Chinastandards.org

ICS 35.040
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 20283-2020

Replacing GB/Z 20283-2006

Information security technology - Guide for the production of protection profiles and security targets

信息安全技术 保护轮廓和安全目标的产生指南

(English Translation)

Issued on: September 29, 2020 **Implemented on: April 1, 2021**

Issued by: State Administration for Market Regulation, China National Standardization Administration

Preview: page 1 of 5 shown, 93 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-20283-2020

Chinastandards.org

Table of Contents

Preface
Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviations
5 Overview of protection profile and safety objectives
5.1 Brief description
5.2 Reader
5.3 Use of protective contours and safety goals
5.4 Protection profile/safety goal development process
5.5 Reading and understanding the protection profile and safety goals
6 Introduction to protection profile/safety goal
7 Declaration of conformity
8 Definition of security issues
8.1 Brief description
8.2 Identify informal safety requirements
8.3 Identifying and determining threats
8.4 Identifying and determining strategies
8.5 Identifying and determining assumptions
8.6 Complete the definition of security issues
9 Security purpose
9.1 Brief description
9.2 Building threats, strategies and assumptions
9.3 Identifying non-IT operating environment security objectives
9.4 Identify the security objectives of the IT operating environment
9.5 Identify TOE Security Purpose
9.6 The basic principle of generating a security purpose
10 Expansion component definition
11 Safety requirements
11.1 Brief introduction
11.2 Safety paradigm

Preview: page 2 of 5 shown, 93 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-20283-2020

11.3 Determine safety function requirements
11.4 Determine safety assurance requirements
12 TOE Summary Specification
13 Protection profile and safety goals of the TOE of the combination and component
13.1 Combined TOE
13.2 Parts TOE
14 Special circumstances
14.1 Low-assurance protection profile and safety objectives
14.2 Function and Guarantee Package
Appendix A (informative appendix) Expansion component definition example

1 Scope

This standard gives a description of the content of each part of the protection profile and safety target document, and provides an overview of the protection profile and safety target, and Protection profile/safety goal introduction, declaration of conformity, safety issue definition, safety purpose, extended component definition, safety requirements, TOE outline specification The protection profile, safety objectives, special circumstances and other information of the TOE of the fan, combination and component.

This standard applies to the testing, evaluation, and procurement of information technology products, and the use of protection profiles for product users, developers, and testers And safety goals.

2 Normative references

The following documents are indispensable for the application of this document. For dated reference documents, only the dated version applies to this article Pieces. For undated references, the latest version (including all amendments) applies to this document.

GB/T 18336-2015 (all parts) Information technology security technology information technology security assessment criteria

GB/T 25069-2010 Information Security Technical Terms

3 Terms and definitions

The terms and definitions defined in GB/T 25069-2010 and GB/T 18336.1-2015 apply to this document.

Preview: page 3 of 5 shown, 93 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-20283-2020

4 Abbreviations

The following abbreviations apply to this document.

5 Overview of protection profile and safety objectives

5.3

Use of protection contours and safety goals

5.1 Brief description

This chapter is an overview of the readers, purpose, development process and use of PP and ST to illustrate the use of GB/T 18336- The role of PP and ST in the 2015 (all parts) information security assessment.

5.2 Readers

This standard applies to two types of readers.

a) IT professionals. They have certain security knowledge, but are not experts in information security assessment, and are 2015 (all parts) not much knowledge;

b) Information security experts. They fully understand GB/T 18336-2015 (all parts), and regard the development of PP and ST as their work content.

For IT professionals, this chapter will provide them with information to understand the purpose and structure of PP and ST, as well as to facilitate their reading and understanding Background information on PP and ST. The specific content of each part of PP and ST will be explained in detail below, and it is assumed that the reader has the GB/T 18336- Knowledge of 2015 (all parts).

For information security experts, they should already be familiar with the content of this chapter and can use the methods, techniques and practical skills provided in the subsequent chapters to achieve Prepare PP and ST in an efficient and consistent way.

If the reader is not an expert in information security, you can also use this standard to develop PP or ST. But users still need to query and read And understand the published PP or ST that has similar requirements, and you can also consider seeking help from others who have the necessary domain expertise and experience.

5.3.1 Brief description

The main purpose of GB/T 18336-2015 (all parts) is to evaluate the security of IT products. The term "IT product" is not used in It is actually defined in GB/T 18336-2015 (all parts), but it can be used to understand any entity constructed using information technology, including A complete IT system used by an organization, or produced by a product manufacturer and

Preview: page 4 of 5 shown, 93 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-20283-2020

sold to many different or unrelated customers COTS. When this standard refers to "IT products" or only "products" and other terms, it is recommended to apply to the above mentioned entities, but when it comes to certain products When there are limitations, it will be expressed in system, COTS or other specific terms.

IT products can be used in multiple environments in a variety of ways, and the concept of security will vary with the product. Therefore, by GB/T 18336- The final assessment result produced in 2015 (all parts) is by no means "this IT product is safe", but "this IT product meets this security specification."

GB/T 18336-2015 (all parts) standardizes safety regulations to facilitate the implementation of two tasks.

--- Mandatory analysis of specific content when evaluating products in accordance with safety regulations;

---Allows to compare the safety regulations of different products.

GB/T 18336-2015 (all parts) specifies two different types of safety specifications. protection contours and safety goals. Between the two The difference lies in the different roles it plays, that is, when a customer wants to buy a product from the developer, the protection profile and safety goal are purchased here. Played different roles in the process.

The concepts of customer, developer, and product are abstract. Customers are people who want to buy products, which can be individuals, single organizations, group groups Organizations, government departments, etc. A developer is a person who wants to sell a product. It can be a programmer, a small company, a large company, a group company, etc.

The product can be as small as an application software or smart card, as large as an operating system or a complex computer system with hundreds of different components.

When a customer wants to purchase a product, there are basically two processes.

---Standard-based procurement process. that is, the customer puts forward a demand to the developer, and the developer develops a product that meets the customer's demand. Adopt this This method is expensive, but the customer gets the product he wants.

---Purchasing process based on selection. that is, customers can choose a product from existing products. The cost of adopting this method is relatively low, However, the final product selected by the customer may or may not fully satisfy his needs.

When IT security requirements are very important, for general customers, these two procurement processes also bring other difficulties to them.

---It is difficult to determine what type of IT security it needs;

--- It is more difficult to determine whether a given product that claims to have IT security is available or effectively meets its needs;

Preview: page 5 of 5 shown, 93 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-20283-2020