intended use and usage of the module, including the intended use environment.

- Schematic diagram, sketch map, or photo of module. If it is a hardware module, it shall contain a photo of the module. If the security policy includes multiple versions of the module, each version shall be stated separately; or NOTE that the statement is for all the versions. For software or firmware cryptographic module, the security policy shall contain block diagram, to illustrate:

    - The location of the logical objects contained in software or firmware module relative to the operating system, other supporting applications, and cryptographic boundary, to make all logical and physical layers between the logical objects and the cryptographic boundary clearly-defined;

    - The interaction OF the logical objects in software or firmware module WITH the supporting applications in operating system and other physical boundaries.

- Module description:

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------