GA

ICS 35.040

A 90

Public Security Industry Standard

of the People's Republic of China

GA/T 671-2006

Information security technology – Technology requirement for terminal computer system of security classified protection

信息安全技术

终端计算机系统安全等级技术要求

Issued on: December 28, 2006 **Implemented on: February 1, 2007**

Issued by: The Ministry of Public Security of the People's Republic of China.

Table of Contents

Information security technology – Technology requirement for terminal computer system of security classified protection

1 Scope

This Standard specifies the security technology requirements needed for the security classified protection of terminal computer system, and makes different technology requirements for each security protection level.

This Standard applies to the design and realization of terminal computer system conducted according to the requirements for security protection level specified in the GB 17859-1999, and also provides a reference for the testing and management of terminal computer system conducted according to the requirements specified in the GB 17859-1999.

2 Normative references

The provisions in the following documents become the provisions of this Standard through reference in this Standard. For dated references, the subsequent amendments (excluding corrections) or revisions do not apply to this Standard. However, parties who reach an agreement based on this Standard are encouraged to study if the latest versions of these documents are applicable. For undated references, the latest versions apply to this Standard.

GB/T 17859-1999 *Classified criteria for security protection of computer information system*

GB/T 20271-2006 *Information security technology – Common security techniques requirement for information system*

GB/T 20272-2006 *Information security technology – Security techniques requirement for operating system*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

The terms and definitions established in the GB 17859-1999, GB/T 20271-2006 and GB/T 20272-2006 AND the following ones apply to this Standard.

equipment protection against theft and destruction of the terminal computer system is divided into:

a) Equipment identification requirements: The equipment of the terminal computer system shall have obvious and non-removable identifications, so as to prevent the replacement and to facilitate the searching;

b) Host physical security: The host of the terminal computer system shall have case encapsulation protection, so as to prevent the system damage caused by dropping and vibration;

c) Requirements for equipment protection against theft and self-destruction: The equipment of the terminal computer system shall provide owners with controllable anti-theft alarm and system self-destruction functions.

4.1.3 High reliability of equipment

According to the application requirements of special environments, the equipment's high reliability of the terminal computer system is divided into:

a) Waterproof requirement: The terminal computer system shall have high sealing property, so as to prevent water drops from entering;

b) Anti-dropping and anti-vibration requirements: The terminal computer system shall have reinforced protection, so as to prevent the system damage caused by dropping and vibration;

c) Requirements for the resistance to high and low temperature and pressure: The terminal computer system shall be able to adapt the environments with high and low temperature and pressure;

d) Resistance to electromagnetic radiation and interference: The terminal computer system shall be able to resist the system security threats caused by electromagnetic interference and radiation.

4.2 Operational security

4.2.1 System security detection and analysis

According to the different requirements of different security levels, the security detection and analysis of the terminal computer system is divided into:

a) Security detection and analysis of the operating system: ASSESS the file permission, file host, network service settings, account settings, program authenticity, and general user-related security points and intrusion signs as an administrator from the aspect of terminal computer operating system, so as to detect and analyze the security of the operating system, to discover the

existing potential security hazards, and to put forward the remedial measures.

b) Security detection and analysis of the hardware system: CONDUCT the security detection to the hardware system supporting the terminal computer system operation. SCAN the specific security vulnerability related to the system operation and data protection in the hardware system, so as to analyze the existing defects and loopholes, and to put forward the remedial measures.

c) Security detection and analysis of applications: CONDUCT the security detection and analysis to the applications operating in the terminal computer system. SCAN the specific security vulnerability related to the identification, authorization, access control, and system integrity in the applications, so as to analyze the existing defects and loopholes, and to put forward the remedial measures.

d) Detection and analysis of the electromagnetic leakage and emission: CONDUCT the detection of the electromagnetic leakage and emission to the environment of the operating terminal computer system. USE a special detection device to check the threats to the security of the terminal computer system caused by electromagnetic interference and radiation in the process of system operation. PUT forward the remedial measures.

4.2.2 Security audit

4.2.2.1 Response of security audit

According to the different requirements of different security levels, the security audit of the terminal computer system is divided into:

a) KEEP audit log: When detecting possible security violation event(s), WRITE the audit data into the audit log;

b) GENERATE real-time alarm: When detecting possible security violation event(s), GENERATE the real-time alarm information;

c) Unauthorized process termination: When detecting possible security violation event(s), TERMINATE the unauthorized process. The unauthorized process includes but not limited to the service process, drive process, and user process;

d) User account disconnection and failure: When detecting possible security violation event(s), DISCONNECT and DISABLE the current user account.

