GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80
File No.: 49738-2015

GM/T 0039-2015

Security test requirements for cryptographic modules

密码模块安全检测要求

Issued on: April 1, 2015 **Implemented on: April 1, 2015**

Issued by: State Cryptography Administration

Table of Contents

Foreword 3
1 Scope 4
2 Normative references 4
3 Terms and definitions 4
4 Abbreviations 4
5 Document organization 5
5.1 General 5
5.2 Clauses and security requirements 5
5.3 Description of reference clauses 6
6 Security test requirements 6
6.1 General requirements 6
6.2 Cryptographic module specification 7
6.3 Cryptographic module interfaces 23
6.4 Roles, services, and authentication 40
6.5 Software / Firmware security 65
6.6 Operational environment 72
6.7 Physical security 88
6.8 Non-invasive security 119
6.9 Sensitive security parameter management 121
6.10 Self-tests 137
6.11 Life-cycle assurance 162
6.12 Mitigation of other attacks 180
6.13 A - Documentation requirements 181
6.14 B - Cryptographic module security policy 182
6.15 C - Approved security functions 183
6.16 D - Approved sensitive security parameter generation and establishment methods 183
6.17 E - Approved authentication mechanisms 183
6.18 F - Non-invasive attacks and common mitigation test metrics 183
Annex A (Informative) Security level correspondence tables 184

Foreword

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

This Standard was prepared by redrafting with reference to ISO / IEC 24759:2014 *Information technology - Security techniques - Test requirements for cryptographic modules*. The degree of consistency with ISO / IEC 24759:2014 is not equivalent.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The issuing authority 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 Technical Committee for Standardization of Cryptography Industry.

Main drafting organizations of this Standard: Bejing Watchdata Intelligent Technology Co., Ltd, Feitian Technologies Co., Ltd, Beijing HuaDa ZhiBao Electronic System Co., Ltd, Beijing Haitai Fangyuan Technologies Co., Ltd, Commercial Cryptography Testing Center of State Cryptography Administration, Data Assurance & Communications Security (DCS) Center, Beijing Creative Century Technology Co., Ltd, Shanghai Koal Software Co., Ltd.

Main drafters of this Standard: Wang Xuelin, Li Dawei, Deng Kaiyong, Chen Guo, Chen Baoru, Zhang Yifei, Hu Boliang, Zhu Pengfei, Luo Peng, Zhang Zhong, Lei Yinhua, Mo Fan, Lin Chun, Jiang Hongyu, Tan Wuzheng, Zhang Wantao, Gao Neng.

Security test requirements for cryptographic modules

1 Scope

This Standard specifies a series of test procedures, test methods and corresponding document submission requirements for cryptographic modules, in accordance with the requirements of GM/T 0028-2014.

This Standard is applicable to the tests of cryptographic modules.

2 Normative references

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

GM/T 0028-2014 *Security requirements for cryptographic modules*

GM/Z 4001 *Cryptology terminology*

3 Terms and definitions

The terms and definitions defined in GM/T 0028-2014 and GM/Z 4001 are applicable to this document.

4 Abbreviations

The following abbreviations are applicable to this document.

API	Application Program Interface
CBC	Cipher Block Chaining
CSP	Critical Security Parameter
EDC	Error Detection Code
EFP	Environmental Failure Protection
EFT	Environmental Failure Testing

Following each clause is the requirements for the required vendor documentation. These requirements describe the types of documentation or explicit information that the vendor shall provide in order for the tester to verify conformity (of the documentation or information) to the given clause.

These requirements are denoted by the form:

CY<requirement number>.<clause sequence number>.<sequence number>

where “CY” represents the requirements for the documents that are submitted by the vendor, “requirement number” and “clause sequence number” are identical to those in the corresponding security requirement, and “sequence number” is a sequential identifier for vendor requirements within the clause.

Following the required vendor documentation is the requirements for the required test procedures. These requirements instruct the tester as to what he or she shall do in order to test the cryptographic module with respect to the given clause.

These requirements are denoted by the form:

JY<requirement number>.<clause sequence number>.<sequence number>

where “JY” represents the requirements for the test procedures and methods, “requirement number” and “clause sequence number” are identical to those in the corresponding security requirement, and “sequence number” is a sequential identifier for tester requirements within the clause.

5.3 Description of reference clauses

For coherence in the statements, this Standard adds supplementary statements to some of the clauses that are direct quotations from GM/T 0028-2014. These statements have been put between curly brackets “***{***” and “***}***” and are italicized in bold font of Song typeface.

In addition, the “shall” used in the requirements for the vendor documentation and the requirements for the test procedures required by this Standard have the same meaning as the “should” in the clauses that are directly quoted from GM/T 0028-2014.

6 Security test requirements

6.1 General requirements

NOTE: This subclause states general requirements to meet the articles of the other subclauses in Clause 6.

description of the approved mode of operation.

JY02.19.02: The tester shall verify that it is able to activate the approved mode of operation according to the method described in the vendor documentation.

JY02.19.03: The tester shall verify that the operator is able to operate the cryptographic module in an approved mode of operation.

AY02.20: (Security levels 1, 2, 3 and 4)

An approved mode of operation shall be defined as the set of services which include at least one service that utilizes an approved cryptographic algorithm, security function or process.

Required vendor documentation

CY02.20.01: The vendor documentation shall describe the approved cryptographic algorithm, security function or process that is used in the approved mode of operation for the cryptographic module and those services specified in 7.4.3 of GM/T 0028-2014.

CY02.20.02: The vendor documentation shall provide a verification certificate that includes all approved cryptographic algorithms, security functions or processes.

Required test procedures

JY02.20.01: The tester shall verify the approved mode of operation described in the documentation, and that at least one service uses the approved cryptographic algorithm, security function or process and those services or processes specified in 7.4.3 of GM/T 0028-2014.

JY02.20.02: The tester shall verify the vendor provided verification certificate for approved cryptographic algorithms, security functions or processes.

JY02.20.03: The tester shall verify that the approved modes of operation and security functions for use described in the documentation meet the requirements of Annex C in GM/T 0028-2014.

AY02.21: (Security levels 1, 2, 3 and 4)

Non-approved cryptographic algorithms, security functions, and processes or other services not specified in *{GM/T 0028-2014}* 7.4.3 shall not be utilized by the operator in an approved mode of operation unless the non-approved cryptographic algorithm or security function is part of an approved process and is non-security relevant to the approved processes operation (e.g. a non-approved cryptographic algorithm or

commands using the external input device(s).

AY03.09: (Security levels 1, 2, 3 and 4)

All output commands, signals, and control data (e.g. control commands to another module) used to control the operation of a cryptographic module shall exit via the "control output" interface.

Required vendor documentation

CY03.09.01: The cryptographic module shall have a control output interface. The output commands, signals, and control data used to control the operation of a cryptographic module must be output via the control output interface.

CY03.09.02: If applicable, the vendor documentation shall describe all external devices that are used in conjunction with the cryptographic module and that are used to output control data from the control output interface, such as smart cards, tokens, displays and / or other storage devices.

Required test procedures

JY03.09.01: The tester shall verify that the output commands, signals and control data used to control the operation of a cryptographic module shall be output via the control output interface.

JY03.09.02: The tester shall verify whether the vendor documentation specifies the external devices that are used in conjunction with the cryptographic module and that are used to output control data from the control output interface, such as smart cards, tokens, displays and / or other storage devices.

AY03.10: (Security levels 1, 2, 3 and 4)

All control output via the "control output" interface shall be inhibited when the cryptographic module is in an error state unless exceptions are specified in the security policy.

Required vendor documentation

CY03.10.01: The vendor documentation shall specify how the cryptographic module ensures that all control output via the "control output" interface is inhibited whenever the module is in an error state.

CY03.10.02: The vendor documentation shall specify how the design of the cryptographic module ensures that all control output via the control output interface is inhibited whenever the module is in a self-test condition.

