ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 22186-2026

Replacing GB/T 22186-2016

Cybersecurity technology - Security specification for IC card chips with a CPU

网络安全技术 具有中央处理器的IC卡芯片安全规范

Issued on: April 30, 2026 **Implemented on: November 1, 2026**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

8.1 Family FPT_EMS

8.1.1 Tribal Behavior The TOE Information Leakage (FPT_EMS) family, as defined in GB/T 18336.2, consists of one component, FPT_EMS.1, "TSF and User Data Information". The "leakage" component, this document extends with a new component FPT_EMS.2.FPT_EMS.1 requires leakage from the attack surface of TOE. The information is insufficient to compromise the security of TSF data and user data. FPT_EMS.2 further requires that even through the integration of various TOE data... The information leaked from the attack surface is still insufficient to affect the security of TSF data and user data.

8.1.2 Component Hierarchy The component hierarchy of this family is shown in Figure 2.

8.1.3 FPT_EMS.2 Management There are no foreseen management activities.

8.1.4 FPT_EMS.2 Audit There are no foreseen audit activities.

8.1.5 FPT_EMS.2 Information Leakage Fusion Subordinate to. No other components. Depends on. FPT_EMS.1 "TSF and user data information leakage". The security feature requirement FPT_EMS.2.1 indicates that even if information leaked from various attack surfaces of TOE is fused, it is still insufficient to affect For details on the security of TSF data and user data, please refer to Table 1.

8.2 Family FPT_TST

8.2.1 Tribal Behavior This document extends the TSF self-test (FPT_TST) family of standards in GB/T 18336.2 with a new component, FPT_TST.2, to enable... Implement TSF self-test function on IC card chip.

8.2.2 Component Hierarchy The component hierarchy of this family is shown in Figure 3.

8.2.3 FPT_TST.2 Management There are no foreseen management activities.

8.2.4 FPT_TST.2 Audit There are no foreseen audit activities.

8.2.5 FPT_TST.2 Subset TSF Test Subordinate to. No other components. Dependency. No dependency. The security function requirement FPT_TST.2.1 specifies that the IC card chip security function should be available during [selection. initial startup, normal operation, authorization]. When a user requests a self-test, under the condition of "Assignment. Condition for Generating Self-Test", a self-test program is run to verify the selection of the TSF group. The correctness of the operation of [components] and [TSF].

9 Safety Requirements

9.1 Overview Chapter 9 mainly covers IC card chips with central processing units that meet security levels EAL4, EAL5, and EAL6. The required safety functions and security requirements.

9.2.1 Overview of Safety Functional Requirements Components

9.2.2 Key Generation (FCS_CKM.1) The security functions of an IC card chip should be based on a specific key generation algorithm that conforms to the following standards [Assignment. Standard List] [Assignment. Key] The key is generated using a key generation algorithm and a specified key length. If the key is generated by an external environment, this component should not be selected. Note

1.This component is only applicable when the key generation function is performed by the IC card chip itself. In this case, the ST writer assigns values according to the specific cryptographic algorithm. Relevant standards and parameters recognized by the national cryptography authority or specified by ISO standards. Note

2.For the standard list, key generation algorithm, and key length assignment, please refer to reference [12].

9.2.3 Cryptographic Operations (FCS_COP.1) The security functions of IC card chips should conform to the specific standards listed below [ISO /IEC 18033 (all parts), assignment. list of standards]. The cryptographic algorithm [Assignment. cryptographic algorithm] and the key length [Assignment. key length] are used to execute [Assignment. list of cryptographic operations].

Note. The ST compiler assigns values to relevant standards and parameters approved by the national cryptography authority or specified by ISO standards based on the specific circumstances of the cryptographic algorithm.

9.2.4 Random Number Generation (FCS_RNG.1) The security requirements are as follows:

a) The IC card chip security function should provide a random number generator with the option of nondeterministic, deterministic, or mixed random number generation, and implement [selection/implementation]. Choose. Start self-test, Online self-test; Assign. Other security self-test capabilities.

b) The IC card chip security function should output [selection. bit, byte, or byte string], and conform to [GB/T 32915, assignment. other countries or] The randomness requirements specified in the International Standard Measurement Method.

9.2.5 Subset Access Control (FDP_ACC.1) IC card chip security function response [IC card embedded software, administrator, assignment. other subject list] [Read, write and execute, assignment. main] [List of other operations between objects] Operations [Flash, RAM, ROM memory, and special function registers, assignment. other objects] [List] Execute [IC card chip memory access control policy, assign value. other IC card chip access control policy].

Note. ST writers refine user data and operation lists according to specific circumstances, and adjust them based on the different user and administrator operation objects and corresponding control strategies. In ST, this component is described by dividing it into different points. This principle applies to the description of the following components.

9.2.6 Access control based on security attributes (FDP_ACF.1) The security requirements are as follows:

a) The security functions of the IC card chip should be based on the value of the memory access control register, and assigned the following security attributes related to other security policies. [Sex or security attribute group] Executes [IC card chip memory access control policy] on the object, assigning. other IC card chip access control Control Strategy.

b) The IC card chip security function shall implement the following rules to determine whether an operation between a controlled subject and a controlled object is permitted. Xu. [Whether the value of the memory access control register meets the access requirements, assign a value. other communication between the controlled subject and the controlled object.] [Rules for managing access by taking controlled actions on controlled objects].

c) The security functions of IC card chips should be based on the following additional rules. [Assignment. Based on security attributes, clearly authorizing the subject to access the object] The rules clearly define the authorized entity to access the object.