4.2.2.2 Security audit data generation

According to the different requirements of different security levels, the security

4.2.4 Protection during operation

4.2.4.1 Malicious code protection

Malicious codes refer to the program codes causing damages or impacts, and generating when users operate the terminal computer system, such as viruses, worms, Trojan horse, malicious software, etc.

According to the different requirements of different security levels, the malicious code protection of the terminal computer system shall be divided into:

a) Usage control of foreign media: Strictly CONTROL the usage of various foreign media, so as to prevent the malicious codes from transmitting via the media.

b) Signature scanning: CONDUCT signature scanning to the file system and memory. TAKE corresponding measures according to the scanning results to eliminate or isolate the malicious codes. UPDATE the feature library of malicious codes in time.

c) CPU-based data execution prevention: PREVENT buffer overflow, and the execution of malicious codes from protected memory locations.

d) Process isolation: USE the logical isolation or physical isolation method of processes to protect processes from being damaged by the malicious codes.

e) Process behavior analysis: CONDUCT grade assessment to the risk degree of process behaviors based on the expert system. TAKE corresponding protective measures according to the assessment results.

4.2.4.2 Network attack protection

The terminal computer system shall take necessary measures to monitor the data communication between host and external network, so as to ensure to protect the system from the external network violation or malicious remote control. The measures that shall be taken include:

a) Firewall functions:

– IP packet filtering: It shall be able to support the access control based on source and destination addresses, and to discard the data packets failing to conform to the preset policy;

– Network protocol analysis: It shall be able to support the access control based on network protocol type;

– Application monitoring: It shall be able to set the network access control rules of applications, including the control of ports, protocols, and access

c) Single-use discrimination: It shall be able to provide the discrimination mechanism for single-use discrimination data operation, which indicates that SSF shall prevent the discrimination data reusing related to the identified discrimination mechanism.

d) Multi-mechanism discrimination: It shall be able to provide different discrimination mechanisms, so as to discriminate the user identification of specific event. Furthermore, SSF shall discriminate the identities claimed by any users according to the described rule on the way for various discrimination mechanisms to provide discrimination.

e) Re-discrimination: It shall be able to stipulate the events requiring user re-discrimination, which indicates that SSF shall re-discriminate the users under the conditions indicated in the condition table requiring re-discrimination. For instance, after the user is disconnected from the network due to the operation timed out, it is necessary to perform re-discrimination during the reconnection.

4.3.2.5 User discrimination failure processing

SFF is requested to define a value for the unsuccessful discrimination attempts (including attempts and time threshold), and to clearly stipulate the actions that shall be taken when coming up to this value. The discrimination failure processing shall include the detected situation that relevant unsuccessful discrimination attempts are the same with the stipulated number, and the predefined processing. PREDEFINE the value for the unsuccessful discrimination attempts (including attempts and time threshold), and clearly STIPULATE the actions that shall be taken when coming up to this value, so as to realize the discrimination failure processing.

4.3.2.6 User-subject binding

Within the SSC, for an identified and discriminated user, it is necessary to activate another subject (such as process) to request SSF to accomplish some task. At this time, it is requested to associate this user with this subject via the user-subject binding, and thus to associate the user identity with all the auditable actions of this user.

4.3.2.7 Secrecy

a) Anonymity: The users do not expose their identities when using resources or services. SSF is requested to ensure that the user and/or subject set cannot determine the actual users related to the subjects and/or operations, and ensure not to ask actual usernames when providing services for the subjects.

b) Pseudonym: The users do not expose their actual names when using resources or equipment. However, they shall still be able to take

– REJECT the subject access to the objects on the basis of the rules of rejecting the subjects to access the objects based on the security properties.

4.3.3.3 Access control range

According to the different requirements of different security levels, the coverage of the discretionary access control is divided into:

a) Subset access control: SSF, each determined discretionary access control, is requested to cover the subject, object and the operations between them defined by the SSOTCS.

b) Full access control: SSF, each determined discretionary access control, is requested to cover all the subjects, objects, and the operations among them in the terminal computer system, that is to say, SSF shall ensure that all the operations between any subject and any object in the SSC shall be at least covered by one determined access control policy.

4.3.3.4 Access control granularity

According to the different requirements of different security levels, the granularity of the discretionary access control is divided into:

a) The subjects are in the user group/at user level, while the objects are at file level;

b) The subjects are at user level, while the objects are at file level.