Required test procedures

JY03.10.01: The tester shall verify that all output via the “control output” interface is inhibited whenever the cryptographic module is in an error state.

JY03.10.02: The tester shall verify that all output via the “control output” interface is inhibited whenever the cryptographic module is in a self-test status.

AY03.11: (Security levels 1, 2, 3 and 4)

All output signals, indicators (e.g. error indicator), and status data [including return codes and physical indicators such as visual (display, indicator lamps), audio (buzzer, tone, ring), and mechanical (vibration)] used to indicate the status of a cryptographic module shall exit via the “status output” interface.

Required vendor documentation

CY03.11.01: The cryptographic module shall have a status output interface. All status information, signals, logical indicators, and physical indicators used to indicate or display the status of the module shall exit via the status output interface, including:

— status information output logically via an API;

— signal outputs logically or physically via one or more physical ports, such as commands and signals sent through a serial port or a PC card;

— manual status outputs (e.g. using lamps, buzzers, tone, ring, indicators or displays);

— any other output status information.

CY03.11.02: If applicable, the vendor documentation shall specify any external output devices to be used for the output of status information, signals, logical indicators, and physical indicators via the status output interface, such as smart cards, tokens, displays, and / or other storage devices.

Required test procedures

JY03.11.01: The tester shall verify, by inspection, that the cryptographic module includes a status output interface, and that the status output interface functions as specified. The tester shall verify that all status information, signals, logical indicators, and physical indicators used to indicate or display the status of the module shall exit via the status output interface, including:

— status information output logically via an API, such as function calls from a software library or a smart card;

— signal outputs logically or physically via one or more physical ports, such

as status information sent through a serial port or a PC card;

— manual status outputs (e.g. using LEDs, buzzers, or a display);

— any other output status information.

JY03.11.02: The tester shall verify that the vendor documentation specifies any external output devices (if applicable) to be used for the output of status information, signals, logical indicators, and physical indicators via the status output interface.

AY03.12: (Security levels 1, 2, 3 and 4)

Except for the software cryptographic modules, all modules shall also have the following interface.

NOTE: This subclause is not tested separately.

AY03.13: (Security levels 1, 2, 3 and 4)

Power interface: All external electrical power that is input to a cryptographic module shall enter via a power interface.

NOTE: A power interface is not required if all power is provided or maintained internal to the cryptographic module, and that replacement of an internal battery is considered a physical maintenance activity, and is subject to the requirements specified in GM/T 0028-2014, 7.7.

Required vendor documentation

CY03.13.01: If the cryptographic module requires or provides power to / from other devices external to the cryptographic boundary (e.g. a power supply or an external battery), the vendor documentation shall specify a power interface and a corresponding physical port.

CY03.13.02: All power entering or exiting the cryptographic module to / from other devices external to the cryptographic boundary shall pass through the specified power interface.

Required test procedures

JY03.13.01: The tester shall verify if the vendor documentation specifies whether the cryptographic module requires or provides power to / from other devices external to the cryptographic boundary (e.g. a power supply, power cord, power inlet / outlet, or an external battery). The tester shall also verify that the vendor documentation specifies a power interface and a corresponding physical port.

JY03.13.02: The tester shall verify, by inspection of the cryptographic module

Required vendor documentation

CY04.47.01: The vendor documentation shall specify means to control access to the module before it is initialized.

Required test procedures

JY04.47.01: The tester shall verify the vendor documentation describes the procedure by which the operator is authenticated upon accessing the module for the first time.

JY04.47.02: If access to the module before initialization is controlled, the tester shall initiate an error on an uninitialized module and shall verify that the module denies access. The tester shall assume the authorized role and verify that the required authentication complies with the documented procedures. The tester shall attempt to assume other roles before the module has been initialized and verify that the module denies access to the roles.

AY04.48: (Security levels 2, 3 and 4)

If default authentication data is used to control access to the module, then default authentication data shall be replaced upon first-time authentication.

Required vendor documentation

CY04.48.01: The vendor shall verify that default authentication data is used to access the cryptographic module for the first time.

Required test procedures

JY04.48.01: The tester shall verify that default authentication data can be used to access the cryptographic module for the first time.

JY04.48.02: The tester shall verify that default authentication data must be required to be replaced upon first-time authentication. If not replaced, the re-authentication utilizing the default authentication data will be denied.

AY04.49: (Security levels 2, 3 and 4)

If the cryptographic module uses security functions to authenticate the operator, those security functions shall be approved security functions.

Required vendor documentation

CY04.49.01: The vendor shall specify the list of approved security functions used to authenticate operators.

authentication mechanism that is supported by the cryptographic module and the strength of authentication.

Required test procedures

JY04.52.01: The tester shall verify the vendor documentation for the authentication strength of each approved authentication mechanism.

JY04.52.02: The tester shall verify the vendor documentation for each approved authentication mechanism that the objective is met.

AY04.53: (Security levels 2, 3 and 4)

For multiple attempts to use the approved authentication mechanism during a one-minute period, the module shall meet the requirements for the strength of authentication.

Required vendor documentation

CY04.53.01: The vendor documentation shall specify each approved authentication mechanism and the associated probability of a successful random attempt during a one-minute period.

Required test procedures

JY04.53.01: The tester shall verify the vendor documentation for each approved authentication mechanism and the associated probability of a successful random attempt during a one-minute period.

JY04.53.02: The tester shall verify the vendor documentation for each approved authentication mechanism that the associated probability of a successful random attempt during a one-minute period is meeting the objective.

AY04.54: (Security levels 2, 3 and 4)

The approved authentication mechanism shall be met by the module's implementation and not rely on documented procedural controls or security rules (e.g. password size restrictions).

Required vendor documentation

CY04.54.01: The vendor documentation shall specify the methods and principle of implementing the authentication mechanism for the cryptographic module.

Required test procedures

JY04.54.01: The tester shall verify that the authentication mechanism for the cryptographic module does not rely on documented procedural controls or

The following security requirements in *{AY05.04 to AY05.11}* shall apply to software and firmware components of a cryptographic module for Security Level 1.

NOTE: This subclause is not tested separately.

AY05.04: (Security levels 1, 2, 3 and 4)

All software and firmware shall be in a form that satisfies the requirements of *{GM/T 0028-2014}* 7.11.7 without modification prior to installation.

Required vendor documentation

CY05.04.01: The vendor shall provide software and firmware specification.

CY05.04.02: The vendor specification shall describe how to ensure that all software and firmware have not been modified prior to installation.

Required test procedures

JY05.04.01: The tester shall verify, by inspection of the cryptographic module, that specifications provided by vendor documentation are consistent with the actual design of the cryptographic module.

JY05.04.02: The tester shall verify the security of method used by the vendor to ensure that all software and firmware have not been modified prior to installation.

AY05.05: (Security levels 1, 2, 3 and 4)

All software and firmware components within the cryptographic boundary shall be protected using approved integrity technique. The integrity technique can be provided by either cryptographic module, or another validated cryptographic module.

Required vendor documentation

CY05.05.01: The vendor documentation shall specify the approved integrity technique that is applied to all software and firmware components. The integrity technique can be provided by either cryptographic module, or another validated cryptographic module.

CY05.05.02: The vendor documentation shall specify how the integrity technique is applied to all software and firmware components (using either a single encompassing message authentication code or signature, or multiple disjoint authentication codes or signatures).

CY05.05.03: The vendor documentation shall specify the location of the key

debugging technology.

JY05.14.03: The tester shall test these services or control settings to verify that the operator is unable to activate or execute the debugging technology.

AY05.15: (Security levels 2, 3 and 4)

All software or firmware within the cryptographic boundary shall employ approved digital signatures or message authentication codes with the keys for protection.

NOTE: This subclause is tested as part of AY05.16.

