GA

PUBLIC SECURITY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

GA 1280-2015

Security requirements for automatic teller machines

自动柜员机安全性要求

Issued on: October 28, 2015 **Implemented on: January 01, 2016**

Issued by: Ministry of Public Security of PRC

Table of contents

Foreword

Chapter 1 to Chapter 3 of this Standard, 4.4, 4.5, 4.10, 5.1.3, 5.2.6, 5.4.3, 5.5.3, 7.1.7, and Chapter 10 are recommended, AND the remainder are mandatory.

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

This standard was proposed by the Public Security Administration Bureau of the Ministry of Public Security.

This standard shall be under the jurisdiction of the National Security Alarm System Standardization Technical Committee (SAC/TC 100).

The drafting organizations of this standard: Public Security Administration Bureau of the Ministry of Public Security, the CBRC Security Bureau, GRG Banking Financial Electronics Co., Ltd., Beijing Telesound Electronics Co., Ltd., Eastern Communications Co., Ltd., Security and Police Electronic Product Quality Detection Center of the Ministry of Public Security, Industrial and Commercial Bank of China, Agricultural Bank of China, Bank of China, China Construction Bank.

The drafters of this standard are: Liu Wei, Yuan He, Yang Jianhua, Ren Ji, Xie Huachun, Bian Sanping, Wang Jianli, Liu Xu, Xing Weidong, Bao Shilong, Qiu Rixiang, Zhang Hongbin, Luo Panfeng, Xu Jun, Nie Rong, Ji Jinglin, Ye Zaiben.

Security requirements for automatic teller machines

1 Scope

This standard specifies the general requirements， the hardware modules, network access, operating systems, application systems and data security requirements, test methods and inspection rules of the automatic teller machine.

This standard applies to the design, production, inspection and acceptance of automatic teller machine security.

2 Normative references

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are applicable to this Standard.

GB10409 Burglary resistant safes

GB/T 18789.1-2013 Information technology - General specification for automated teller machine - Part 1: Device

GB/T 19584 Magnetic stripe data content and specification for bank card

GA 745 Regulations of security and protection for bank self-service equipment and self-service bank

JR/T 0002-2009 Specification on automatic teller machine (ATM) terminal for bank card

JR/T 0025.3 China financial integrated circuit (IC) card specifications - Part 3: Debit/credit application independent ICC to terminal interface requirements

JR/T 0025.11 China financial integrated circuit (IC) card specifications - Part 11: Contactless integrated circuit card communication specification

3 Terms, definitions and abbreviations

3.1 Terms and definitions

The following terms and definitions apply to this document.

3.1.1

Automatic teller machine

It refers to the self-service equipment, which integrates a variety of different financial business functions, through which customers can finish the bank counter services such as deposit, withdrawal, transfer, information inquiry and other agency business, including automatic teller machine AND cash recycling system.

3.1.2

Automatic teller machine control software

It refers to the control system software running at the automatic teller machine terminal equipment at the bottom of the terminal trading channel, through which the ATM components can be controlled. It is mainly used to provide customers and ATM equipment administrator with a variety of transaction and management interface, AND realizes certain functions together with the ATM front-end processing system through message exchange.

3.1.3

Automatic teller machine front-end processing system

It refers to, in case of dealing with online transactions, the processing system that is responsible for the communication between the ATM terminal and the ATM management center, which can receive, process and forward the transaction request information from the ATM terminal and the transaction result information from the management center.

3.1.4

Message

It refers to the data unit used for exchanging and transmission in the network.

3.1.5

4.6 Different ATM cabinet doors shall not use the same key, AND the different cabinet doors of the same ATM shall not use the same key.

4.7 ATM cabinet inside shall reserve the installation openings for the face surveillance camera and the cash deposit and withdrawal surveillance camera.

4.8 The surveillance cameras installed in ATM shall comply with the relevant requirements of GA 745.

4.9 ATM cabinet enclosure shall be made of steel plate of thickness greater than or equal to 1 mm.

4.10 ATM should support the national commercial password series algorithm.

4.11 ATM shall have the function of outputting the status information such as working normal and fault.

4.12 ATM with a cabinet door shall be installed with alarm detection device, to detect and alarm the abnormal door opening and closing. When the safe lock is opened, the ATM shall not enter service mode.

4.13 The card mouth shall have the function of preventing from illegal installation of reading device, detecting the illegal installation of reading device, AND issuing alarm.