4.3.4 Marks

4.3.4.1 Subject marks

The subjects refer to active entities, which are the entities in the SSC initiating operations. The subjects generally include people, processes, external equipment, etc.

ALLOCATE marks for the subjects. These marks are the combination of grade category and non-grade category, and the basis of implementing the mandatory access control.

4.3.4.2 Object marks

The objects refer to passive entities, which are the entities in the SSC accessed by the subjects. The objects include or receive the information concerned by the subjects. The objects generally include files, equipment, status information, etc.

DESIGNATE sensitive marks for the objects. These sensitive marks are the

combination of grade category and non-grade category, and the basis of implementing the mandatory access control.

4.3.5 Mandatory access control

4.3.5.1 Access control policy

The mandatory access control policy shall include the subjects and objects under policy control, and the policy-covered operations between the controlled subject and object. It is allowed to have multiple access control security policies. However, they shall be named independently without conflicting with each other.

4.3.5.2 Access control function

Clearly POINT out the specific functions realized by using one named mandatory access control policy. It shall be able to provide:

– IMPLEMENT the access control policy on the objects in the mark or named mark group;

– DECIDE to allow the controlled subject to implement controlled operations to the controlled object according to the access allowing rule between controlled subject and controlled object;

– DECIDE to refuse the controlled subject to implement controlled operations to the controlled object according to the access refusing rule between controlled subject and controlled object.

4.3.5.3 Access control range

According to the different requirements of different security levels, the coverage of the mandatory access control is divided into:

a) Subset access control: Each determined mandatory access control is requested to cover the subject, object and the operations between them defined by the policy.

b) Full access control: Each determined mandatory access control is requested to cover all the subjects, objects, and the operations among them in the terminal computer system, which is to request that all the operations between any subject and any object in the terminal computer system shall be at least covered by one determined access control policy.

4.3.5.4 Access control granularity

According to the different requirements of different security levels, the granularity of the mandatory access control is divided into:

5.1.1.1.1 Equipment security availability

DESIGN and REALIZE the function of equipment security availability of the terminal computer system according to the requirements for basic operational support specified in the Section 4.1.1 of this Standard.

5.1.1.1.2 Equipment protection against theft and destruction

DESIGN and REALIZE the function of equipment protection against theft and destruction of the terminal computer system according to the requirements for equipment identifications specified in the Section 4.1.2 of this Standard.

5.1.1.2 Operating system

According to the requirements specified in the Section 4.1.1 of the GB/T 20272-2006, DESIGN, REALIZE or PURCHASE the operating system required for the terminal computer system at user discretionary protection level from the following aspects:

a) User identification and discrimination: According to the descriptions given in the Section 4.1.1.1 of the GB/T 20272-2006, REALIZE the user identification, user discrimination, user discrimination failure processing, and user-subject binding of the operating system.

b) Discretionary access control: According to the descriptions given in the Section 4.1.1.2 of the GB/T 20272-2006, CONDUCT access control to the operating system, ALLOW legal operations, and FORBID illegal operations.

c) User data integrity: According to the descriptions given in the Section 4.1.1.7 of the GB/T 20272-2006, PROVIDE the function of ensuring the user data integrity to the user data stored, processed and transmitted in the operating system.

5.1.1.3 Trusted computing platform

5.1.1.3.1 Password support

DESIGN and REALIZE the function of password support of the terminal computer system at discretionary protection level according to the descriptions given in the Section 4.3.1 of this Standard and the following requirements.

a) USE the cryptographic algorithm approved by relevant competent government departments and the software to realize relevant cryptographic algorithms and operations;

b) Key management: All the keys shall be protected by the root of trust for storage.

Section 6.1.3.1 of the GB/T 20271-2006, REALIZE the functions of user identification, user discrimination, user discrimination failure processing, and user-subject binding.

b) Discretionary access control: According to the descriptions given in the Section 6.1.3.2 of the GB/T 20271-2006, CONDUCT access control to the relevant resources of the application system, ALLOW legal operations, and FORBID illegal operations.

c) Data integrity protection: According to the descriptions given in the Section 6.1.3.3 of the GB/T 20271-2006, PROVIDE the function of ensuring the user data integrity to the user data stored, processed and transmitted in the application system.