AY05.16: (Security levels 2, 3 and 4)

{In conjunction with AY05.15} **If the calculated result does not equal to the previously generated result, the test will fail AND the module shall enter into an error state.**

Required vendor documentation

CY05.16.01: The vendor documentation shall identify the technique used for maintaining the integrity of the cryptographic software and firmware components.

Required test procedures

JY05.16.01: The tester shall verify that the vendor documentation meets the requirements of CY05.16.01.

JY05.16.02: The tester shall attempt to damage the cryptographic software and firmware components. If the integrity is not damaged, the test will fail.

AY05.17: (Security levels 3 and 4)

The following requirements of *{AY05.18 to AY05.21}* shall apply to software and firmware components of a cryptographic module for Security Levels 3 and 4.

NOTE: This subclause is not tested separately.

AY05.18: (Security levels 3 and 4)

All software or firmware within the cryptographic boundary shall employ approved digital signatures for protection.

NOTE: This subclause is tested as part of AY05.19.

AY05.19: (Security levels 3 and 4)

Required test procedures

JY06.06.01: The tester shall verify from the vendor documentation and by inspection of the operational environment mechanism used that it provides the capability to separate individual application processes from each other in order to prevent uncontrolled access to CSPs and uncontrolled modifications of SSPs regardless if CSPs and SSPs are in the process memory or stored on persistent storage within the operational environment.

JY06.06.02: The tester shall perform cryptographic functions as described in the crypto officer and user guidance documentation. While the cryptographic functions are executing, the same or another tester shall attempt to gain access to CSPs and perform modifications of SSPs regardless if CSPs and SSPs are in the process memory or stored on persistent storage within the operational environment.

AY06.07: (Security levels 1 and 2)

Restrictions to the configuration of the operational environment shall be documented in the security policy of the cryptographic module.

Required vendor documentation

CY06.07.01: The vendor shall provide documentation which provides a description of any restrictions to the operational environment.

Required test procedures

JY06.07.01: The tester shall verify any restrictions to the configuration of the operational environment in the vendor documentation.

JY06.07.02: The tester shall verify that any restrictions to the configuration of the operational environment are documented in the Security Policy.

AY06.08: (Security levels 1 and 2)

Processes that are spawned by the cryptographic module shall be owned by the module and are not owned by external processes / operators.

NOTE: This requirement cannot be enforced by administrative documentation and procedures but by the cryptographic module itself.

Required vendor documentation

CY06.08.01: The vendor shall provide a description of the operating system mechanism used to ensure that processes that are spawned by the cryptographic module are owned by the module and are not owned by external processes / operators.

AY06.10: (Security level 2)

All cryptographic software, SSPs, and control and status information shall be under the control of an operating system that implements either role-based access controls or a discretionary access control with robust mechanism of defining new groups and assigning restrictive permissions, for example, through access control lists (ACLs) and with the capability of assigning each user to more than one group.

Required vendor documentation

CY06.10.01: The vendor shall provide operating system documentation which provides a description of the operating system control mechanisms which implements either role-based access controls or a discretionary access control with robust mechanism of defining new groups and assigning restrictive permissions, for example, through access control lists (ACLs) and with the capability of assigning each user to more than one group.

Required test procedures

JY06.10.01: The tester shall verify that the vendor documentation, and by inspection of operating system control mechanisms, that the operating system implements either role-based access controls or a discretionary access control with robust mechanism of defining new groups and assigning restrictive permissions, for example, through access control lists (ACLs) and with the capability of assigning each user to more than one group.

JY06.10.02: The tester shall configure the operating systems role-based access controls or discretionary access controls to give permissions to a specific user or group. The tester, assuming a permitted user or group role, shall attempt to execute, modify, or read SSPs, control or status data which the tester has authorized access.

JY06.10.03: The tester shall configure the operating systems role-based access controls or discretionary access controls to give permissions to a specific user or group. The tester, assuming a different user or group role, shall attempt to execute, modify, or read SSPs, control or status data which the tester has unauthorized access.

AY06.11: (Security level 2)

The operating system shall be configured to protect against unauthorized execution, modification, and reading of SSPs, control and status data.

Required vendor documentation

CY06.11.01: The vendor shall provide operating system documentation which

CY06.18.01: The vendor shall provide operating system documentation which provides a description of how the operating system prevents user process from gaining either read or write access to SSPs owned by other processes and to system SSPs.

CY06.18.02: The vendor provided specifications of how the operating system prevents user process from gaining either read or write access to SSPs owned by other processes and to system SSPs shall be consistent with the roles, groups and services as defined in the Security Policy.

Required test procedures

JY06.18.01: The tester shall verify that the vendor documentation, and by inspection of operating system control mechanisms, that the operating system is configured to prevent user process from gaining either read or write access to SSPs owned by other processes and to system SSPs.

JY06.18.02: The tester shall verify that the roles, groups and services as defined in the Security Policy is consistent with how the operating system is configured to prevent user process from gaining either read or write access to SSPs owned by other processes and to system SSPs.

JY06.18.03: The tester shall configure the operating system control mechanisms to prevent user process from gaining either read or write access to SSPs owned by other processes and to system SSPs. The tester shall verify that user process is prevented from gaining either read or write access to SSPs owned by other processes and to system SSPs.

AY06.19: (Security level 2)

The configuration of the operating system that meets the above requirements *{AY06.16 to AY06.18}* shall be specified in the Administrator Guidance.

Required vendor documentation

CY06.19.01: The vendor shall provide the Administrator Guidance documents which provides a description of how the operating system is configured to meet the requirements in AY06.16 to AY06.18.

Required test procedures

JY06.19.01: The tester shall verify that the vendor provided Administrator Guidance documents provide a description of how the operating system is configured to meet the requirements in AY06.16 to AY06.18.

AY06.20: (Security level 2)

CY06.24.01: The vendor shall provide operating system documentation which provides a description of the audit mechanism provided by the operating system and how each event is marked with the date and time.

Required test procedures

JY06.24.01: The tester shall verify that the vendor documentation, and by inspection of operating system, that an audit mechanism is provided and that each event is marked with the date and time.

AY06.25: (Security level 2)

The cryptographic module shall not include SSPs as part of any audit record.

Required vendor documentation

CY06.25.01: The vendor shall provide operating system documentation which provides a description of the cryptographic module's services that provide audit records to the audit mechanism of the operating system.

Required test procedures

JY06.25.01: The tester shall verify that the vendor documentation, and by inspection of the cryptographic module's services that provide audit records to the audit mechanism of the operating system, that no SSPs are provided in the audit records.

JY06.25.02: The tester shall execute the cryptographic module's services that provide audit records and examine the operating system audit logs to verify that no SSPs were provided.

AY06.26: (Security level 2)

***{The cryptographic module}* shall provide the following events to be recorded by the audit mechanism of the operating system:**

- **modifications, accesses, deletions, and additions of cryptographic data and SSPs;**
- **attempts to provide invalid input for Crypto Officer functions;**
- **addition or deletion of an operator to and from a Crypto Officer role (if those roles are managed by the cryptographic module);**
- **the use of a security-relevant Crypto Officer function;**
- **requests to access authentication data associated with the**

roles are managed by the cryptographic module);

— the use of a security-relevant Crypto Officer function;

— requests to access authentication data associated with the cryptographic module;

— the use of an authentication mechanism (e.g. login) associated with the cryptographic module;

— explicit requests to assume a Crypto Officer role.

NOTE: The tester does not have to test the audit mechanism provided by the operating system and identified by the vendor.

AY06.27: (Security level 2)

The audit mechanism of the operating system shall be capable of auditing the following operating system related events:

— **all operator read or write accesses to audit data;**

— **access to files used by the cryptographic module to store cryptographic data or SSPs;**

— **addition or deletion of an operator to and from a Crypto Officer role (if those roles are managed by cryptographic module);**

— **requests to use authentication data management mechanisms;**

— **attempts to use the trusted channel function and whether the request was granted, when trusted channel is supported at this security level;**

— **identification of the initiator and target of a trusted channel, when trusted channel is supported at this security level.**

Required vendor documentation

CY06.27.01: The vendor shall provide operating system documentation which provides a description of the operating system events that are provided and recorded by the audit mechanism of the operating system.