5 Hardware module security requirements

5.1 Card reader module

5.1.1 The card reader module shall have the function of returning card in case of power failure.

5.1.2 Contact card reader module shall have the card retention function, during which it shall produce a fault signal.

5.1.3 Contact card reader module should have the jitter card feeding function.

5.1.4 Contact IC card reader module shall comply with the relevant provisions of JR/T 0025.3, the contactless IC card reader module shall comply with the relevant provisions of JR/T 0025.11, AND the magnetic stripe card reader module shall comply with the relevant provisions of GB/T 19584.

5.2 Cash dispense module

5.2.1 It shall have the function of rejecting unauthorized instructions.

5.5.1 The anti-destructive capacity of the safe shall comply with the requirements of C.3 in Appendix C of GB/T 18789.1-2013. The safe door shall have safety locking device, AND the number of such safety locking devices and the safety locking directions shall be not less than 2. The other requirements of the safe shall comply with the relevant provisions of GB 10409.

5.5.2 The safe shall have a device and fittings fixed to the ground, AND the fixation and connection devices shall be not less than 4, with the diameter of the fittings greater than or equal to 12 mm.

5.5.3 The safe should be added with dynamic electronic password lock.

5.5.4 The inside of the safe door shall be installed with temperature sensor, to conduct detection and alarming for the conditions when the temperature is greater than or equal to 70 °C.

5.6 Encrypting PIN pad module

Encrypting PIN pad module shall simultaneously comply with the PCI-EPP requirements AND the China UnionPay card acceptance terminal PIN input device safety assessment requirements.

6 Network access security requirements

6.1 Access control

6.1.1 When ATMC registers for the first time, it shall provide identity validity verification information to ATMP.

6.1.2 ATM shall have a network access control mechanism, AND conduct identity validity verification of the terminal devices accessing the ATM through network.

6.2 Intrusion prevention

ATM shall have intrusion prevention mechanism. In case of detecting the network attack, it shall record the attack address, time, type and other information, AND take the initiative to prevent transactions and other means of protection.

6.3 Transmission security

The communication data transmission security from ATMC to ATMP shall comply with the following requirements:

7.3.2 Remote login control

It shall turn off the operating system remote login service.

7.3.3 Password policy

7.3.3.1 It shall set a unique initial password for each user, AND prompt the user to change it after first use. It shall authenticate the user identity before performing a password reset.

7.3.3.2 It shall have a policy mechanism for the maximum service life of the set password.

7.3.3.3 It shall have a policy mechanism for the controlling of password complexity requirements, including:

a) It shall not contain the user name or the part of the user name which exceeds two consecutive characters;

b) It shall be at least 6 characters long;

c) It shall contain three types of characters in the following four categories of characters: English capital letters, lowercase letters, 10 basic numbers or characters (for example: !, $, #, %).

7.3.3.4 It shall have a mandatory password history policy mechanism, AND it is not allowed for the submitted new password to be same as the recently used four passwords.

7.3.4 File/file directory protection

It shall conduct security reinforcement against the operating system, protect the designated file/file directory, AND prevent the unauthorized addition, deletion, or modification.

7.3.5 Registry protection

It shall conduct security reinforcement against the operating system, conduct access control against the designated registry entry, AND prevent the unauthorized addition, deletion, or modification.

7.3.6 Storage media management

It shall conduct access authorization management against the external storage device, AND it shall not recognize the unauthorized external storage device.

8.4.4 It shall have the function of the data statistics, query, and analysis of the log records.

8.4.5 Logs shall not contain sensitive information such as complete track data (or IC card equivalent data), PIN, card verification code, etc. of the magnetic stripe card.

8.5 Residual information protection

The application system shall have the residual information protection mechanism, AND the user authentication information which is no longer used in memory shall be erased.

9 Data security requirements

9.1 Data confidentiality

9.1.1 It shall perform encryption protection on the key data such as ATM serial number, transaction amount, MAC check code, and so on.

9.1.2 Key management shall comply with the relevant provisions of JR/T 0002-2009.

9.2 Customer information security

9.2.1 Account information security

9.2.1.1 ATM shall correctly read the bank card information in sequence, and can accurately identify the main account in accordance with the relevant provisions of GB/T 19584.

9.2.1.2 It shall perform encrypt protection on the second track data (or IC card equivalent second track data) information as specified in GB/T 19584, AND perform the hard encryption process by the encrypting PIN pad.

9.2.2 PIN security

9.2.2.1 When entering a PIN during a transaction, a meaningless character (such as an asterisk) or an indistinguishable signal shall be displayed, AND the length of the supported input PIN shall be at least 4 digits.

9.2.2.2 It shall perform encrypt protection on the PIN information, AND perform the hard encryption process by the encrypting PIN pad.

