

ICS 35.240
CCS A 90

GA

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

GA/T 1549-2019

**Information security technology - Security technical
requirements for dual-interface authentication card**

信息安全技术 双接口鉴别卡安全技术要求

(English Translation)

Issued on: January 1, 1970

Implemented on: March 19, 2019

Issued by: Ministry of Public Security

Table of Contents

Foreword
1 Scope
2 Normative references
3 Terms and definitions
4 Acronyms
5 Description of dual interface authentication card
6 Safety function requirements
6.1 General safety function requirements
6.2 Requirements for contact safety functions
6.3 Requirements for non-contact safety functions
7 Security requirements
7.1 Development
7.2 Guidance documents
7.3 Life cycle support
7.4 Testing
7.5 Vulnerability assessment
References

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, and the Third Research Institute of the Ministry of Public Security.

1 Scope

This standard specifies the security function requirements and security guarantee requirements of dual-interface authentication cards.

This standard applies to the design, development, and testing of dual-interface authentication cards.

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 requirements 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.

Dual-interface authentication card Smart cards with both contact and contactless interfaces, and such cards carry at least one contactless and contactless application.

Application software the architecture is software based on the chip operating system that implements the application functions of the smart card.

Cardholder

End users who use contact applications for their intended purpose.

Issuer

Administrator user who is responsible for product release, product obsolescence, etc.

4 Acronyms

The following abbreviations apply to this document.

CAD. Card Acceptor Device DIAC. Dual-Interface Authentication Card PIN. Personal Identification Number

5 Description of dual interface authentication card

The dual-interface authentication card is a multi-application dual-interface smart card. The card has both contact and non-contact interfaces.

The port can be used in different application scenarios, including at least the following aspects.

- a) Access by contactless applications can only be achieved through contactless interfaces;
- b) Contact application access can only be achieved through a contact interface, and cardholders are required to enter a PIN code to complete the card and host system Two-way authentication to complete the verification of the smart card.

6.1.1 Application Interface Restrictions

All data of contactless applications can only communicate with external entities through contactless interfaces; all data of contactless applications can only pass the contact interface communicates with external entities.

6.1.2 Application isolation

The code or data of any application must not be accessed and manipulated by other applications unless the application has been explicitly authorized to access Ask for the corresponding code or data.

6.1.3.1 Handling of authentication failure

When the number of failed user authentication attempts reaches the specified number, the product shall be able to terminate the authentication session process.

6.1.3.2 Reuse of authentication information

The product should prevent the reuse of authentication information related to the authentication mechanism.

6.1.3.3 Re-identification

The product shall re-identify the user under the following conditions.

- a) Termination of the smart card session;
- b) Smart card reset.

6.1.4.1 Security function management

The product should be limited to authorized users to manage the following security features.

- a) application software management;
- b) Smart card life cycle management;
- c) key management;
- d) PIN code management.

6.1.4.2 Management of security attributes

The product should only allow authorized users to update the smart card lifecycle status one-way, modify application software lifecycle status, user permissions, PIN status and other security attributes.

6.1.4.3 Initialization of static attributes

The product should provide a limited default value for security attributes and allow only authorized users to modify these default values.

6.1.4.4 Security roles

The product should be able to maintain security roles such as cardholder, issuer, and runtime context.

6.1.5.1 Access control policy

The product shall ensure that all operations involved in the security function are covered by the access control policy, and the subject shall be able to follow the predefined access control Strategic access objects.

6.1.5.2 Access Control Based on Security Attributes

Products should provide clear access assurance capabilities and denial of access capabilities based on the security attributes of the subject and object.

6.1.5.3 Data confidentiality

Product security functions should perform confidentiality processing of user data.

6.1.5.4 Data integrity

Product security functions should perform integrity checks on user data.

6.1.6.1 Safety function test

When the product is initialized, it should run a self-test procedure to prove the correct operation of the product.

6.1.6.2 Fail-safe

The product should automatically return to a safe state when the following failure conditions occur.

a) identification of data integrity violations;