Required test procedures

JY06.27.01: The tester shall, by review of the operating system documentation, verify that the documentation described operating system events that are provided and recorded by the operating system audit mechanism include:

— all operator read or write accesses to audit data;

Required test procedures

JY07.11.01: The tester shall verify that the vendor documentation describes the maintenance access interface.

JY07.11.02: The tester shall verify that the vendor documentation and implementation are consistent.

AY07.12: (Security levels 1, 2, 3 and 4)

{If a module includes a maintenance role that requires physical access to the contents of the module or if the module is designed to permit physical access (e.g. by the module vendor or other authorized individual), then} **the maintenance access interface shall include all physical access paths to the contents of the cryptographic module, including any covers or doors.**

Required vendor documentation

CY07.12.01: The vendor documentation shall specify the maintenance access interface, including any covers or doors.

Required test procedures

JY07.12.01: The tester shall verify in the vendor documentation that a maintenance access interface is provided, including any covers or doors.

AY07.13: (Security levels 1, 2, 3 and 4)

{If a module includes a maintenance role that requires physical access to the contents of the module or if the module is designed to permit physical access (e.g. by the module vendor or other authorized individual), then} **any covers or doors included within the maintenance access interface shall be safeguarded using the appropriate physical security mechanisms.**

Required vendor documentation

CY07.13.01: The vendor documentation shall specify the maintenance access interface, including any covers or doors.

Required test procedures

JY07.13.01: The tester shall verify that any removable covers or doors included within the maintenance access interface are safeguarded using the appropriate physical security mechanisms.

AY07.14: (Security levels 1, 2, 3 and 4)

The following requirement *{AY07.18 to AY07.20}* shall apply to all cryptographic modules for Security Level 2.

NOTE: This subclause is tested as part of AY07.18 to AY07.20.

AY07.18: (Security levels 2, 3 and 4)

The cryptographic module shall provide evidence of tampering (e.g. on the cover, enclosure, and seal) when physical access to the module is attempted.

NOTE: This subclause is tested as part of AY07.34 to AY07.35 for single-chip embodiments;

This subclause is tested as part of AY07.44 and AY07.45 for multiple-chip embedded embodiments;

This subclause is tested as part of AY07.62 and AY07.63 for multiple-chip standalone embodiments.

AY07.19: (Security levels 2, 3 and 4)

The tamper-evident material, coating or enclosure shall either be opaque or translucent within the visible spectrum (i.e. light of wavelength range of 400 nm to 750 nm) to prevent the gathering of information about the internal operations of the critical areas of the module.

Required vendor documentation

CY07.19.01: The vendor documentation shall specify that the tamper evident material, coating, or enclosure shall be opaque or translucent within the visible spectrum.

Required test procedures

JY07.19.01: The tester shall verify by inspection and from the vendor documentation that the tamper evident material, coating, or enclosure is opaque or translucent within the visible spectrum.

AY07.20: (Security levels 2, 3 and 4)

If the cryptographic module contains ventilation holes or slits, the module shall be constructed in a manner to prevent the gathering of information of the module's internal construction or components by direct visual observation.

Required vendor documentation

CY07.20.01: If the module is contained within a cover or enclosure that contains

The cryptographic module shall provide protection from fault induction.

Required vendor documentation

CY07.32.01: The vendor documentation shall specify the protection mechanism from fault induction.

Required test procedures

JY07.32.01: The tester shall verify from the vendor documentation and by inspection of the module the specified protection mechanisms.

AY07.33: (Security level 4)

The fault induction mitigation techniques and the mitigation metrics employed shall be documented as specified in *{GM/T 0028-2014}* Annex B.

Required vendor documentation

CY07.33.01: The vendor documentation shall specify the fault induction mitigation techniques and the mitigation metrics employed by the module, and document according to the requirements of Annex B in GM/T 0028.

Required test procedures

JY07.33.01: The tester shall verify that the fault induction mitigation techniques and the mitigation metrics employed by the module are documented as specified.

6.7.3 Physical security requirements for each physical security embodiment

6.7.3.1 Single-chip cryptographic modules

NOTE 1: In addition to the general security requirements specified in GM/T 0028-2014, 7.7.2, the following requirements are specific to single-chip cryptographic modules.

NOTE 2: There are no additional Security Level 1 requirements for single-chip cryptographic modules.

AY07.34: (Security levels 2, 3 and 4)

The following requirements *{AY07.35}* shall apply to single-chip cryptographic modules for Security Level 2.

NOTE: This subclause is tested as part of AY07.35.

AY07.35: (Security levels 2, 3 and 4)

The cryptographic module shall be covered with a tamper-evident coating

probability of resulting in serious damage to the module (i.e. the module will not function).

Required vendor documentation

CY07.41.01: The vendor documentation shall clearly identify the kind of coating used and shall provide details of its characteristics, especially hardness and removal resistance.

CY07.41.02: The module shall be covered with a hard, opaque removal-resistant coating. The hardness and adhesion characteristics of the material shall be such that attempting to peel or pry the material from the module will have a high probability of resulting in serious damage to the module (i.e. the module does not function). The material shall be opaque within the visible spectrum.

Required test procedures

JY07.41.01: The tester shall verify by inspection and from the vendor documentation that the module is covered with a hard, opaque removal-resistant coating.

JY07.41.02: The tester shall verify the removal-resistant properties of the module coating. The tester shall attempt to peel or pry the material from the module and verify that this is not possible with a reasonable application of force that the module ceased to function or that the module circuitry was obviously physically destroyed.

AY07.42: (Security level 4)

The removal-resistant coating shall have solvency characteristics such that dissolving the coating will have a high probability of dissolving or seriously damaging the module (i.e. the module will not function).

Required vendor documentation

CY07.42.01: The vendor documentation shall describe the solvency characteristics of the removal-resistant coating. The solvency characteristics of the material shall be such that dissolving the material to remove it will have a high probability of dissolving or seriously damaging the module.

Required test procedures

JY07.42.01: The tester shall verify the vendor documentation to determine the solvency properties of the module's removal-resistant coating.

JY07.42.02: The tester shall test the solvency properties of the module's

Required vendor documentation

CY07.50.01: The vendor documentation shall provide design documentation for the hard coating or potting material.

CY07.50.02: The vendor documentation shall provide documentation regarding the opacity characteristics of the hard coating or potting material.

Required test procedures

JY07.50.01: The tester shall verify that the vendor documentation specifies the hard coating or potting material (e.g. a hard epoxy material).

JY07.50.02: The tester shall verify by inspection and from the vendor documentation the opacity characteristics of the hard coating or potting material.

JY07.50.03: The tester shall verify by inspection and from the vendor documentation that the hard coating or potting material (e.g. a hard epoxy material) cannot be removed or penetrated without having a high probability of causing serious damage to the module.

AY07.51: (Security levels 3 and 4)

***{If the requirement AS07.50 does not apply,}* the module shall be contained within a strong enclosure.**

Required vendor documentation

CY07.51.01: The vendor documentation shall provide supporting design documentation for the strong enclosure. The module shall be entirely contained within a strong enclosure. The enclosure shall be designed such that attempts to remove it will have a high probability of causing serious damage to the circuitry within the module (i.e. the module does not function).

CY07.51.02: If the enclosure contains any doors or covers, the cryptographic module shall contain tamper response and zeroization circuitry. The circuitry shall be able to continuously test these covers and doors, and all unencrypted CSPs shall be zeroized before the covers are removed and the doors are opened. As long as the unencrypted CSPs are included in the module, the circuitry shall be under operation.

Required test procedures

JY07.51.01: The tester shall verify that the vendor documentation specifies whether the enclosure contains any doors or covers and whether a maintenance access interface is specified, then the module shall contain tamper response and zeroization circuitry.