5.1.2 Security assurance requirements

5.1.2.1 SSOTCS security protection

a) Trusted root security protection: REALIZE the trusted root of the terminal computer system according to the following requirements:

– PROTECT the root of trust for storage from being disclosed and tampered;

– TAKE physical protection measures for the root of trust for measurement.

b) SSF physical security protection: REALIZE the SSF physical security protection at user discretionary protection level of the terminal computer system according to the requirements specified in the Section 6.1.4.1 of the GB/T 20271-2006.

c) SSF operational security protection: REALIZE the SSF operational security protection at user discretionary protection level of the terminal computer system according to the requirements specified in the Section 6.1.4.2 of the GB/T 20271-2006.

d) SSF data security protection: REALIZE the SSF data security protection at user discretionary protection level of the terminal computer system according to the requirements specified in the Section 6.1.4.3 of the GB/T 20271-2006.

e) Resource utilization: REALIZE the resource utilization at user discretionary protection level of the terminal computer system according to the requirements specified in the Section 6.1.4.4 of the GB/T 20271-2006.

f) SSOTCS access control: REALIZE the SSOTCS access control at user discretionary protection level of the terminal computer system according to the requirements specified in the Section 6.1.4.5 of the GB/T 20271-2006.

5.1.2.2 SSOTCS design and realization

Standard, and the password support configured in the Section 4.3.1 of this Standard, TAKE transmission encryption measures for the data requiring transmission privacy protection, DESIGN and REALIZE the function of data transmission privacy protection.

5.2.1.3.9 Data integrity protection

According to the descriptions given in the Section 4.3.7 of this Standard, PROVIDE the function of ensuring the data integrity for the data stored, processed and transmitted in the trusted computing platform.

5.2.1.3.10 Security audit

According to the descriptions given in the Section 4.2.2 of this Standard, and the requirements specified in the Section 6.2.2.3 of the GB/T 20271-2006, DESIGN and REALIZE the function of security audit of the trusted computing platform:

a) The design of the security audit function shall be closely combined with the design of security functions, such as password support, identification and discrimination, discretionary access control, data privacy protection, user data integrity, trust service, etc.

b) SUPPORT audit log, generation of security audit events, potential invasion analysis, and basic audit review; PROVIDE audit event selection and protected audit trail storage.

c) It shall be able to generate, maintain and protect the audit processes, and to protect them from modification, illegal access and corruption. PROTECT the audit data especially. Strictly RESTRICT the unauthorized user access.

d) It shall be able to create and maintain an audit trail to the protected object access. PROTECT the audit records from unauthorized access, modification and corruption.

5.2.1.3.11 Backup and fault recovery

DESIGN and REALIZE the function of backup and recovery of the terminal computer system according to the requirements for the backup and recovery of user data, incremental information and local system specified in the Section 4.2.5 of this Standard.

5.2.1.3.12 I/O interface configuration

DESIGN and REALIZE the function of I/O interface configuration according to the requirements for the user discretionary configuration specified in the Section 4.2.7 of this Standard.

Section 4.3.1.2 of the GB/T 20272-2006, CONDUCT access control to the operating system, ALLOW legal operations, and FORBID illegal operations.

c) Marks: According to the descriptions given in the Section 4.3.1.3 of the GB/T 20272-2006, DESIGN and REALIZE the marking function of the operating system, so as to set the sensitive marks required for the subject and object.

d) Mandatory access control: According to the descriptions given in the Section 4.3.1.4 of the GB/T 20272-2006, CONDUCT access control to the operating system, ALLOW legal operations, and FORBID illegal operations. REALIZE the function of mandatory access control to the operating system, including the system files, services, drive, registries and processes.

e) Data flow control: For the operating system using data flow to realize the data exchange, according to the descriptions given in the Section 4.3.1.5 of the GB/T 20272-2006, DESIGN and REALIZE the function of data flow control of the operating system.

f) Security audit: According to the descriptions given in the Section 4.3.1.6 of the GB/T 20272-2006, PROVIDE the security audit function for the operating system.

g) User data privacy: According to the descriptions given in the Section 4.3.1.8 of the GB/T 20272-2006, DESIGN and REALIZE the function of user data privacy protection of the operating system.

h) User data integrity: According to the descriptions given in the Section 4.3.1.7 of the GB/T 20272-2006, PROVIDE the function of ensuring the user data integrity to the user data stored, processed and transmitted in the operating system.

