

ICS 35.040
CCS L 80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 18336.2-2015

**Information technology -- Security techniques -- Evaluation
criteria for IT security -- Part 2: Security functional components**

信息技术 安全技术 信息技术安全评估准则 第2部分：安全功能组件

(English Translation)

Issued on: May 15, 2015

Implemented on: January 1, 2016

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine of the People's Republic of China**

Table of Contents

Foreword...	6
Introduction...	8
1 Scope...	9
2 Normative references...	9
3 Terms and definitions...	9
4 Overview...	9
4.1 Organisation of this Part...	10
5 Functional requirements paradigm...	10
6 Security functional components...	15
6.1 Overview...	15
6.2 Component catalogue...	19
7 Class FAU. Security audit...	21
7.1 Security audit automatic response (FAU_ARP)...	21
7.2 Security audit data generation (FAU_GEN)...	22
7.3 Security audit analysis (FAU_SAA)...	23
7.4 Security audit review (FAU_SAR)...	27
7.5 Security audit event selection (FAU_SEL)...	29
7.6 Security audit event storage (FAU_STG)...	29
8 Class FCO. Communication...	32
8.1 Non-repudiation of origin (FCO_NRO)...	32
8.2 Non-repudiation of receipt (FCO_NRR)...	34
9 Class FCS. Cryptographic support...	36
9.1 Cryptographic key management (FCS_CKM)...	37
9.2 Cryptographic operation (FCS_COP)...	39
10 Class FDP. User data protection...	40
10.1 Access control policy (FDP_ACC)...	43
10.2 Access control functions (FDP_ACF)...	44
10.3 Data authentication (FDP_DAU)...	45
10.4 Export from the TOE (FDP_ETC)...	47
10.5 Information flow control policy (FDP_IFC)...	49
10.6 Information flow control functions (FDP_IFF)...	50
10.7 Import from outside of the TOE (FDP_ITC)...	55

10.8 Internal TOE transfer (FDP_ITT)...	57
10.9 Residual information protection (FDP_RIP)...	60
10.10 Rollback (FDP_ROL)...	61
10.11 Stored data integrity (FDP_SDI)...	62

Foreword

GB/T 18336 "Information technology - Security techniques - Evaluation criteria for IT security" includes the following 3 parts.

- Part 1.Introduction and general model;
- Part 2.Security functional components;
- Part 3.Security assurance components.

This Part is part 2 of GB/T 18336.

This Part is drafted in accordance with specifications in GB/T1.1-2009.

This Part shall replace GB/T 18336.2-2008 "Information technology - Security techniques - Evaluation criteria for IT security - Part 2.Security functional components".

The main differences between this Part and GB/T 18336.2-2008 are as follows.

- "assurance" is replaced by "assurances" [Translator note. This is mainly adjustment on Chinese. In English, the same word "assurances" should remain the most appropriate, given that "Assurances" is still used in the corresponding ISO/IEC 15408-2:2008.This translation still uses the term "Assurances"];
- "10.4 Export outside TSF control (FDP_ETC)" is amended as "10.4 Export from TOE (FDP_ETC)";
- "10.7 Import from outside TSF control(FDP_ITC)" is amended as" 10.7 Import from outside TOE (FDP_ITC)";
- "14.1 Bottom abstract machine test (FPT_AMT)", "14.10 Referring to arbitration (FPT_RVM)" and "14.11 Domain separation" in "14 FPT class. TSF protection" are deleted;
- "14.12 Test of external entity(FPT_TEE)" is added in "14 FPT class. TSF protection";

- "16.3 Session lock (FTA_SSL)" is amended as "16.3 Session lock and termination(FTA_SSL)";
- "threshold value" is replace by "critical value" [Translator note. As the corresponding ISO/IEC 15408-2.2008 still uses term "Threshold value", this translation follows the term "Threshold value", given that "This Part uses translation method to equivalently adopt the international standard ISO/IEC 15408-2.2008"];
- "mediate" is replaced by "promote" [Translator note. This is mainly adjustment on Chinese. In English, the same word "mediate" should remain the most appropriate, given that "Mediate" is still used in the corresponding ISO/IEC 15408-2.2008.This translation still uses the term "Mediate"];

This Part uses translation method to equivalently adopt the international standard ISO/IEC 15408-1.2008 "Information technology - Security techniques - Evaluation criteria for IT security - Part 2.Security functional components".

The domestic documents that are consistently corresponding to the normative international references in this Part are as follows.

- GB/T 18336.1 "Information technology - Security techniques - Evaluation criteria for IT security Part 1.Introduction and general model". (GB/T 18336.1-2015, ISO/IEC 15408-1.2009, IDT)"

This Part has the following editorial amendments.

- There is editorial error in the original text of sub-clause 4.1; it is now amended as "Those who author PP or ST should refer to clause 3 and relevant annexes of ISO/IEC 15408-1 for relevant structures, rules, and guidance".

This Part was proposed by and shall be under the jurisdiction of

China Information Security Standardization Technical Committee (SAC/TC 260).

The main drafting organizations of this Part. China Information Technology Security Evaluation Centre, Information Technology Security Test and Evaluation Centre, The Third Research Institute of Ministry of Public Security AND China Information Technology Security Evaluation Centre Jilin Centre.

Introduction

Security functional components, as defined in this Part, are the basis for the security functional requirements expressed in a Protection Profile (PP) or a Security Target (ST). These requirements describe the desired security behaviour expected of a Target of Evaluation (TOE) and are intended to meet the security objectives as stated in a PP or an ST. These requirements describe security properties that users can detect by direct interaction (i.e. inputs, outputs) with the IT or by the IT response to stimulus.

Security functional components express security requirements intended to counter threats in the assumed operating environment of the TOE and/or cover any identified organisational security policies and assumptions.

The audience for this Part includes consumers, developers, and evaluators of secure IT products. ISO/IEC 15408-1 Clause 5 provides additional information on the target audience of ISO/IEC 15408, and on the use of ISO/IEC 15408 by the groups that comprise the target audience. These groups may use this Part as follows.

- a) Consumers, who use this Part when selecting components to express functional requirements to satisfy the security objectives expressed in a PP or ST. ISO/IEC 15408-1 provides more detailed information on the relationship between security objectives and security requirements.
- b) Developers, who respond to actual or perceived consumer security requirements in constructing a TOE, may find a standardised method to understand those requirements in this Part. They can also use the contents of this Part as a basis for further defining the TOE security functionality and mechanisms that comply with those requirements.
- c) Evaluators, who use the functional requirements defined in this Part in verifying that the TOE functional requirements expressed in the PP or ST satisfy the IT security objectives and that all dependencies are accounted for and shown to be satisfied. Evaluators also should use this Part to assist in determining whether a given TOE satisfies stated requirements.