Required vendor documentation

CY07.53.01: The module shall be contained within a tamper detection envelope that will detect tampering attacks against the potting material or enclosure. The vendor documentation shall describe the tamper detection envelope design.

Required test procedures

JY07.53.01: The tester shall verify from the vendor documentation and by inspection that the module contains a tamper detection envelope that surrounds the module components. This barrier shall be designed such that any breach by means such as drilling, milling, grinding, or dissolving to access the module components can be detected by monitoring components in the module.

AY07.54: (Security level 4)

The enclosure shall be encapsulated by a tamper detection envelope (e.g. a flexible mylar printed circuit with a serpentine geometric pattern of conductors or a wire-wound package or a non-flexible, brittle circuit or a strong enclosure).

NOTE: This subclause is not tested separately. It is tested in AY07.55.

AY07.55: (Security level 4)

{In conjunction with AY07.54} **The enclosure shall be able to detect tampering by means such as cutting, drilling, milling, grinding, burning, melting, or dissolving of the potting material or enclosure to an extent sufficient for accessing SSPs.**

Required vendor documentation

CY07.55.01: The module shall be contained within a tamper detection envelope that will detect tampering attacks against the potting material or enclosure. The vendor documentation shall describe the tamper detection envelope design.

Required test procedures

JY07.55.01: The tester shall verify, by review of the vendor documentation and inspection of the module, that the vendor module disassembles the probing enclosure, and that the module is completely encapsulated in the enclosure. This barrier shall be designed such that any breach by means such as drilling, milling, grinding, or dissolving to access the module components can be detected by monitoring components in the module.

AY07.56: (Security level 4)

The module shall contain tamper response and zeroization circuitry.

JY07.65.08: If the enclosure has doors or covers, or if a maintenance access interface is specified, the tester shall test that the module zeroizes all unencrypted CSPs when a door or cover is removed or if the maintenance access interface is accessed.

JY07.65.09: The tester shall test that the enclosure cannot be removed or penetrated without having a high probability of causing serious damage to the module.

AY07.66: (Security level 4)

The following requirements *{AY07.67 to AY07.72}* shall apply to multiple-chip standalone cryptographic modules for Security Level 4.

NOTE: This subclause is tested in AY07.67 to AY07.72.

AY07.67: (Security level 4)

The enclosure of the cryptographic module shall contain a tamper detection envelope that use tamper detection mechanisms such as cover switches (e.g. micro-switches, magnetic Hall effect switches, permanent magnetic actuators, etc.), motion detectors (e.g. ultrasonic, infrared, or microwave), or other tamper detection mechanisms as described in *{GM/T 0028-2004}* 7.7.3.2 Security Level 4.

Required vendor documentation

CY07.67.01: The enclosure or potting material shall be encapsulated by a tamper detection envelope by the use of tamper detection mechanisms. The vendor documentation shall describe the tamper detection envelope design.

Required test procedures

JY07.67.01: The tester shall verify from the vendor documentation and by inspection that the module enclosure or potting material contains tamper detection mechanisms, which shall form a tamper detection envelope that protects the module components. The mechanisms shall be designed such that any breach of the enclosure or potting material to access the module components can be detected.

AY07.68: (Security level 4)

The tamper detection mechanisms shall respond to attacks such as cutting, drilling, milling, grinding, burning, melting, or dissolving to an extent sufficient for accessing SSPs.

NOTE: This subclause is tested as part of AY07.71.

6.7.4.1 General requirements for environmental failure protection / testing

AY07.73: (Security levels 3 and 4)

A module for Security Level 3 shall either employ EFP features or undergo EFT.

Required vendor documentation

CY07.73.01: The vendor shall use either of the following:

— EFP features; or

— EFT.

as specified in GM/T 0028-2014, 7.7.4 to ensure that the following four unusual environmental conditions or fluctuations (accidental or induced) outside of the module's normal operation range will not compromise the security of the module:

— low temperature;

— high temperature;

— large negative voltage;

— large positive voltage.

The vendor shall choose to use EFP or EFT for each condition, but each choice is independent of the choices for the other conditions. The vendor shall provide corresponding supporting documentation for each condition, specifying how the selected approach is used.

Required test procedures

JY07.73.01: The tester shall verify that the documentation states EFP / EFT selection for each condition and how the specified approach is used.

AY07.74: (Security level 4)

A module for Security Level 4 shall employ EFP features.

NOTE: This subclause is tested in AY07.75 to AY07.77.

6.7.4.2 Environmental failure protection features

AY07.75: (Security levels 3 and 4)

specified normal range and verify that the module either shuts down to prevent further operations or zeroizes all unencrypted CSPs.

JY07.77.03: If the module is designed to zeroize all unencrypted CSPs, and the module was still operational after returning to the normal environmental range, the tester shall perform services that require keys and verify that the module does not perform these services.

6.7.4.3 Environmental failure testing procedures

AY07.78: (Security levels 3 and 4)

EFT shall involve a combination of analysis, simulation, and testing of a cryptographic module to provide reasonable assurance that the environmental conditions (accidental or induced) when outside the module's normal operating ranges for temperature and voltage will not compromise the security of the cryptographic module.

NOTE: This subclause is tested as part of AY07.81.

AY07.79, AY07.80: (Security level 4)

EFT shall demonstrate that, if the operating temperature or voltage falls outside the normal operating range of the cryptographic module resulting in a failure, at no time shall the security of the cryptographic module be compromised.

NOTE: This subclause is tested as part of AY07.81.

AY07.81: (Security level 4)

The temperature range shall be tested in the following manners: from a temperature within the normal operating temperature range to the lowest temperature that either shuts down the module to prevent further operation or immediately zeroizes all unprotected SSPs; and from a temperature within the normal operating temperature range to the highest temperature that either shuts down the module to prevent further operation or immediately zeroizes all unprotected SSPs.

Required vendor documentation

CY07.81.01: If EFP is chosen for a particular condition, the module shall be tested within the temperature and voltage ranges specified in AY07.82. The module shall either

— continue to operate normally, or

— shut down, or

to which the SSP is assigned.

Required vendor documentation

CY09.03.01: The vendor provided documentation shall describe the association of an SSP which is generated, entered into or output from the module with the entity (i.e. person, group, role, or process).

Required test procedures

JY09.03.01: The tester shall verify that the association of an SSP which is generated, entered into or output from the module with the entity (i.e. person, group, role, or process) is consistent with the description in the documentation.

JY09.03.02: For each module that can be entered, the tester shall first enter the SSP while assuming the correct entity, the module shall be able to enter correctly. The tester shall then enter the SSP while assuming the incorrect entity, the module shall deny the entry.

JY09.03.03: For each module that can be output, the tester shall first output the SSP while assuming the correct entity, the module shall be able to output correctly. The tester shall then output the SSP while assuming the incorrect entity, the module shall deny the output.

AY09.04: (Security levels 1, 2, 3 and 4)

Hash values of passwords, RBG state information, and intermediate key generation values shall be considered as protected CSPs.

Required vendor documentation

CY09.04.01: The vendor provided documentation shall describe how to protect the hash values of passwords, RBG state information, and intermediate key generation values.

Required test procedures

JY09.04.01: The tester shall verify that the protection method described in the documentation is valid.

JY09.04.02: The tester shall attempt to obtain the hash values of passwords, RBG state information, and intermediate key generation values.

AY09.05: (Security levels 1, 2, 3 and 4)

The *{Sensitive Security Parameter Management}* documentation shall be compiled in accordance with the requirements specified in *{GM/T 0028-2014 Annex}* A.2.9.

module's boundary is defined as a CSP.

Required test procedures

JY09.07.01: The tester shall verify that the input data-stream generated from entropy collected from outside the cryptographic module's boundary is defined as a CSP.