5.3.1.3 Trusted computing platform

5.3.1.3.1 Password support

DESIGN and REALIZE the function of password support of the terminal computer system at security marking level according to the descriptions given in the Section 4.3.1 of this Standard and the following requirements:

a) Cryptographic algorithm: USE the cryptographic algorithm approved by the national cryptography administrative department. USE hardware to realize the cryptographic algorithms.

b) Cryptographic operation: The key generation, digital signature and verification, and other critical cryptographic operations shall base on the cryptographic hardware support.

as the detection and analysis of electromagnetic leakage and emission specified in the Section 4.2.1 of this Standard, USE relevant tools to detect the security and electromagnetic leakage of the selected or developed operating system, hardware system and applications. Furthermore, IMPROVE the existing security problems by analyzing the detection results according to the requirements of the security marking protection level.

5.3.1.3.5 Trust service

DESIGN and REALIZE the function of trust service at security marking protection level of the trusted computing platform according to the descriptions given in the Section 4.3.8 of this Standard and the following requirements:

a) Specially SET a protected area in the trusted hardware modules, so as to store the integrity metrics of all the static trusted chains;

b) SET a protected area in the trusted hardware modules, so as to store the integrity metrics of all the dynamic trusted chains;

c) REPORT the integrity metrics of the operating system to national specialized agencies when necessary.

5.3.1.3.6 Identification and discrimination

5.3.1.3.6.1 System identification and discrimination

According to the requirements specified in the Section 4.3.2 of this Standard, REALIZE the function of system identification and discrimination from the following aspects:

a) According to the requirements specified in the Section 4.3.2.1 of this Standard, DESIGN and REALIZE the functions of unique identification, identification credibility and secrecy, and identification information management of the terminal computer system, so as to ensure the identity uniqueness and authenticity of the trusted computing platform in the terminal computer system.

b) According to the requirements specified in the Section 4.3.2.2 of this Standard, DESIGN and REALIZE the function of system identity discrimination.

5.3.1.3.6.2 User identification and discrimination

According to the requirements specified in the Section 4.3.2 of this Standard, DESIGN and REALIZE the function of user identification and discrimination from the following aspects:

a) According to the requirements specified in the Section 4.3.2.3 of this

b) According to the requirements specified in the Section 4.3.4.2 of this Standard, DESIGN and REALIZE the function of object marks.

5.3.1.3.9 Mandatory access control

According to the requirements for mandatory access control specified in the Section 4.3.5 of this Standard, DESIGN and REALIZE the function of mandatory access control of the trusted computing platform from the following aspects:

a) According to the requirements specified in the Section 4.3.5.1 of this Standard, DETERMINE the mandatory access control policy;

b) According to the requirements specified in the Section 4.3.5.2 of this Standard, DESIGN and REALIZE the function of mandatory access control;

c) According to the requirements for subset access control specified in the Section 4.3.5.3 of this Standard, DETERMINE the range of mandatory access control;

d) According to the requirements for access control granularity specified in the Section 4.3.5.4 of this Standard, DETERMINE the granularity of mandatory access control.

5.3.1.3.10 Data privacy protection

According to the requirements specified in the Section 4.3.6 of this Standard, DESIGN and REALIZE the function of data privacy protection of the trusted computing platform from the following aspects:

a) According to the requirements for data encryption, data binding, and data sealing specified in the Section 4.3.6.1 of this Standard, and the password support configured in the Section 4.3.1 of this Standard, TAKE storage encryption measures for the data requiring storage privacy protection, DESIGN and REALIZE the function of data storage privacy protection;

b) According to the requirements specified in the Section 4.3.6.2 of this Standard, and the password support configured in the Section 4.3.1 of this Standard, TAKE transmission encryption measures for the data requiring transmission privacy protection, DESIGN and REALIZE the function of data transmission privacy protection;

c) According to the requirements for subset information protection specified in the Section 4.3.6.3 of this Standard, DESIGN and REALIZE the function of object security reuse.

5.3.1.3.11 Data integrity protection

application system.

5.3.2 Security assurance requirements

5.3.2.1 SSOTCS security protection

a) Trusted root security protection: REALIZE the trusted root of the terminal computer system according to the following requirements:

– SET the root of trust for storage and the root of trust for reporting in the trusted hardware modules;

– The trusted hardware modules shall pass the evaluation and certification of national specialized agencies;

– TAKE physical protection measures for the root of trust for measurement.

b) SSF physical security protection: REALIZE the SSF physical security protection at security marking protection level of the terminal computer system according to the following requirements:

– REALIZE the SSF physical security protection at security marking protection level of the terminal computer system according to the requirements specified in the Section 6.3.4.1 of the GB/T 20271-2006;

– TAKE appropriate hardware protection measures to prevent the cryptographic computation modules in the trusted hardware modules from energy attack.

