

ICS 35.040
CCS L 80



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

GB/T 18336.1-2015

**Information technology -- Security techniques -- Evaluation
criteria for IT security -- Part 1: Introduction and general model**

信息技术安全技术信息技术安全评估准则 第1部分：简介和一般模型

(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	4
Introduction	6
1 Scope	8
2 Normative references	8
3 Terms and definitions	9
4 Abbreviated terms	35
5 Overview	36
5.1 General	36
5.2 The TOE	36
5.3 Target audience of ISO/IEC 15408	38
5.4 The different parts of ISO/IEC 15408	39
5.5 Evaluation context	40
6 General model	41
6.1 Introduction	41
6.2 Assets and countermeasures	41
6.3 Evaluation	46
7 Tailoring Security Requirements	47
7.1 Operations	47
7.2 Dependencies between components	50
7.3 Extended components	51
8 Protection Profiles and Packages	51
8.1 Introduction	51
8.2 Packages	51
8.3 Protection Profiles	52
8.4 Using PPs and packages	55
8.5 Using Multiple Protection Profiles	56
9 Evaluation results	56
9.1 Introduction	56
9.2 Results of a PP evaluation	57
9.3 Results of an ST/TOE evaluation	57
9.4 Conformance claim	57
9.5 Use of ST/TOE evaluation results	59

Annex A (Informative) Specification of Security Targets	60
Annex B (Informative) Specification of Protection Profiles	80
Annex C (Informative) Guidance for Operations	86
Annex D (Informative) PP conformance	90
Bibliography	92

1 Scope

This Part of GB/T 18336 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.

It provides an overview of all parts of ISO/IEC 15408. It describes the various parts of the ISO/IEC 15408; defines the terms and abbreviations to be used in all parts of the ISO/IEC 15408; establishes the core concept of a Target of Evaluation (TOE); the evaluation context; and describes the audience to which the evaluation criteria are addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given.

It defines the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 may be tailored through the use of permitted operations.

The key concepts of protection profiles (PP), packages of security requirements and the topic of conformance are specified and the consequences of evaluation and evaluation results are described. This Part of ISO/IEC 15408 gives guidelines for the specification of Security Targets (ST) and provides a description of the organization of components throughout the model. General information about the evaluation method and the scope of evaluation schemes shall be provided in IT safety evaluation methodology.

2 Normative references

The articles contained in the following documents have become part of this document when they are quoted herein. For the dated documents so quoted, all the modifications (including all corrections) or revisions made thereafter shall be applicable to this document.

ISO/IEC 15408-2, Information technology - Security techniques - Evaluation criteria for IT security - Part 2. Security functional components

ISO/IEC 15408-3, Information technology - Security techniques - Evaluation criteria for

IT security - Part 3. Security assurance components

ISO/IEC 18045, Information technology - Security techniques - Methodology for IT Annex D (Informative)

PP conformance

D.1 Introduction

A PP is intended to be used as a "template" for an ST. That is, the PP describes a set of user needs, while an ST that conforms to that PP describes a TOE that satisfies those needs.

Note that it is also possible for a PP to be used as a template for another PP. That is PPs can claim conformance to other PPs. This case is completely similar to that of an ST vs. a

PP. For clarity this Annex describes only the ST/PP case, but it holds also for the PP/PP case.

ISO/IEC 15408 does not allow any form of partial conformance, so if a PP is claimed, the

PP or ST must fully conform to the referenced PP or PPs. There are however two types of conformance ("strict" and "demonstrable") and the type of conformance allowed is determined by the PP. That is, the PP states (in the PP conformance statement, see B.5) what the allowed types of conformance for the ST are. This distinction between strict and demonstrable conformance is applicable to each PP to which an ST may claim conformance on an individual basis. This may mean that the ST conforms strictly to some

PPs and demonstrably to other PPs. An ST is only allowed to conform to a PP in a demonstrable manner, if the PP explicitly allows this, whereas an ST can always conform with strict conformance to any PP.

Restating this in other words, an ST is only allowed to conform to a PP in a demonstrable manner, if the PP explicitly allows this.

Conformance to a PP means that the PP or ST (and if an ST is of an evaluated product, the product as well) meets all requirements of that PP.

Published PPs will normally require demonstrable conformance. This means that STs claiming conformance with the PP must offer a solution to the generic security problem described in the PP, but can do so in any way that is equivalent or more restrictive to that described in the PP. "Equivalent but more restrictive" is defined at length within ISO/IEC 15408, but in principle it means that the PP and ST may contain entirely different statements that discuss different entities, use different concepts etc., provided that overall the ST levies the same or more restrictions on the TOE, and the same or less restrictions on the operational environment of the TOE.