AY09.08: (Security levels 1, 2, 3 and 4)

Whether the entropy is collected from inside or outside the cryptographic boundary, the minimum entropy value for any CSP shall be no less than 256 bits.

Required vendor documentation

CY09.08.01: Whether the entropy is collected from inside or outside the cryptographic boundary, the vendor documentation shall specify that the minimum entropy value for any CSP be no less than 256 bits.

Required test procedures

JY09.08.01: Whether the entropy is collected from inside or outside the cryptographic boundary, the tester shall verify that the minimum entropy value for any CSP is no less than 256 bits.

AY09.09: (Security levels 1, 2, 3 and 4)

If the entropy is collected from inside, it shall also describe the random bit generation principle.

Required vendor documentation

CY09.09.01: If the entropy is collected from inside, the vendor documentation shall describe the random bit generation principle.

Required test procedures

JY09.09.01: If the entropy is collected from inside, the tester shall verify that the random bit generation principle is described in the vendor documentation.

6.9.3 Sensitive security parameter generation

AY09.10: (Security levels 1, 2, 3 and 4)

Compromising the security of the SSP generation method which uses the output of an approved RBG (e.g. guessing the seed value to initialize the deterministic RBG) shall require at least as many operations as

CY09.18.01: If the module outputs any plaintext CSPs, the vendor documentation shall describe the output services.

CY09.18.02: The finite state model and other vendor documentation shall indicate, for the output of plaintext CSPs, that two independent internal actions that are required.

Required test procedures

JY09.18.01: The tester shall verify from the vendor documentation or finite state model that the module allows the output of plaintext CSPs.

JY09.18.02: The tester shall verify from the finite state model and other vendor documentation that the output of plaintext CSPs requires two independent internal actions.

JY09.18.03: The tester shall attempt to output plaintext CSPs without the module performing two independent internal actions. The module shall fail if the module allows such action.

AY09.19: (Security levels 1, 2, 3 and 4)

{In conjunction with AY09.18} **These two independent internal actions shall be dedicated to mediating the output of the CSPs.**

NOTE: This subclause is not tested separately. It is tested in AY09.18.

AY09.20: (Security levels 1, 2, 3 and 4)

For electronic entry or output via a wireless connection, CSPs, key components, and authentication data shall be encrypted.

Required vendor documentation

CY09.20.01: If the module inputs or outputs CSPs, key components, and authentication data via wireless interfaces, the vendor documentation shall describe the wireless services.

CY09.20.02: If the module inputs or outputs CSPs, key components, and authentication data via wireless interfaces, the vendor documentation shall describe the encryption methods employed to encrypt the CSPs, key components, and authentication data.

Required test procedures

JY09.20.01: The tester shall verify whether the module inputs or outputs CSPs, key components, and authentication data via wireless interfaces.

NOTE: This subclause is tested in AY09.01.

AY09.29: (Security levels 1, 2, 3 and 4)

Modification of PSPs by unauthorized operators shall be prohibited.

Required vendor documentation

CY09.29.01: The vendor shall provide documentation that modification of PSPs by unauthorized operators shall be prohibited.

Required test procedures

JY09.29.01: The tester shall verify that the vendor provides documentation that modification of PSPs by unauthorized operators shall be prohibited.

JY09.29.02: The tester shall assume an unauthorized role and attempt to modify PSPs stored within the module and verify that this attempt fails.

6.9.7 Sensitive security parameter zeroization

AY09.30: (Security levels 1, 2, 3 and 4)

A module shall provide methods to zeroize all unprotected SSPs and key components within the module.

NOTE: This subclause is tested in AY09.01.

AY09.31: (Security levels 1, 2, 3 and 4)

A zeroized SSP shall not be retrievable or reusable.

Required vendor documentation

CY09.31.01: The vendor documentation shall specify how to ensure that a zeroized SSP cannot be retrievable or reusable.

Required test procedures

JY09.31.01: The tester shall verify the accuracy of any rationale provided by the vendor. The burden of proof is on the vendor; if there is any uncertainty or ambiguity, the tester shall require the vendor to produce additional information as needed.

AY09.32: (Security levels 2, 3 and 4)

The cryptographic module shall perform the zeroization of unprotected SSPs (e.g. overwriting with all zeros or all ones or with random data).

verify that the module has returned to the factory state.

6.10 Self-tests

6.10.1 Self-test general requirements

AY10.01: (Security levels 1, 2, 3 and 4)

All self-tests shall be performed.

NOTE: This subclause is not tested separately.

AY10.02: (Security levels 1, 2, 3 and 4)

***{In conjunction with AY10.01}* and determination of pass or fail shall be made by the module, without external controls, externally provided input text vectors, expected output results, or operator intervention or whether the module will operate in an approved or non-approved mode.**

NOTE: This subclause is not tested separately.

AY10.03: (Security levels 1, 2, 3 and 4)

The pre-operational self-tests shall be performed and passed successfully prior to the module providing any data output (via the data output interface).

NOTE: This subclause is tested as part of AY10.14.

AY10.04: (Security levels 1, 2, 3 and 4)

Conditional self-tests shall be performed when an applicable security function or process is invoked.

NOTE: This subclause is tested as part of AY10.24.

AY10.05: (Security levels 1, 2, 3 and 4), AY10.06: (Security levels 1, 2, 3 and 4)

All self-tests identified in underlying cryptographic algorithms defined in *{GM/T 0028-2014}* Annex C, Annex D and Annex E shall be implemented as applicable within the cryptographic module.

NOTE: This subclause is tested as part of AY10.25.

AY10.06: (Security levels 1, 2, 3 and 4)

If a cryptographic module fails a self-test, the module shall enter an error state.

JY10.06.05: The tester shall verify by inspection and from the vendor documentation that determination of pass or fail of each self-test is made by the module, without external controls, externally provided input text vectors, expected output results, or operator intervention.

AY10.07: (Security levels 1, 2, 3 and 4)

***{In conjunction with AY10.06}* and shall output an error indicator as specified in *{GM/T 0028-2014}* 7.3.3.**

Required vendor documentation

CY10.07.01: The vendor shall document all error states associated with each self-test and shall indicate for each error state the expected error indicator.

Required test procedures

JY10.07.01: The tester shall verify the vendor documentation, check that it lists every error state that the module enters upon failure of a self-test, and indicates the error indicator associated with each error state. The tester shall compare the list of error states to those defined in the finite state model (SEE AY11.10) to verify that they agree.

JY10.07.02: By inspecting the vendor documentation that specifies how each self-test handles errors, the tester shall verify that:

— the module enters an error state upon failing a self-test;

— the error state is consistent with the documentation and the finite state model;

— the module outputs an error indicator;

— the error indicator is consistent with the documented error indicator.

JY10.07.03: The tester shall run each self-test and cause the module to enter every error state. The tester shall compare the observed error indicator with the indicator specified in the vendor documentation. If they are not the same, this test is failed.

AY10.08: (Security levels 1, 2, 3 and 4)

The cryptographic module shall not perform any cryptographic operations or output control and data via the control and data output interface while in an error state.

Required vendor documentation

AY10.20: (Security levels 1, 2, 3 and 4)

If a cryptographic module implements a bypass capability, the module shall ensure that the logic governing the bypass capability is correct.

Required vendor documentation

CY10.20.01: The vendor documentation shall specify how the cryptographic module ensures the correct logic governing the bypass capability.

Required test procedures

JY10.20.01: The tester shall verify from the vendor documentation and by inspection of the module that the logic governing activation of the bypass capability is implemented as specified.

JY10.20.02: The tester shall verify by inspection and from the vendor documentation that the pre-operational bypass test is implemented which exercises the logic governing activation of the bypass capability.

JY10.20.03: The tester shall cause each error condition of the pre-operational bypass test to occur and shall verify that the inhibition of output was performed under JY03.07.01 to JY03.07.05 and JY03.10.01 to JY03.10.05.