c) SSF operational security protection: REALIZE the SSF operational security protection at security marking protection level of the terminal computer system according to the following requirements:

– REALIZE the SSF operational security protection at security marking protection level of the terminal computer system according to the requirements specified in the Section 6.3.4.2 of the GB/T 20271-2006;

– TAKE appropriate power failure protection measures, so as to ensure that the terminal computer system can recover to the configurations before exiting the operating mode after exiting the sleeping or standby mode, and to ensure that the trusted chain system can still function properly.

d) SSF data security protection: REALIZE the SSF data security protection at security marking protection level of the terminal computer system according to the requirements specified in the Section 6.3.4.3 of the GB/T 20271-2006.

e) Resource utilization: REALIZE the resource utilization at security marking protection level of the terminal computer system according to the

the operating system.

g) User data privacy: According to the descriptions given in the Section 4.4.1.8 of the GB/T 20272-2006, DESIGN and REALIZE the function of user data privacy protection of the operating system.

h) User data integrity: According to the descriptions given in the Section 4.4.1.7 of the GB/T 20272-2006, PROVIDE the function of ensuring the user data integrity to the user data stored, processed and transmitted in the operating system.

i) Trusted paths: According to the descriptions given in the Section 4.4.1.9 of the GB/T 20272-2006, ESTABLISH a safe data transmission path when the users conduct initial login and/or discrimination.

5.4.1.3 Trusted computing platform

5.4.1.3.1 Password support

DESIGN and REALIZE the function of password support of the terminal computer system at access verification protection level according to the descriptions given in the Section 4.3.1 of this Standard and the following requirements:

a) Cryptographic algorithm: USE the cryptographic algorithm approved by the national cryptography administrative department. USE hardware to realize the symmetric cipher algorithm, public-key cryptographic algorithm, hash algorithm, and random number generation algorithm.

b) Cryptographic operation: All the cryptographic operations shall base on the support of trusted hardware modules and other cryptographic hardware modules.

c) Key management: All the keys shall be protected by the root of trust for storage. The root of trust for storage shall be protected by the security hardware.

5.4.1.3.2 Trusted chains

DESIGN and REALIZE the function of trusted chains of the terminal computer system according to the descriptions given in the Section 4.2.3 of this Standard and the following requirements.

a) REALIZE the establishment of static and dynamic trusted chains based on the trusted hardware modules;

b) The criteria of integrity measurement of the operating system (OS) in the static trusted chains shall be managed by national specialized agencies, and

c) According to the requirements specified in the Section 4.3.2.4 of this Standard, SUPPORT to provide the discrimination information in the form of digital certificate, IC cards, fingerprints, iris, etc.;

d) According to the requirements specified in the Section 4.3.2.5 of this Standard, DESIGN and REALIZE the function of user discrimination failure processing;

e) According to the requirements specified in the Section 4.3.2.6 of this Standard, DESIGN and REALIZE the function of user-subject binding;

f) According to the requirements specified in the Section 4.3.2.4 of this Standard, ESTABLISH the communication paths of the discrimination equipment and trusted hardware modules for the discrimination information in the form of IC cards, fingerprints, iris, etc., so as to ensure that the trusted hardware modules can obtain the original identity discrimination information without being tampered and disclosed.

g) According to the requirements specified in the Section 4.3.2.7 of this Standard, DESIGN and REALIZE the secrecy functions of anonymity and non-association.

5.4.1.3.7 Discretionary access control

According to the requirements for discretionary access control specified in the Section 4.3.3 of this Standard, DESIGN and REALIZE the function of discretionary access control of the trusted computing platform from the following aspects:

a) According to the requirements specified in the Section 4.3.3.1 of this Standard, DETERMINE the discretionary access control policy;

b) According to the requirements specified in the Section 4.3.3.2 of this Standard, DESIGN and REALIZE the function of discretionary access control;

c) According to the requirements for full access control specified in the Section 4.3.3.3 of this Standard, DETERMINE the range of discretionary access control;

d) According to the requirements for access control granularity specified in the Section 4.3.3.4 of this Standard, DETERMINE the granularity of discretionary access control.

