

ICS 35.240.40
CCS A 11

JR

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

JR/T 0068-2012

Replacing JR/T 0068-2012

**General specification of information security for internet
banking system
(English Translation)**

Issued on: February 5, 2020

Implemented on: February 5, 2020

Issued by: People's Bank of China

Table of Contents

Foreword
Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviations
5 Overview of Online Banking System
6 Safety regulations
References

Foreword

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

This standard replaces JR/T 0068-2012 "General Specification for Internet Banking System Information Security".

Compared with JR/T 0068-2012, the main changes of this standard are as follows.

- Add the related requirements of SM series algorithms (see 5.4);
- Deleted content that overlapped with JR/T 0071 "Implementation Guidelines for Information Security Level Protection of Information Systems in the Financial Industry" (2012 6.1.4 and 6.2 of the annual version);
- Modified the description of client security and added security requirements such as self-protection and sensitive information protection (see 6.2.1.1, 2012 Version 6.1.1);
- Added barcode payment related requirements (see 6.2.1.1, 6.2.4.3);
- Modified the safety requirements of special safety equipment and renamed it "Special safety mechanism" (see 6.2.2, 6.1.2 of the 2012 edition);
- Added security unit and mobile terminal payment trusted environment related requirements (see 6.2.2.1, 6.2.2.5);
- Added biometric requirements (see 6.2.2.5);
- Added cloud computing security related requirements (see 6.2.4.1, 6.3.1);
- Added IPv6 related requirements (see 6.2.4.3);

- Added virtualization security related requirements (see 6.2.4.4);
- Added the basic description and security requirements of the connection security between the online banking system and external systems (see 6.2.5);
- Modified business continuity and disaster recovery safety requirements (see 6.3.7, k and l in 6.2.6 of the 2012 edition);
- Modified the security requirements for security incidents and emergency response (see 6.3.8, m and n in 6.2.6 of the 2012 edition);
- Added the relevant requirements for bank settlement accounts and transaction security locks for types II and III (see 6.4.1);
- Deleted the basic network protection architecture reference diagram, enhanced network protection architecture reference diagram and physical security (2012 Appendix A, Appendix B, and Appendix C of the annual edition).

This standard was proposed by the People's Bank of China.

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

Drafting organizations of this standard. Science and Technology Department of the People's Bank of China, China UnionPay Co., Ltd., Bank Card Testing Center, Industrial and Commercial Bank of China Co., Ltd., China Construction Bank Co., Ltd., Agricultural Bank of China Co., Ltd., China Postal Savings Bank Co., Ltd.

Company, China Merchants Bank Co., Ltd., China Minsheng Bank Co., Ltd., National Information Technology Security Research Center, CICC Certificate Center Co., Ltd.

Introduction

This standard collects and analyzes the information security problems of the online banking system and the online banking cases that have occurred during the assessment and inspection.

Put forward safety requirements pertinently.

The purpose of this standard is to effectively enhance the security protection capabilities of the existing online banking system and promote the standardized and healthy development of online banking. This standard can either as a security basis for the construction, transformation and upgrading of various units' online banking systems, security inspections and internal audits, it can also be used as an industry leader the basis for inspection, testing and certification by administrative departments and professional testing institutions.

General Specification for Information Security of Online Banking System

1 Scope

This standard specifies the security technical requirements, security management requirements, and business operation security requirements of the online banking system, and provides Design, operation and evaluation provided the basis.

This standard applies to the online banking system operated by commercial banks and other banking financial institutions established within the territory of the People's Republic of China. Other the business system of financial institutions providing online financial services should refer to this standard.

Note 1: This standard is divided into two levels. basic requirements and enhanced requirements. The basic requirements are the minimum security requirements, and the enhanced requirements are to further enhance the security of the system.

Claim. All units shall, while complying with the basic requirements for implementation, actively take improvement measures in accordance with the enhanced requirements to continuously improve their safety assurance capabilities.

Note 2: If there is no "corporate online banking" specified in the terms of this standard, it applies to both personal online banking and corporate online banking.

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 document.

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

GB/T 25069-2010 Information Security Technical Terms GB/T 27912-2011 Financial Services Biometrics Security Framework GM/Z 0001-2013 Cryptographic terms GM/T 0002-2012 SM4 block cipher algorithm GM/T 0003-2012 SM2 Elliptic Curve Public Key Cryptographic Algorithm GM/T 0004-2012 SM3 cryptographic hash algorithm GM/T 0021-2012 Dynamic Password Password Application Technical Specification JR/T 0071 Implementation Guidelines for the Cyber Security Level Protection of the Financial Industry JR/T 0098.5 China Financial Mobile Payment Testing Specification Part 5: Security Unit (SE) Embedded Software Security JR/T 0118-2015 Financial Electronics Certification Specification JR/T 0149-2016 China Financial Mobile Payment Tokenization Technical Specification JR/T 0156-2017 Technical Specification for Trusted Environment of Mobile Terminal Payment JR/T 0166-2018 Cloud Computing Technology Financial Application Specification Technical Architecture JR/T 0167-2018 Cloud Computing Technology Financial Application Specification Security Technical Requirements JR/T 0168-2018 Cloud Computing Technology Financial Application Specification Disaster Recovery Notice of the People's Bank of China on Improving Personal Bank Account Services and Strengthening

Account Management (Yinfa [2015] No. 392), 2015-12-25 Notice of the People's Bank of China on Further Strengthening Bank Card Risk Management (Yinfa [2016] No. 170), 2016-06-13 Notice of the People's Bank of China on Strengthening the Management of Payment and Settlement and Preventing New Types of Illegal Crimes in Telecommunications Networks 261), 2016-09-30

Notice of the People's Bank of China on Implementing the Classification Management System for Personal Bank Accounts (Yinfa [2016] No. 302), 2016-11-25 Notice of the General Office of the People's Bank of China on Strengthening the Security Management of Bank Card Magnetic Strip Transactions (Yinbanfa [2017] No. 120), 2017-05-31 Barcode Payment Security Technical Specifications (for Trial Implementation) (Yinbanfa [2017] No. 242 issued), 2017-12-22 Notice of the People's Bank of China on Issues Concerning the Improvement of Classified Management of Personal Bank Accounts (Yinfa [2018] No. 16), 2018-01-10 Notice of the People's Bank of China on Further Strengthening the Administration of Payment and Settlement and Preventing New Types of Illegal Crimes in Telecommunications Networks [2019] No. 85), 2019-03-22

3 Terms and definitions

The following terms and definitions defined in GB/T 25069-2010 and GM/Z 0001-2013 apply to this document. For ease of use, Some terms and definitions in GM/Z 0001-2013 are repeated below.

Internet banking

Commercial banks and other banking financial institutions use the Internet, mobile communication networks, other open public networks or private network infrastructure Online financial services provided to its customers.

Personal internet banking Online financial services provided by banking financial institutions such as commercial banks to individual users.

Corporate internet banking Commercial banks and other banking financial institutions provide online financial services to enterprises, institutions and other organizations.

Payment sensitive information Passwords, keys, and sensitive transaction data that affect the security of online banking.

Note: Passwords include but are not limited to transfer passwords, query passwords, login passwords, certificate PINs, etc. Keys include but are not limited to ensure communication security, report Symmetric keys, private keys, etc. for document integrity, transaction sensitive data include but are not limited to complete track information, validity period, CVN, CVN2, etc.

Mobile terminal