9.2.3 Card number printing

10.2.7 CHECK whether the ATM cabinet is reserved with the installation openings for the face surveillance camera and the deposit and withdrawal cash surveillance camera; JUDGE whether it complies with the requirements of 4.7.

10.2.8 In accordance with the relevant requirements of GA 745, TEST the function and performance of the camera installed on the ATM; JUDGE whether it complies with the requirements of 4.8.

10.2.9 USE a caliper of precision 0.02 mm to measure the thickness of the steel plate; JUDGE whether it complies with the requirements of 4.09.

10.2.10 In accordance with the third party inspection report or related supporting materials provided by the manufacturer, VERIFY whether the ATM supports the national commercial password series algorithm; JUDGE whether it complies with the requirements of 4.10.

10.2.11 Respectively MAKE the encrypting PIN pad, card reader, cash dispense module, and cash deposit module at the normal state and the non-connected state; CHECK the status information of ATM output; JUDGE whether it complies with the requirements of 4.11.

10.2.12 CHECK whether the ATM cabinet door is equipped with alarm detection device, VERIFY whether it detects and alarms on the abnormal door opening and closing; MAKE the safe lock open, CHECK whether the ATM is under service mode; JUDGE whether it complies with the requirements of 4.12.

10.2.13 USE a metal blank with a length greater than or equal to 70 mm and a width greater than or equal to 20 mm to cover the ATM card mouth, with a distance from the metal blank to the ATM card mouth less than 50 mm; COVER each side for 60 s, to check whether it alarms; JUDGE whether it complies with the requirements of 4.13.

10.3 Hardware module security requirements inspection

10.3.1 Card reader module inspection

10.3.1.1 INSERT a bank card and PERFORM power failure operation; JUDGE whether it complies with the requirements of 5.1.1.

10.3.1.2 In the online state, artificially SIMULATE the card retention operation; JUDGE whether it complies with the requirements of 5.1.2.

10.3.1.3 In the online state, OBSERVE the card feeding effect; JUDGE whether it complies with the requirements of 5.1.3.

10.3.3.5 CHECK the internal structure; CONDUCT the returned deposit cash non-collection test and the make the counterfeit cash deposit test; CHECK whether the function is normal; deposit return and the counterfeit banknotes check, check whether the function is normal; JUDGE whether it complies with the requirements of 5.3.5.

10.3.4 Cash cycling module inspection

10.3.4.1 CONDUCT test in accordance with the test method of 10.3.2; JUDGE whether it complies with the requirements of 5.4.1.

10.3.4.2 CONDUCT test in accordance with the test method of 10.3.3; JUDGE whether it complies with the requirements of 5.4.2.

10.3.4.3 PLACE counterfeit cash into the cash box; CONDUCT cash withdrawal test; JUDGE whether it complies with the requirements of 5.4.3.

10.3.5 Safe inspection

10.3.5.1 CHECK the transmission mechanism, installation structure and lock configuration of the ATM; CONDUCT the anti-damage capability test on the safe in accordance with C.3 of Appendix C in GB/T 18789.1-2013 and GB10409; JUDGE whether it complies with the requirements of 5.5.1.

10.3.5.2 CHECK the number of fixed connection devices for the safe and MEASURE the diameter of the accessory; JUDGE whether it complies with the requirements of 5.5.2.

10.3.5.3 CHECK the lock configuration of the safe; JUDGE whether it complies with the requirements of 5.5.3.

10.3.5.4 USE the heating device to heat the position near the temperature sensor contact on the door. When the temperature reaches 70 °C, CHECK the alarm status of the sensor; JUDGE whether it complies with the requirements of 5.5.4.

10.3.6 Encrypting PIN pad module inspection

CHECK the PCI-EPP certification document of the encrypting PIN pad AND the China UnionPay card acceptance terminal PIN input device safety assessment document; JUDGE whether it complies with the requirements of 5.6.

10.4 Network access security requirements inspection

10.4.1 Access control inspection

10.5.1.5 EVALUATE the security policy configuration list of the ATM operating system as provided by the manufacturer; LOG in the ATM operating system to check the security configurations; JUDGE whether the results comply with the requirements of 7.1.5.

10.5.1.6 USE tools to directly modify the BIOS configuration data or CONDUCT discharge operation against the CMOS; CHECK whether the ATM can automatically restore the BIOS configuration to the factory settings; JUDGE whether the results comply with the requirements of 7.1.6.

10.5.1.7 CHECK whether ATM installs and enables firewall and antivirus software; JUDGE whether the results comply with the requirements of 7.1.7.

