

ICS 35.240
CCS A 90

GA

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

GA/T 1552-2019

**Information security technology - Security technical
requirements for disk array safety storage products**

信息安全技术 盘阵安全存储产品安全技术要求

(English Translation)

Issued on: January 1, 1970

Implemented on: April 9, 2019

Issued by: Ministry of Public Security

Table of Contents

Foreword
1 Scope
2 Normative references
3 Terms and definitions
4 Acronyms
5 General description
5.1 Classification of safety technical requirements
5.2 Classification of Security Levels.
6 Safety function requirements
6.1 Storage type support
6.2 Storage Resource Access Control
6.3 Data security
6.4 Storage reliability
6.5 Identification and identification
6.6 Management function requirements
6.7 Audit function requirements
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.

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, China Dianhaikang Group Co., Ltd., Zhejiang Dahua Technology Co., Ltd., Hangzhou Hongshan Technology Co., Ltd.

1 Scope

This standard specifies the security function requirements, security guarantee requirements, and classification requirements for disk array secure storage products.

This standard applies to the design, development, and testing of disk array secure storage 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.

Disk array safety storage product Disk array storage products with security functions.

Redundant array of independent disk A redundant array of independent disks.

Storage body

Consumers of storage resources, including hosts and users.

4 Acronyms

The following abbreviations apply to this document.

ISCSI. Internet Small Computer System Interface FC. Fibre Channel SAN. Storage Area Network NAS. Network Attached Storage RAID. Redundant Array of Independent Disk

5.1 Classification of safety technical requirements

This standard divides the security technical requirements for disk array secure storage products into two categories. security functions and security assurance requirements. Among them, the safety function should Qiushi put forward specific requirements for the security functions that disk array secure storage products should have, including storage type support, storage resource access control, data Data security, storage reliability, etc .; security requirements require specific requirements for the life cycle process of disk array secure storage products, such as Development, instructional documentation, lifecycle support and testing.

5.2 Classification of security levels

The security level of disk array security storage products is divided into basic level and enhanced level according to the strength of their security function requirements and security guarantee requirements.

Among them, security requirements refer to GB/T 18336.3-2015.

6.1 Storage type support

Support at least one of iSCSI, FC SAN, NAS.

6.2.1 Storage subject management

Should be able to manage storage principals.

- a) You can add or delete hosts or users using storage resources;
- b) Manage hosts or users in groups. Host groups and user groups with different levels can be established and different access rights can be set.

6.2.2 Storage Resource Management

Should be able to manage storage resources.

- a) storage resources can be allocated to authorized subjects;
- b) monitoring the use of storage resources;
- c) Ability to expand storage resources.

6.2.3 Access Control Policy

It should support the configuration of access control policies based on storage subjects, storage resources, and access methods.

6.2.4 Access assurance capabilities

Authorized principals should be able to access corresponding storage resources based on predefined policies.

6.2.5 Access control capabilities

The following access control capabilities should be supported.

- a) Access subject restrictions. Only authorized subjects can access storage resources;
 - b) Access content restrictions. The content that authorized subjects can access to storage resources cannot exceed a predefined range;
 - c) Access address restrictions. When an authorized subject is allowed to remotely access storage resources through the network, the address of the subject cannot exceed a predetermined address the scope of justice
 - d) Restriction on access actions. The actions of authorized subjects to access storage resources cannot exceed the predefined allowable range.
- 1) If iscsi or FC SAN is supported, it should be able to restrict read-only, read-write and other actions of authorized entities to storage resources.

Out of the predefined allowable range;

- 2) If the NAS method is supported, it should be able to restrict read-only, write, execute, attribute modification, and deletion of storage resources by authorized subjects Operation cannot exceed the predefined allowable range.

6.3.1 Data transmission security

It should be able to protect the remote access session content when the subject accesses the storage resource from unauthorized access through encryption and other methods.

6.3.2 Data storage security

Encryption or other protection measures should be used to achieve confidentiality of data storage.

6.3.3 Encryption Algorithm

Data storage should use a cryptographic algorithm approved by the national password management authority.