

ICS 03.060
CCS A 11

JR

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

JR/T 0192-2020

**Security Regulations for Mobile Internet Applications in the
Securities and Futures Industry
(English Translation)**

Issued on: July 10, 2020

Implemented on: July 10, 2020

Issued by: People's Bank of China

Table of Contents

Foreword	
Introduction	
1 Scope	
2 Normative references	
3 Terms and definitions	
4 Mobile terminal security	
4.1 Mobile Internet Applications	
4.2 Mobile terminal environment	
4.3 Installation and Uninstallation	
4.4 Upgrade and update	
5 Identity authentication	
5.1 Identification method	
5.2 Authentication data protection	
5.3 Password security	
6 Network Communication Security	
6.1 Communication protocol	
6.2 Session Management	
6.3 Third-party network communication	
7 Data Security	
7.1 Data Entry	
7.2 Data storage	
8 Development Security	
8.1 Safety requirements	
8.2 Security Development	
8.3 Safety test	
8.4 Security Release	
9 Security Audit	
9.1 Log generation	
9.2 Log Management	
References	

Foreword

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

This standard was proposed by the Securities Sub-Technical Committee of the National Financial Standardization Technical Committee (SAC/TC 180/SC4).

This standard is under the jurisdiction of the National Financial Standardization Technical Committee (SAC/TC 180).

Drafting organizations of this standard. China Securities Regulatory Commission Information Center, Shanghai Stock Exchange, Shenzhen Stock Exchange, China Securities Regulatory Commission Information Technology Services Co., Ltd., Shanghai Futures Exchange, Dalian Commodity Exchange, China Financial Futures Exchange, China Securities Accounting Co., Ltd., China Futures Market Monitoring Center Co., Ltd., China Futures Association, Industrial Securities Co., Ltd., Taijunan Securities Co., Ltd., Soochow Securities Co., Ltd., Everbright Securities Co., Ltd., Huatai Securities Co., Ltd., Haitong Futures Co., Ltd., Industrial Fund Management Co., Ltd., the Third Research Institute of the Ministry of Public Security, Shanghai Information Security Evaluation and Certification Center.

Introduction

With the vigorous rise of emerging technologies of the mobile Internet, an endless stream of innovative businesses has emerged in the areas of business model application and technological risk control.

Facing the financial industry poses new challenges. In the current wave of Internet finance, the pressure on information system construction and safe operation is increasing.

The information security situation is becoming increasingly complex. The security issues of mobile Internet applications (APP) in the financial industry are particularly severe.

In order to strengthen the standardized management of mobile Internet application information services, the state encourages relevant industry associations to formulate self-regulatory management in accordance with the law System to strengthen the protection of user rights.

Industry's mobile terminal application security regulations, conduct security testing and risk assessment on mainstream mobile terminal applications in the market, and improve monitoring channels and Early warning mechanism, establish a mobile terminal application security risk warning system, and promptly discover and report design flaws and security vulnerabilities in mobile terminal applications, as well as counterfeit and tampered mobile terminal applications. Supervise operating agencies to strengthen the safety management of mobile terminal applications, and effectively increase investor risks Awareness of

prevention.

Security Regulations for Mobile Internet Applications in the Securities and Futures Industry

1 Scope

This standard specifies mobile terminal security, identity authentication, network communication security, and data security for mobile Internet applications in the securities and futures industry.

Complete, develop safety and safety audit.

This standard applies to the development and release of mobile Internet applications by securities and futures industry institutions.

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 22239-2008 Information Security Technology Information System Security Level Protection Basic Requirements
GB/T 25069-2010 Information Security Technical Terms
JR/T 0060-2010 Basic requirements for security level protection of information systems in the securities and futures industry

3 Terms and definitions

The following terms and definitions defined in GB/T 25069-2010, GB/T 22239-2008 and JR/T 0060-2010 apply to this article Pieces.

Mobile terminal

Representatives of smart devices such as mobile phones and tablet computers can install and use securities and futures mobile Internet applications.

Computer equipment used in.

Mobile internet application; app Installed on the mobile terminal, used for securities and futures inquiry, trading, business handling and other business-related native applications.

Note: Mobile Internet applications include, but are not limited to, mobile Internet applications related to business processing, securities and futures trading, office, information disclosure Public mobile Internet applications, mobile Internet applications issued by other participating institutions (service agencies) in the securities and futures industry.

Customer information the mobile Internet application program is related to a specific natural person or legal person, which can be identified alone or in combination with other

information.

Determine the computer data of a natural person.

Note: Computer data is a set of data related to the identity and property attributes of natural persons.

Sensitive information Once leaked, illegally provided, or abused, it may endanger personal and property safety, and easily cause personal or corporate reputation and property damage, etc.

Personal and corporate information.

4.1 Mobile Internet applications

The mobile Internet application program is stored on the mobile terminal in the form of an independent program, and it should meet the security requirements.

- a) Adopt anti-dynamic debugging, code obfuscation, anti-reverse technologies to protect key codes and core logic;
- b) No interface of any type that violates and bypasses security measures and interfaces of any mode not explained in the development document should not be designed;
- c) Ensure the confidentiality of input information, such as adopting custom keyboards, random keyboard positions, and preventing keyboard eavesdropping techniques;
- d) Identify the legality of the input information;
- e) Do not access, modify, or delete data irrelevant to the business on the mobile terminal without the user's permission;
- f) To obtain other permissions on the mobile terminal, the user should be prompted in an obvious way, including but not limited to icons, text and sound prompts;
- g) Have an integrity check mechanism to prevent re-signature and secondary packaging. Critical verification codes should be protected;
- h) When an exception occurs, clear and easy-to-understand business operation information should be prompted to avoid directly returning the program code error to the user.

4.2 Mobile terminal environment

The mobile terminal environment should support the following security checks.

- a) Mobile Internet applications should check the security of the operating environment before each run, and prompt the risks found;
- b) During the startup and operation of mobile Internet applications, corresponding process protection measures should be taken to prevent illegal programs from acquiring the process