10.5.2 Operating system security audit inspection

CHECK the ATM operating system log; CHECK whether the log category includes login success and failure AND whether the log content includes user login time, login mode, login results and other information; JUDGE whether the results comply with the requirements of 7.2.

10.5.3 Operating system access control inspection

10.5.3.1 Guest account access control inspection

TURN on the ATM to verify the operation; CHECK whether the Guest account has been disabled; JUDGE whether the results comply with the requirements of 7.3.1.

10.5.3.2 Remote login control inspection

TURN on the ATM to verify the operation; CHECK whether the operating system remote login service has been closed; JUDGE whether the results comply with the requirements of 7.3.2.

10.5.3.3 Password policy inspection

10.5.3.3.1 TURN on the ATM to verify whether the operating system authenticates the user after the password reset by the user, whether the operating system sets a unique initial password for each user, AND prompts the user to change it after the initial use; JUDGE whether the results comply with the requirements of 7.3.3.1.

10.5.3.3.2 CHECK the password security policy configuration of the operating system; FOLLOW the password security policy to conduct actual operation; JUDGE whether the results comply with the requirements of 7.3.3.2 ~ 7.3.3.4.

EVALUATE the development documents of the product; CHECK whether the ATM has the mechanism of daily time synchronization with the ATMP; in the online state, MODIFY the ATM clock to check whether the time synchronization mechanism is valid; JUDGE whether the results comply with the requirements of 8.2.

10.6.3 Application system access control inspection

10.6.3.1 In the online state, USE the users of different rights to log in the background maintenance interface to verify whether the application system has the function of accessing the background function resources in accordance with the user role; JUDGE whether the results comply with the requirements of 8.3.1.

10.6.3.2 In the online state, CHECK whether the application system user authorization module provides the configuration access control policy function to the administrator; JUDGE whether the results comply with the requirements of 8.3.2.

10.6.3.3 In the online state, CHECK the user authorization of the application system; JUDGE whether the results comply with the requirements of 8.3.3.

10.6.4 Application system log inspection

10.6.4.1 EVALUATE the development documents of the product; CHECK whether the security audit functions of the system covers all users, without any unaudited super users; VERIFY whether such important safety events as user login success, login failure, password modification, new user creation, and log off, etc., are recorded in the corresponding application system log; JUDGE whether the results comply with the requirements of 8.4.1.

10.6.4.2 EVALUATE the development documents of the product; USE the administrator account to log in to the application system to check whether the application system does not have the function of closing the logging module. USE the administrator accounts of different roles to login the application system; CHECK whether no user can delete/modify the application system log record in the application system; JUDGE whether the results comply with the requirements of 8.4.2.

10.6.4.3 CHECK the application system log content to confirm whether it includes the date, time, originator information, type, description and result fields of the event; JUDGE whether the results comply with the requirements of 8.4.3.

10.6.4.4 EVALUATE the development documents of the product; USE the administrator account to log in to the application system to check whether the

10.7.2.2 PIN security inspection

10.7.2.2.1 In the online state, when the PIN is entered, CHECK whether the ATM screen displays meaningless characters (such as asterisks) or non-distinguishing characters. CHECK whether the length of the input PIN as supported by ATM is not less than 4 digits; JUDGE whether the results comply with the requirements of 9.2.2.1.

10.7.2.2.2 EVALUATE the development documents of the product; CHECK whether the PIN information is encrypted and protected during the transmission process, AND whether it has hardware encryption through the encrypting PIN pad; JUDGE whether the results comply with the requirements of 9.2.2.2.

10.7.2.3 Card number printing inspection

EVALUATE the development documents of the product; in the online state, SIMULATE such operations as transfer, deposit, withdrawal, and inquiry; and continuously INPUT wrong password to make the ATM retain the card; CHECK the transaction voucher as printed from the ATM; JUDGE whether the results comply with the requirements of 9.2.3.

11 Inspection rules

11.1 Inspection Classification

Automatic teller machine product inspection is divided into type inspection and exit-factory inspection.

11.2 Type inspection

11.2.1 Type inspection shall be carried out in any of the following cases:

a) In case of new product design finalized or production type finalized;

b) When the major change of material, structure or production technology as well as the change of ATM key hardware module (card reader module, cash dispense module, deposit module, cash recycling module, safe, encrypting PIN pad module) may affect the security performance;

c) In case of the initial production of product OR the production restoration after production suspension for one year;

d) In case of periodic inspection which shall be conducted after accumulating a certain amount of production;

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------