Chinastandards.org

ICS 35.240
CCS A 90

GA

INDUSTRY STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GA/T 1545-2010

Information security technology - Security technical requirements for smart tokens

信息安全技术 智能密码钥匙安全技术要求

(English Translation)

Issued on: January 1, 1970 **Implemented on: March 4, 2019**

Issued by: Ministry of Public Security

Preview: page 1 of 5 shown, 9 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-1545-2010

Chinastandards.org

Table of Contents

Foreword
1 Scope
2 Normative references
3 Terms and definitions
4 Network and Security Device Configuration Check Product Description
5 General description
5.1 Classification of safety technical requirements
5.2 Classification of Security Levels.
6 Safety function requirements
6.1 Configuring collection
6.2 Configuration check
6.3 Inspection results
6.4 Device support
6.5 Identification and identification
6.6 Security management
6.7 Data security
6.8 Audit logs
7 Security requirements
7.1 Development
7.2 Guidance documents
7.3 Life cycle support
7.4 Testing
7.5 Vulnerability assessment
8 Requirements for different security levels
8.1 Safety function requirements
8.2 Security requirements

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This standard was proposed by the Cyber Security Bureau of the Ministry of Public Security.

Preview: page 2 of 5 shown, 9 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-1545-2010

This standard is under the jurisdiction of the Information System Security Standardization Technical Committee of the Ministry of Public Security.

This standard was drafted. Computer Information System Security Product Quality Supervision and Inspection Center of the Ministry of Public Security, Network Security and Protection Bureau of the Ministry of Public Security, Public Security the Third Research Institute of Ministry of Security, Beijing Suifang Information Technology Co., Ltd., and Beijing Shenzhou Green League Technology Co., Ltd.

1 Scope

This standard specifies the security function requirements, security assurance requirements, and classification requirements for network and security equipment configuration inspection products.

This standard applies to the design, development, and testing of network and security equipment configuration inspection products.

2 Normative references

The following documents are essential for the application of this document. For dated references, only the dated version applies to this document.

For undated references, the latest version (including all amendments) applies to this document.

GB/T 18336.3-2015 Information technology security technology Information technology security assessment guidelines Part 3. Security assurance components GB/T 25069-2010 Information Security Technology Terminology

3 Terms and definitions

GB/T 18336.3-2015 and GB/T 25069-2010 and the following terms and definitions apply to this document.

Configuration of network and security equipment Records network settings, security policies, enabling services, and related parameters of the network and security devices.

Product inspecting configuration of network and security equipment Obtain network and security device configurations and compare them with predefined baselines to determine if they meet the baseline requirements of the product.

4 Network and Security Device Configuration Check Product Description

Network and security device configuration inspection products are usually deployed in the

Preview: page 3 of 5 shown, 9 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-1545-2010

target network in a bypass manner, and collected and analyzed online or offline.

Network and security equipment configuration and configuration check.

Figure 1 is a typical operating environment of network and security equipment configuration check products.

switch

Firewall router

server

Intrusion detection

Network and security equipment Configuration check product Configuration file Target network

Figure 1 Network and security equipment configuration check product typical operating environment

5.1 Classification of safety technical requirements

This standard divides the security technical requirements for network and security equipment configuration inspection products into two categories. security functions and security assurance requirements. its , Security function requirements are specific requirements for the security functions that network and security device configuration inspection products should have, including configuration acquisition, Configuration checks, check results, device support, identification and authentication, security management, data security, and audit logs; security assurance requirements are specific to the network Network and safety equipment configuration inspection product life cycle process put forward specific requirements, including development, guidance documents, life cycle support, Testing and vulnerability assessment.

5.2 Classification of security levels

Network and security equipment configuration check The product's security level is divided into basic according to the strength of its security function requirements and security assurance requirements.

Level and enhanced level, in which the security requirements refer to GB/T 18336.3-2015.

6.1.1 Information Collection

The product should be able to collect the following configuration information for network and security devices.

a) System information such as the brand, model and operating system version of the

Preview: page 4 of 5 shown, 9 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-1545-2010

device;

b) Configuration and related parameters of device authentication, remote login, audit, access control and other policies.

6.1.2 Collection method

The product should be able to collect configuration information for network and security devices in the following ways.

a) Collect online through login device;

b) Offline import by manually importing the device configuration file.

6.1.3 Collection impact

When obtaining configuration information of network and security devices through online collection, the product should meet the following requirements.

a) Do not change the configuration of the acquisition target;

b) Does not affect the normal operation of the acquisition target function.

6.2.1 Identification Strategy Check

The product should be able to check the configuration and related parameters of network and security device authentication policies, including at least password complexity and other configurations.

6.2.2 Locking Policy Check

The product should be able to check the configuration and related parameters of network and security device lockout policies, including at least login failure lockout and timeout lockout Fixed configuration.

6.2.3 Remote login policy check

The product should be able to check the configuration and related parameters of the network and security device remote login policies, including at least login IP restrictions, login Configuration, etc.

6.2.4 SNMP Policy Check

The product should be able to check the configuration of SNMP policies and related parameters of network and security devices, including at least the SNMP community name and SNMP version and other configurations.

Preview: page 5 of 5 shown, 9 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-1545-2010