5.4.1.3.8 Marks

According to the marking requirements specified in the Section 4.3.4 of this

– REALIZE the SSF physical security protection at structured protection level of the terminal computer system according to the requirements specified in the Section 6.4.4.1 of the GB/T 20271-2006;

– TAKE appropriate hardware protection measures to prevent the cryptographic computation modules in the trusted hardware modules from energy attack.

d) SSF operational security protection: REALIZE the SSF operational security protection at structured protection level of the terminal computer system according to the following requirements:

– REALIZE the SSF operational security protection at structured protection level of the terminal computer system according to the requirements specified in the Section 6.4.4.2 of the GB/T 20271-2006;

– TAKE appropriate power failure protection measures, so as to ensure that the terminal computer system can recover to the configurations before exiting the operating mode after exiting the sleeping or standby mode, and to ensure that the trusted chain system can still function properly.

e) SSF data security protection: REALIZE the SSF data security protection at structured protection level of the terminal computer system according to the requirements specified in the Section 6.4.4.3 of the GB/T 20271-2006.

f) Resource utilization: REALIZE the resource utilization at structured protection level of the terminal computer system according to the requirements specified in the Section 6.4.4.4 of the GB/T 20271-2006.

g) SSOTCS access control: REALIZE the SSOTCS access control at structured protection level of the terminal computer system according to the requirements specified in the Section 6.4.4.5 of the GB/T 20271-2006.

5.4.2.2 SSOTCS design and realization

a) Configuration management: REALIZE the configuration management at structured protection level of the terminal computer system according to the requirements specified in the Section 6.4.5.1 of the GB/T 20271-2006.

b) Distribution and operation: REALIZE the distribution and operation at structured protection level of the terminal computer system according to the requirements specified in the Section 6.4.5.2 of the GB/T 20271-2006.

c) Development: REALIZE the development at structured protection level of the terminal computer system according to the requirements specified in the Section 6.4.5.3 of the GB/T 20271-2006.

5.5.1.2 Operating system

According to the requirements specified in the Section 4.5.1 of the GB/T 20272-2006, DESIGN, REALIZE or PURCHASE the operating system meeting the privacy functional requirements of the terminal computer system at access verification protection level from the following aspects:

a) Identity discrimination: According to the descriptions given in the Section 4.5.1.1 of the GB/T 20272-2006, REALIZE the functions of user identification, user discrimination, user discrimination failure processing, and user-subject binding of the operating system.

b) Discretionary access control: According to the descriptions given in the Section 4.5.1.2 of the GB/T 20272-2006, CONDUCT access control to the operating system, ALLOW legal operations, and FORBID illegal operations.

c) Marks: According to the descriptions given in the Section 4.5.1.3 of the GB/T 20272-2006, DESIGN and REALIZE the marking function of the operating system, so as to set the sensitive marks required for the subject and object.

d) Mandatory access control: According to the descriptions given in the Section 4.5.1.4 of the GB/T 20272-2006, CONDUCT access control to the operating system, ALLOW legal operations, and FORBID illegal operations. REALIZE the function of mandatory access control to the operating system, including the system files, services, drive, registries and processes.

e) Data flow control: For the operating system using data flow to realize the data exchange, according to the descriptions given in the Section 4.5.1.5 of the GB/T 20272-2006, DESIGN and REALIZE the function of data flow control of the operating system.

f) Security audit: According to the descriptions given in the Section 4.5.1.6 of the GB/T 20272-2006, DESIGN and REALIZE the security audit function of the operating system.

g) User data privacy: According to the descriptions given in the Section 4.5.1.8 of the GB/T 20272-2006, DESIGN and REALIZE the function of user data privacy protection of the operating system.

h) User data integrity: According to the descriptions given in the Section 4.5.1.7 of the GB/T 20272-2006, PROVIDE the function of ensuring the user data integrity to the user data stored, processed and transmitted in the operating system.

i) Trusted paths: According to the descriptions given in the Section 4.5.1.9 of the GB/T 20272-2006, ESTABLISH a safe data transmission path when the users conduct initial login and/or discrimination.

5.5.1.3 Trusted computing platform

5.5.1.3.1 Password support

DESIGN and REALIZE the function of password support of the terminal computer system at access verification protection level according to the descriptions given in the Section 4.3.1 of this Standard and the following requirements:

a) Cryptographic algorithm: USE the cryptographic algorithm specified by the national cryptography administrative department. USE hardware to realize the symmetric cipher algorithm, public-key cryptographic algorithm, hash algorithm, and random number generation algorithm.

b) Cryptographic operation: All the cryptographic operations shall base on the support of trusted hardware modules and other cryptographic hardware modules.

c) Key management: All the keys shall be protected by the root of trust for storage. The root of trust for storage shall be protected by the security hardware.

