

ICS 35.240
CCS A 90

GA

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

GA/T 1547-2019

**Information security technology - Security technical
requirements and testing and evaluation methods for user data
storage of mobile intelligent terminal**

信息安全技术 移动智能终端用户数据存储安全技术要求和测试评价方法
(English Translation)

Issued on: January 1, 1970

Implemented on: March 8, 2019

Issued by: Ministry of Public Security

Table of Contents

1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 General description	1
4.1 Classification of safety technical requirements	2
4.2 Classification of safety technical requirements	2
5 Safety technical requirements	2
5.1 Data storage	2
5.2 Data access control	2
5.3 Data backup and recovery	3
5.4 Data destruction	3
5.5 Security Audit	3
6 Test Evaluation Method	3
6.1 Data storage	4
6.2 Data access control	5
6.3 Data backup and recovery	6
6.4 Data destruction	6
6.5 Security audit	7
7 Requirements for different security levels	7

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.

1 Scope

This standard specifies the technical requirements for user data storage security, testing and evaluation methods, and classification requirements for mobile smart terminals.

This standard applies to mobile smart terminal operating systems and applications in information systems of different security levels.

Design, development and testing.

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 18336.2-2015 Information technology security technology Information technology security assessment guidelines Part 2. Security function components GB/T 25069-2010 Information Security Technology Terminology GB/T 30284-2013 Security technical requirements for operating systems of mobile communication intelligent terminals (EAL level 2)

3 Terms and definitions

The terms and definitions defined in GB/T 18336.2-2015, GB/T 25069-2010 and GB/T 30284-2013 and the following apply to this file.

Mobile intelligent terminal A mobile communication terminal device that is connected to a public mobile communication network, has an operating system, and can be installed and uninstalled by a user.

User data

Important data generated by or serving users.

Subject

The entity that performed the operation.

Object

The entity object operated by the principal.

4.1 Classification of safety technical requirements

The security level required by mobile smart terminal user data storage security technology is in accordance with data storage, data access control, data backup and recovery the intensity of recovery, data destruction, and security auditing is divided into basic and enhanced levels.

4.2 Classification of safety technical requirements

This standard mainly proposes specific security technical requirements for each stage based on the life cycle of data storage of mobile intelligent terminal users, including Storage, data access control, data backup and recovery, data destruction and security audit.

5.1.1 Storage media

Provide secure storage media and storage paths for user data.

- a) User data should be stored in a non-volatile storage medium at power failure;
- b) The user data generated by the subject should be stored in the default or set path.

5.1.2 Resource Control

The ability to allocate resources should be designed and implemented according to the following requirements.

- a) can limit the storage resources occupied by user data generated by the application;
- b) When the data storage space reaches the threshold, the mobile smart terminal operating system user can be alerted.

5.1.3 Defining data attributes

Data attributes should be defined by default or authorization configuration.

- a) Basic attributes. generation time, last modification time, last access time, etc .;
- b) Security attributes. owner, read/write permissions, data category, authorized subject and permissions, scope of use, etc .;
- c) the importance of the data.

5.1.4 Data confidentiality

Measures should be taken to ensure the confidentiality of user data on mobile smart terminals.

- a) Use password technology to ensure the confidentiality of user data when stored locally;
- b) Encrypt and decrypt important user data using a cryptographic algorithm approved by the national cryptographic authority.

5.1.5 Data integrity

Protect and monitor the integrity of user data on mobile smart terminals.

- a) Use verification technology or password technology to ensure the integrity of user data storage;
- b) monitoring the integrity of user data, with clear prompts when integrity is breached;
- c) adopting cryptographic technology to ensure the integrity of important user data during storage, and adopting cryptographic algorithms approved by the national password authority;
- d) When integrity errors are detected, necessary recovery measures should be taken for user data.

5.2.1 Access Control Policy

Should provide a default or definable access control policy.

- a) The access control policy should include elements such as authorized subjects, access methods (read, write, delete, etc.) and objects;
- b) the access control policy should cover all subjects, objects and operations between them;
- c) an access control policy using the default prohibition principle;
- d) Following the principle of least authorization, grant the entity the least necessary authority for the business.

5.2.2 Subject Identification and Identification

Before performing any operation on user data, authenticate or identify the subject.

- a) When the operator is a person, his identity should be identified;
- b) When the operating entity is an entity such as application software, its identity should be identified.

5.2.3 Access Control Based on Security Attributes

Access control based on security attributes should be provided, and only subjects allowed by the access control policy can perform corresponding operations on user data Make.