JY10.20.04: The tester shall run the pre-operational bypass test and shall verify that any functionality relies on the logic governing activation of the bypass capability cannot be utilized under JY10.10.01 and JY10.10.02.

AY10.21: (Security levels 1, 2, 3 and 4)

The module shall also verify the data path by

- **setting the bypass switch to an encrypted location, and verify that data transferred through the bypass mechanism is cryptographically processed, and**
- **setting the bypass switch to an unencrypted location, and verify that data transferred through the bypass mechanism is not cryptographically processed.**

Required vendor documentation

CY10.21.01: The vendor provided documentation shall describe the pre-operational bypass test.

CY10.21.02: The vendor documentation shall specify how to set the bypass switch to an encrypted location.

tested.

Required vendor documentation

CY10.23.01: The vendor shall provide documentation of all critical security functions. For each critical security function, the vendor shall indicate:

a) the purpose of the critical security function;
b) which critical security functions are tested by which pre-operational self-tests;
c) which critical security functions are tested by which conditional self-tests.

Required test procedures

JY10.23.01: The tester shall verify the vendor provided documentation of the critical security functions and the self-tests that are designed to test them. This documentation shall include the following:

a) identification and description of all critical security functions;
b) identification of at least one self-test for every critical security function.

JY10.23.02: By checking the code and / or design documentation, the tester shall verify that the module performs the specified self-tests for each critical security function.

6.10.3 Conditional self-tests

6.10.3.1 General requirements for conditional self-tests

AY10.24: (Security levels 1, 2, 3 and 4)

Conditional self-tests shall be performed by a cryptographic module when the conditions specified for the following tests *{AY10.26 to AY10.55}* occur: Cryptographic Algorithm Self-Test, Pair-Wise Consistency Test, Software / Firmware Load Test, Manual Entry Test, Bypass Test and Critical Functions Test.

Required vendor documentation

CY10.24.01: The vendor documentation shall provide the information on the conditional self-tests.

Required test procedures

JY10.24.01: The tester shall verify that the vendor documentation includes the information on conditional self-tests.

JY10.24.02: The tester shall verify that the conditional self-tests for the

CY10.27.02: The documentation shall show the transition into an error state and output of an error indicator when the two outputs are not equal.

Required test procedures

JY10.27.01: The tester shall verify that the vendor documentation is consistent with the implementation of the cryptographic module.

JY10.27.02: This is tested as specified in JY10.06.02, JY10.07.01, JY10.07.02, and JY10.07.03.

AY10.28: (Security levels 1, 2, 3 and 4)

An algorithm self-test shall at a minimum use the smallest approved key length, modulus size, prime, or curves as appropriate that is supported by the module.

Required vendor documentation

CY10.28.01: The vendor documentation shall provide the specification of each conditional cryptographic algorithm self-test that is implemented by the module.

Required test procedures

JY10.28.01: The tester shall verify by inspection and from the vendor documentation that each algorithm self-test implements, at a minimum, the smallest approved key length, modulus size, prime, or curves as appropriate that are supported by the module.

AY10.29: (Security levels 1, 2, 3 and 4)

If an algorithm specifies multiple modes (e.g. ECB, CBC, etc.), at a minimum, one mode shall be selected for the self-test that is supported by the module or as specified by the validation authority.

NOTE: This subclause is tested as part of AY10.28.

AY10.30: (Security levels 1, 2, 3 and 4)

***{Examples of known-answer tests}* One-way functions: Input test vector(s) generate output which shall be identical to expected output [e.g. hashing, keyed hashes, message authentication, RBG (fixed entropy vector), SSP agreement].**

NOTE: This subclause is tested as part of AY10.27.

AY10.31: (Security levels 1, 2, 3 and 4)

entry tests *{AY10.43 to AY10.46}* shall be performed.

NOTE: This subclause is not tested separately.

AY10.42: (Security levels 1, 2, 3 and 4), AY10.44: (Security levels 1, 2, 3 and 4)

The SSP or key components shall have an error detection code (EDC) applied, *{or shall meet AY10.43}*.

NOTE: This subclause is not tested separately.

AY10.43: (Security levels 1, 2, 3 and 4), AY10.44: (Security levels 1, 2, 3 and 4)

***{If AY10.43 is not satisfied, the SSP or key components}* shall be entered using duplicate entries.**

NOTE: This subclause is not tested separately.

AY10.44: (Security levels 1, 2, 3 and 4)

If an EDC is used, the EDC shall be at least 16 bits in length.

NOTE: This subclause is not tested separately.

AY10.45: (Security levels 1, 2, 3 and 4)

If the EDC cannot be verified, or the duplicate entries do not match, the test shall fail.

Required test procedures

JY10.45.01: The vendor shall document the manual entry test. Depending on whether error detection codes or duplicate entries of SSPs or key components are used, the manual entry test shall include the following:

a) error detection code (EDC):

— description of EDC calculation algorithm;

— description of verification process;

— expected outputs for success or failure of test.

b) duplicate key entries:

— description of verification process;

manual entry test, the test is failed.

c) The tester shall attempt to perform cryptographic operations with each entered SSP to verify that it was entered correctly.

d) The tester shall modify either the EDC associated with each manually entered SSP or the SSP itself and shall enter them into the module. The tester shall verify the indicator that is output from the status output interface; if no indicator is output, or the indicator does not match the documented indicator for the failure of the manual entry test, the test is failed.

e) The tester shall attempt to perform cryptographic operations with each SSP that was not successfully entered. Each operation using each SSP is required to fail, verifying that the SSP was not entered.

JY10.45.04: For manual entry tests using duplicate entries of SSPs or key components, the tester shall perform the following tests:

a) The tester shall enter each type of manually-entered SSP without any errors and shall verify the status output interface. If no indicator is output, or if the indicator does not match the documented indicator for the success of the manual entry test, the test is failed.

b) The tester shall attempt to perform cryptographic operations with each entered SSP to verify that it was entered correctly.

c) The tester shall modify one of the manually entered SSPs, either the first or second duplicate entry, and shall enter them into the module. The tester shall verify the indicator that is output from the status output interface; if no indicator is output, or the indicator does not match the documented indicator for the failure of the manual entry test, the test is failed.

d) The tester shall attempt to perform cryptographic operations with each SSP that was not successfully entered. Each operation using each SSP is required to fail, verifying that the SSP was not entered.

6.10.3.6 Conditional bypass test

AY10.46: (Security levels 1, 2, 3 and 4)

If a cryptographic module implements a bypass capability where the services may be provided without cryptographic processing (e.g. transferring plaintext through the module), the following suite of bypass tests *{AY10.48 to AY10.51}* shall be performed to ensure that a single point of failure of module components will not result in the unintentional output of plaintext.

NOTE: This subclause is tested as part of AY10.47 to AY10.50.

AY10.47: (Security levels 1, 2, 3 and 4)

A cryptographic module shall test for the correct operation of the services

All of the conditional self-tests have to be included.

Required test procedures

JY10.52.01: The tester shall inspect the vendor documentation to verify that initiation of pre-operational self-tests on demand is specified for all of the pre-operational self-tests.

JY10.52.02: The tester shall initiate the pre-operational self-tests on demand to verify that the initiation of the pre-operational self-tests on demand is consistent with the vendor documentation.

JY10.52.03: The tester shall initiate the conditional self-tests on demand to verify that the initiation of the conditional self-tests on demand is consistent with the vendor documentation.

AY10.53: (Security levels 3 and 4)

The module shall repeatedly, upon a defined time period automatically, without external input or control, perform the pre-operational or conditional self-tests.

Required vendor documentation

CY10.53.01: The vendor shall provide documentation that specifies how the pre-operational and conditional self-tests are repeatedly performed upon a defined time, automatically, without external input or control.

CY10.53.02: The vendor documentation shall include the specification on the status indicator used to indicate that the cryptographic module's operations are interrupted due to the pre-operational or conditional self-tests.

