

ICS 35.240.40
CCS A 11

JR

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

JR/T 0185-2020

**Commercial bank application programming interface secure
management specification
(English Translation)**

Issued on: February 13, 2020

Implemented on: February 13, 2020

Issued by: People's Bank of China

Table of Contents

Foreword	
1 Scope	
2 Normative references	
3 Terms and definitions	
4 Abbreviations	
5 Overview	
6 Interface Type and Security Level	
7 Safety design	
8 Security deployment	
9 Security Integration	
10 Security Operation and Maintenance	
11 Service termination and system offline	
12 Security Management	
Appendix A (Normative Appendix) Diagram of Commercial Bank Application Program Interface Relationship	
Appendix B (Normative Appendix) Uniform Identification Code Coding Rules for Commercial Bank Application Program Interface	
References	

Foreword

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

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. Department of Science and Technology of the People's Bank of China, China Financial Electronics Corporation, China UnionPay Co., Ltd., China Industry and Commerce Bank Co., Ltd., Agricultural Bank of China Co., Ltd., Bank of China Co., Ltd., China Construction Bank Co., Ltd., China Postal Savings Bank Co., Ltd., China Merchants Bank Co., Ltd., Shanghai Pudong Development Bank Co., Ltd., China CITIC Bank Co., Ltd., Industrial Bank Co., Ltd., China Minsheng Bank Co., Ltd., China Everbright Bank Co., Ltd., Ping An Ann Bank Co., Ltd., China Guangfa Bank Co., Ltd., Bank of Beijing Co., Ltd., Huishang Bank Co., Ltd., Shandong Provincial City Commercial Bank

Cooperative Alliance Co., Ltd., Qilu Bank Co., Ltd., Zhejiang Internet Commercial Bank Co., Ltd., CITIC Baixin Bank Co., Ltd., Shandong Rural Credit Cooperatives Association, Beijing Zhongjin Guosheng Certification Co., Ltd., Beijing UnionPay Gold Card Technology Co., Ltd., CICC Financial Certification Center Co., Ltd., China Foreign Exchange Trading Center.

1 Scope

This standard specifies the types and security levels, security design, security deployment, security integration, and security operation of commercial bank application program interfaces.

Security technology and security requirements such as maintenance, service termination, system offline, and security management.

This standard applies to the design and application of application program interfaces for external interconnection of commercial banks to guide the application of commercial banks.

Banking financial institutions that provide sequential interface services, and applications of integrated interface services carry out relevant work, and provide services for third-party security assessment agencies and other units Carrying out safety inspection and evaluation work to provide reference (see Appendix A for the relationship of interface types). Design and application of other types of application program interfaces can refer to this standard for implementation.

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 Information Security Technical Terms JR/T 0071 Implementation Guidelines for Information Security Level Protection of Information Systems in the Financial Industry JR/T 0124-2014 Financial institution coding standard

3 Terms and definitions

The following terms and definitions defined in GB/T 25069 apply to this document.

Application programming interface A set of pre-defined functions, through which developers can easily access related services without paying attention Design and implementation of services.

Application agency

The institution that calls the commercial bank application program interface.

Application programming interface unique ID it is defined by the commercial bank and is used to distinguish the unique identifier of the commercial bank application program interface function.

Uniform application programming interface ID the unified identification code of the commercial bank application program interface generated by the commercial bank in accordance with the coding rules issued by the competent department of the industry.

Note: It is used to identify the commercial bank institution code, interface type, service category, interface sequence number, etc.

Application software development kit software development kit A collection of software development tools used when building applications based on specific software packages, software frameworks, hardware platforms, operating systems, etc.

Application unique ID After the application party's identity is verified, it is a unique identifier granted by the commercial bank according to the type of financial products and services it calls.

Note: Including server-side application identification and mobile terminal application software identification.

Application secret

The application legitimacy authentication certificate is used in conjunction with the application's unique identifier to verify the legitimacy of the application accessed through the API, and the access verification After passing the certificate, you can complete the system docking, call the application program interface or use the functions and data provided by the application program interface.

Financial mobile application software Application software that provides users with financial transaction services on mobile terminals.

Note: Including but not limited to executable files, components, etc.

Personal financial information Personal information obtained, processed and stored by financial institutions through the provision of financial products and services or other channels.

Note 1: Including account information, identification information, financial transaction information, personal identification information, property information, loan information, and other information that reflect certain situations of specific individuals.

Situation information.

Note 2: Rewrite GB/T 35273-2017, definition 3.1.

3.10

Payment sensitive information the payment information involves important information about the privacy and identification of the payment subject.

Note: Including but not limited to bank card track or chip information, card verification code, card validity period, bank card password, online payment transaction password, etc.

3.11

Payment account

The code and bank card number of bank accounts with financial transaction functions and payment accounts of non-bank payment institutions.

[JR/T 0149-2016, definition 3.1] 3.12 Explicit consent the subject of personal financial information clarifies the specific processing of his personal financial information through a written statement or proactive affirmative action Authorized behavior.

Note: Affirmative actions include the personal information subject actively making a statement (electronic or paper format), actively checking, and actively clicking "agree", "register", and "send" Send" "Dial" etc.

[GB/T 35273-2017, definition 3.6]

4 Abbreviations

The following abbreviations apply to this document.

5 Overview

Commercial bank application program interface service is a financial service model that relies on API technology to realize internal and external interconnection. Commercial Bank Link by providing partners with an application program interface for interconnection, exporting their own financial service capabilities and information technology capabilities, in order to increase the financial ecosystem Viscosity provides a useful supplement. External institutions can call commercial bank application program interfaces through Internet channels (external API, see appendix for details) A) To obtain various services provided by commercial banks, the logical structure is shown in Figure 1.

Participants of commercial bank application program interface services mainly include users, application parties and commercial banks. Commercial banks directly the connection or SDK indirect connection provides application program interface services to application parties and users to realize the external output of commercial banking services.

The user initiates a commercial bank application program interface application request, and receives the processing result returned by the application party or the commercial bank.

The application party is responsible for receiving and processing user requests, submitting