

ICS 35.020
CCS V 07

MH

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

MH/T 0068-2018

**Civil Aviation Mobile App Security Assessment Guide
(English Translation)**

Issued on: December 14, 2018

Implemented on: April 1, 2019

Issued by: Civil Aviation Administration of China

Table of Contents

Foreword	
1 Scope	
2 Normative references	
3 Terms and definitions	
4 Basic requirements for cyber security of civil aviation mobile applications	
4.1 Identification	
4.2 Access Control	
4.3 Security Audit	
4.4 Protection of Sensitive Information	
4.5 Security of communication	
4.6 Software fault tolerance	
4.7 Software protection	
4.8 Data backup and recovery	
5 Overview of Civil Aviation Mobile Application Security Evaluation	
5.1 Basic principles of evaluation	
5.2 How the assessment works	
6 Phased work of civil aviation mobile application security evaluation	
6.1 Evaluation process	
6.2 Evaluation preparation stage	
6.3 Preparation stage of evaluation plan	

Foreword

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

This standard was proposed by the Department of Personnel, Science and Education, Civil Aviation Administration of China.

This standard is under the jurisdiction of the China Academy of Civil Aviation Science and Technology.

Drafting organizations of this standard. Civil Aviation University of China, Guangdong Airport Baiyun Information Technology Development Co., Ltd., Nankai University, Beijing Bangbang Security Technology Co., Ltd., Beijing Zhiyou Wangan Technology Co., Ltd.

1 Scope

This standard specifies the basic principles and working methods for the evaluation of civil aviation mobile applications.

This standard is applicable to guide the safety evaluation of civil aviation mobile applications.

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 20984 Information Security Technology Information Security Risk Assessment Specification
GB/T 25058 Information Security Technology Information System Security Level Protection Implementation Guide
GB/T 28448 Information Security Technology Information System Security Level Protection Evaluation Requirements
GB/T 31509 Information Security Technology Information Security Risk Assessment Implementation Guide

3 Terms and definitions

The following terms and definitions apply to this document.

Smart mobile terminal A mobile communication terminal product that is connected to the public mobile communication network, has an operating system, and can be installed and uninstalled by users by themselves.

[GB/T 34975-2017, definition 3.1] **3.2 Application software of smart mobile terminal**
Application software developed for mobile smart terminals, including third-party application software preset on mobile smart terminals, and Internet service Application programs provided by the provider that can be downloaded, installed, and upgraded through mobile application distribution platforms such as websites and application stores.

[GB/T 34975-2017, definition 3.3] **3.3 Civil aviation application program of smart mobile terminal**
Various mobile applications used to serve civil aviation passengers and to develop civil aviation's own business.

4.1 Identification

The identification requirements are as follows.

a) When logging in with a password, check the complexity of the user's authentication

information;

- b) When the user identification information is lost or invalid, the authentication information reset or other technical measures should be adopted to ensure system security;
- c) The user who logs in should be identified and authenticated. The identification is unique and the authentication information has complexity requirements;
- d) The civil aviation mobile application should provide and enable the login failure handling function, and take necessary protective measures after multiple login failures.

Shi;

- e) Two or more combinations of authentication technologies should be used for the same user to realize user identity authentication;
- f) When the user changes the mobile device, the legitimacy of the user's identity should be re-verified.

4.2 Access Control

The access control requirements are as follows.

- a) Necessary measures should be taken to restrict and protect account login;
- a) Only the necessary system permissions should be applied to prevent the risk of deduction and privacy leakage;
- b) Should meet the principle of minimum authorization, different user types (ordinary users, administrators, operators, auditors) and other roles the authority possessed is the minimum authority necessary for its operation;
- c) The civil aviation mobile application should not limit the user's authority only through the interface, and should prevent attackers from bypassing the interface restrictions directly.

Submit a request;

- d) All requests submitted by users and administrators should first be identified and verified to prevent unauthorized access.

4.3 Security Audit

The security audit requirements are as follows.

- a) The security audit function should be enabled, and the audit covers every mobile terminal, and important terminal behaviors and important security events are audited;
- b) It should be able to conduct individual behavior audit and data analysis of user behavior;
- c) The log retention period is not less than 6 months.

4.4 Protection of Sensitive Information

The sensitive information protection requirements are as follows.

- a) The instructions for using mobile application user data should be reviewed to determine the necessity of data collection and use;
- b) Cryptographic technology should be used to ensure the integrity of data during communication;
- c) Verification technology or cryptographic technology should be used to ensure the integrity of important data during storage, and necessary measures should be taken when integrity errors are detected.

Recovery measures;

- d) Checking technology should be used to ensure the integrity of the code;
- e) Encryption technology should be used to ensure the confidentiality of important data when stored locally;
- f) Important data between mobile applications should not be unauthorized interoperability;
- g) The storage space where the data files of the civil aviation mobile application are located should be completely cleared before being released or reallocated;
- h) Encrypt the sensitive information fields or the entire message in the communication process;
- i) The related cryptographic algorithms used for data storage and transmission shall comply with relevant national requirements.

4.5 Security of communication

The security requirements for communication are as follows.

- a) Encryption technology should be used to ensure the integrity of data during wireless communication;
- b) The confidentiality of sensitive information fields or the entire message should be guaranteed during wireless communication;
- c) The relevant cryptographic algorithms used in the wireless communication process should meet the relevant national requirements;

4.6 Software fault tolerance

Civil aviation mobile applications should be fault-tolerant.