CY10.53.03: The vendor provided non-proprietary security policy shall provide the information on the defined time period and any conditions that result in the interruption of the module's operation during the time to repeat pre-operational or conditional self-tests.

Required test procedures

JY10.53.01: The tester shall verify, by inspection of the cryptographic module, that the pre-operational and conditional self-tests are repeatedly performed as specified in CY10.53.01, and CY10.53.02.

AY10.54: (Security levels 3 and 4)

The time period and any conditions that may result in the interruption of the module's operations during the time to repeat the pre-operational or conditional self-tests shall be specified in the security policy (*{GM/T 0028-*

— maintenance role (if a maintenance access interface is provided);

— SSP generation and establishment services (if applicable);

— SSP output services (if applicable);

— idle states (if applicable);

— uninitialized states (if applicable).

JY11.08.03: The tester shall verify that each distinct cryptographic module service, security function use, error state, self-test, or operator authentication is depicted as a separate state.

JY11.08.04: The tester shall verify that every state that is identified in the finite state diagram is also identified and described in the description of the finite state model.

JY11.08.05: The tester shall verify that every state that is identified and described in the finite state model is also identified in the finite state diagram(s).

JY11.08.06: The tester shall verify that the operation of the module is consistent with the finite state diagram(s) and the descriptions.

JY11.08.07: If the module includes a maintenance access interface, the tester shall verify that the finite state model has at least one maintenance state defined. All maintenance states have to be contained in the finite state diagram(s) and described in the description of the finite state model.

JY11.08.08: The tester shall verify the descriptions of the states of the cryptographic module if the descriptions clearly define disjoint states. The tester shall verify that all possible combinations of data and control inputs can be partitioned into disjoint sets.

JY11.08.09: The tester shall exercise the cryptographic module, causing it to enter each of its major states. For each state that has a distinct indicator, the tester shall attempt to verify the indicator while the module is in the state. If the expected indicator is not observed, or two or more such indicators are observed at the same time (indicating that the module is in more than one state at one time), this test is failed.

JY11.08.10: The tester shall verify that there exists a chain of transitions from an initial power on state to each other state in the model (that is not an initial power on state).

JY11.08.11: The tester shall verify that there exists a chain of transitions from each non-power off state to a power off state of the model.

AY11.16: (Security levels 1, 2, 3 and 4)

If a cryptographic module contains software or firmware, the source codes shall be annotated with comments that depict the correspondence of the software or firmware to the design of the module.

Required vendor documentation

CY11.16.01: The vendor shall supply a list of the names of all the software and firmware components contained in the cryptographic module.

CY11.16.02: The vendor shall supply an annotated source listing of each software and firmware component contained in the cryptographic module.

Required test procedures

JY11.16.01: The tester shall use the list supplied by the vendor to verify that a source listing for each software or firmware component is contained in the cryptographic module.

JY11.16.02: The tester shall verify that the source codes are annotated with comments that depict the correspondence of the software or firmware to the design of the module.

AY11.17: (Security levels 1, 2, 3 and 4)

If a cryptographic module contains hardware, documentation shall specify the schematics and / or Hardware Description Language (HDL), as applicable.

Required vendor documentation

CY11.17.01: The vendor shall supply a list of the hardware components contained in the cryptographic module.

Required test procedures

JY11.17.01: The tester shall use the list supplied by the vendor to verify that the documentation includes schematics and / or Hardware Description Language (HDL) listings for the hardware components.

AY11.18: (Security levels 1, 2, 3 and 4)

If a cryptographic module contains hardware, the HDL shall be annotated with comments that depict the correspondence of the hardware to the design of the module.

Required vendor documentation

{For software and firmware cryptographic modules and the software or firmware component of a hybrid module} **the cryptographic module shall be developed using industry-grade development tools (e.g. compilers).**

Required vendor documentation

CY11.21.01: The vendor shall provide documentation that the cryptographic module shall be developed using industry-grade development tools (e.g. compilers).

Required test procedures

JY11.21.01: The tester shall verify that the vendor provides documentation that the module meets the cryptographic module shall be developed using industry-grade development tools (e.g. compilers).

AY11.22: (Security levels 2, 3 and 4)

The following requirements *{AY11.23 to AY11.26}* shall apply to cryptographic modules for Security Levels 2 and 3.

NOTE: This subclause is tested as part of AY11.23 to AY11.26.

AY11.23: (Security levels 2, 3 and 4)

All software or firmware within a cryptographic module shall be implemented using a high-level, non-proprietary language *{or satisfying the requirements of AY011.24}*.

Required vendor documentation

CY11.23.01: The vendor shall provide documentation that all software or firmware within a cryptographic module is implemented using a high-level, non-proprietary language.

Required test procedures

JY11.23.01: The tester shall verify that the vendor provides documentation that all software or firmware within a cryptographic module is implemented using a high-level, non-proprietary language.

AY11.24: (Security levels 2, 3 and 4)

{In case of not satisfying the requirements of AY011.23} **rationale shall be provided for the use of a low-level language (e.g. assembly language or microcode) if essential to the performance of the module or when a high-level language is not available.**

cryptographic module.

6.11.9 Guidance documents

AY11.38: (Security levels 1, 2, 3 and 4)

Administrator guidance shall specify:

- **the administrative functions, security events, security parameters (and parameter values, as appropriate), physical ports, and logical interfaces of the cryptographic module available to the Crypto Officer and / or other administrative roles;**
- **procedures required to keep operator authentication data and mechanisms functionally independent;**
- **procedures on how to administer the cryptographic module in an approved mode of operation;**
- **assumptions regarding User behavior that are relevant to the secure operation of the cryptographic module.**

Required vendor documentation

CY11.38.01: The vendor shall provide documentation that includes the information list in AY11.38.

CY11.38.02: The non-proprietary guidance shall be available to the appropriate administrators of the module.

Required test procedures

JY11.38.01: The tester shall verify that the vendor provides documentation that includes the information list in AY11.38.

AY11.39: (Security levels 1, 2, 3 and 4)

Non-administrator guidance shall specify:

- **the approved and non-approved security functions, physical ports, and logical interfaces available to the users of a cryptographic module;**
- **all User responsibilities necessary for the approved mode of operation of a cryptographic module.**

Required vendor documentation

CY11.39.01: The vendor shall provide documentation that includes the information list in AY11.39.

NOTE: This subclause is tested as part of AY12.04.

AY12.04: (Security level 4)

If the mitigation of specific attacks not defined elsewhere in this Standard is claimed, documentation shall specify the methods used to mitigate the attacks and the methods to test the effectiveness of mitigation techniques.

Required vendor documentation

CY12.04.01: The vendor shall specify in the documentation the methods used to mitigate the attack(s).

CY12.04.02: The vendor shall specify in the documentation the test methods used to test the effectiveness of the mitigation techniques.

CY12.04.03: The vendor shall specify in the documentation the effectiveness of the mitigation techniques.

Required test procedures

JY12.04.01: The tester shall verify that the vendor provides documentation that specifies the methods used to mitigate the attack(s).

JY12.04.02: The tester shall verify that the vendor provides documentation that specifies the test methods used to test the effectiveness of the mitigation techniques.

JY12.04.03: The tester shall verify that the vendor provides documentation that specifies the effectiveness of the mitigation techniques.

6.13 A - Documentation requirements

NOTE: GM/T 0028-2014, Annex A specifies the minimum documentation requirements of a cryptographic module.

AYA.01: (Security levels 1, 2, 3 and 4)

This Annex *{GM/T 0028-2014 Annex A}* specifies the minimum documentation which shall be required for a cryptographic module. The cryptographic module to be tested shall meet the requirements of the following documentations.

Required vendor documentation

CYA.01.01: The vendor shall provide documentation for a cryptographic module that fulfils but is not limited to the minimum documentation requirements as specified in GM/T 0028-2014, A.2.1 to A.2.12.

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

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