5.5.1.3.2 Trusted chains

DESIGN and REALIZE the function of trusted chains of the terminal computer system according to the descriptions given in the Section 4.2.3 of this Standard and the following requirements.

a) REALIZE the establishment of static and dynamic trusted chains based on the trusted hardware modules;

b) The criteria of integrity measurement of the operating system (OS) in the static trusted chains shall be managed by national specialized agencies, and shall support online or offline verification. If the metrics and criteria of measurement are inconsistent, STOP starting up the operating system.

c) The criteria of integrity measurement of all the applications in the dynamic trusted chains shall be managed by national specialized agencies, and shall support online or offline verification. If the metrics and criteria of measurement are inconsistent, STOP the application operation immediately.

d) DESIGN and REALIZE the functions of module real-time repair and module upgrading of trusted chains according to the requirements specified in the Section 4.2.3 of this Standard.

5.5.1.3.3 Protection during operation

DESIGN and REALIZE the following functions according to the requirements

REALIZE the function of identification and discrimination of the trusted computing platform from the following aspects:

a) According to the requirements specified in the Section 4.3.2.1 of this Standard, DESIGN and REALIZE the functions of unique identification, identification credibility and secrecy, and identification information management of the terminal computer system, so as to ensure the identity uniqueness and authenticity of the trusted computing platform in the terminal computer system.

b) The system identifications shall be managed by the national administrative authorities.

c) According to the requirements specified in the Section 4.3.2.2 of this Standard, DESIGN and REALIZE the function of system identity discrimination.

5.5.1.3.6.2 User identification and discrimination

According to the requirements specified in the Section 4.3.2 of this Standard, DESIGN and REALIZE the function of user identification and discrimination from the following aspects:

a) According to the requirements specified in the Section 4.3.2.3 of this Standard, DESIGN and REALIZE the functions of user basic identification, unique identification, and identification information management;

b) According to the requirements specified in the Section 4.3.2.4 of this Standard, DESIGN and REALIZE the functions of user basic discrimination, unforgeable discrimination, single-use discrimination, multi-mechanism discrimination, and re-discrimination;

c) According to the requirements specified in the Section 4.3.2.4 of this Standard, SUPPORT to provide the discrimination information in the form of digital certificate, IC cards, fingerprints, iris, etc.;

d) According to the requirements specified in the Section 4.3.2.5 of this Standard, DESIGN and REALIZE the function of user discrimination failure processing;

e) According to the requirements specified in the Section 4.3.2.6 of this Standard, DESIGN and REALIZE the function of user-subject binding;

f) According to the requirements specified in the Section 4.3.2.4 of this Standard, ESTABLISH the communication paths of the discrimination equipment and trusted hardware modules for the discrimination information in the form of IC cards, fingerprints, iris, etc., so as to ensure that the trusted

the GB/T 20271-2006, DESIGN and REALIZE the function of trusted paths of the application system.

h) Data integrity protection: According to the descriptions given in the Section 6.5.3.7 of the GB/T 20271-2006, PROVIDE the function of ensuring the user data integrity to the user data stored, processed and transmitted in the application system.

5.5.2 Security assurance requirements

5.5.2.1 SSOTCS security protection

a) Trusted root security protection: REALIZE the trusted root of the terminal computer system according to the following requirements:

– SET the root of trust for storage and the root of trust for reporting in the trusted hardware modules;

– The trusted hardware modules shall be developed by national specialized agencies;

– TAKE physical protection measures for the root of trust for measurement.

b) Keyboard input protection: REALIZE the keyboard input protection according to the following requirements:

– There shall be physical paths to support the direct communication between keyboard input and trusted hardware module;

– There shall be physical switches to control whether to enable the communication paths of the keyboard input and trusted hardware modules.

c) SSF physical security protection: REALIZE the SSF physical security protection at access verification protection level of the terminal computer system according to the following requirements:

– REALIZE the SSF physical security protection at access verification protection level of the terminal computer system according to the requirements specified in the Section 6.5.4.1 of the GB/T 20271-2006;

– TAKE appropriate hardware protection measures to prevent the cryptographic computation modules in the trusted hardware modules from energy attack.

d) SSF operational security protection: REALIZE the SSF operational security protection at access verification protection level of the terminal computer system according to the following requirements:

References

[1] GB/T 18336.1-2001 *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*

[2] GB/T 18336.2-2001 *Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements*

[3] GB/T 18336.3-2001 *Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements*

[4] GB/T 17901.1-1999 *Information technology – Security techniques – Key management – Part 1: Framework*

[5] *Trusted Computing Group TPM Main Specification Version 1.2: Part 1 Design Principles, May 2004*

_____ END _____

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

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