YD

COMMUNICATION INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 33.060

M 36

YD/T 2407-2013

Technical requirements for security capability of smart mobile terminal

(ITU-T X.msec-6:2012, Security aspects of smartphones, NEQ)

移动智能终端安全能力技术要求

Issued on: April 25, 2013 **Implemented on: November 1, 2013**

Issued by: Ministry of Industry and Information Technology of the People 's Republic of China

Table of Contents

Foreword

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

This Standard uses redrafting method to modify and adopt ITU-T X.msec-6:2012 *Security aspects of smartphones*, a related advice of International Telecommunication Union (ITU). It is inequivalent to ITU-T X.msec-6.

This Standard is one of the series of mobile intelligent terminal security series. The names and structures of this series are expected to be as follows:

a) *Guidelines for the design for security capability of smart mobile terminal*;

b) YD/T 2407-2013, *Technical requirements for security capability of smart mobile terminal*;

c) YD/T 2408-2013, *Test methods for security capability of smart mobile terminal*;

d) YD/T 1886-2009, *Security requirements and test specification for SoC in mobile terminal*.

This Standard was proposed by and shall be under the jurisdiction of China Communications Standardization Association.

The drafting organizations of this Standard: Ministry of Industry and Information Technology, Beijing Spreadtrum Hi-Tech Communications Technology Co., Ltd., Datang Telecom Technology & Industry Group.

Main drafters of this Standard: Pan Juan, Kuang Xiaoxuan, Luo Hongwei, Wang Kun, Li Yunfan, Yu Lu, Yuan Guangxiang, He Guili, Shi Denian, Li Wei, Yu Huawei, Li Jianwei, Li Qian.

Introduction

With the extensive application of smart mobile terminals and the continuous expansion of functions, the security issues during the use are concerned by more and more users. In recent years, security incidents such as malicious charge, eavesdropping, theft record, location information leakage make user worry about the security of smart mobile terminals, which shall affect the development of smart mobile terminals and mobile Internet applications. The purpose of this Standard is to improve the smart mobile terminal's own security protection, to prevent a variety of security threats on smart mobile terminals, to protect users from interest damage, while preventing adverse effects on mobile communication network security caused by smart mobile terminals.

The basic principle of this Standard is that the behavior and application on smart mobile terminal shall be in line with the user's wishes. This Standard does not specify specific implementation methods and measures to facilitate innovation and development. This Standard specifies the requirements to the security capability of smart mobile terminal, from five aspects: hardware security capability requirements, operating system security capability requirements, peripheral interface security capability requirements, application software security requirements, and user data security protection requirements. And it grades the security capability from basic security protection, difficulty of achievement, special security capability, so as to make the product has a specific quality, make it easy for consumer to choose. This Standard not only guides smart mobile terminals to preset application software more standardized and safer, but also guides smart mobile terminals to improve their own security capabilities, which shall make them perform security control on the third-party applications downloaded latter. Meanwhile, it can also prevent security impact on network caused by the preset malicious codes in smart mobile terminals.

Technical requirements for security capability of smart mobile terminal

1 Scope

This Standard specifies the technical requirements for security capability of smart mobile terminal, including hardware security capability of smart mobile terminal, operating system security capability of smart mobile terminal, peripheral interface security capability of smart mobile terminal, application layer security requirements of smart mobile terminal, user data protection security capability of smart mobile terminal, etc. And it also grades the security capability.

This Standard is applicable to various formats of smart mobile terminals. Individual terms do not apply to special industries, professional applications. Other terminals shall also refer to use.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

YD/T 1699-2007, *Information security technical specification for mobile terminal*

YD/T 1760-2012, *Technical requirements for data exchange via peripheral interface of mobile terminal*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1 Smart Mobile Terminal

an open operating system capable of accessing a mobile communication network, capable of providing an application development interface, and a

mobile terminal capable of installing and operating a third-party application software

3.1.2 Security Capability

technical means that can be achieved in smart mobile terminal and can prevent security threats

3.1.3 User

an object that uses smart mobile terminal's resources, including human or third-party applications

3.1.4 User Data

personal information stored on smart mobile terminal, including data generated locally by user, locally generated data for user, data coming into user data area from the outside after user's permission, etc.

3.1.5 Authorization

a process of granting user the appropriate authority according to pre-set security policy after user's identity is certified

3.1.6 Digital Signature

data attached to data unit, or data obtained by cryptographic transformation of data unit; allowing the recipient of data to verify the source and integrity of data, protecting data from being tampered, forged, and ensuring that data is undeniable

3.1.7 Code Signature

a mechanism that uses a digital signature mechanism to sign all or part of a code by an entity with signed permission

3.1.8 Operator System of Smart Mobile Terminal

the most basic system software of smart mobile terminal; it controls and manages various hardware and software resources of smart mobile terminal and provides application development interfaces

3.1.9 Malicious Charge

user economic losses caused by application software on the terminal without knowledge or authorization of user

3.2 Abbreviations

- confirm every call of application software;
- confirm the first call of application software; this confirmation shall be valid for a certain period of time and the confirmation shall be carried out separately for each call;
- confirm the first installation or call of application software; this confirmation shall be valid for long term and the confirmation shall be carried out separately for each call.

The user's prompts and user confirmation mentioned in this Clause refer to the capabilities that the operating system shall have when a third-party application calls related functions. For a third-party application, the operation performed by the person-machine interface provided by the calling operating system is deemed as an operation performed at the user's knowledge, and the user has been prompted, it has been confirmed by the user.

For operations that are set to allow access in the security configuration of application software, it is considered that the operation performed by the user is informed and has been confirmed by the user.

For mobile communication network connection, WLAN connection, opening of wireless peripheral interface in any case shall be prompted to the user and confirmed by the user.

The security capability requirements referred in 5.3 and 5.4 are only applicable to the situation where a third-party application calls corresponding functions provided by the operating system. The application software referred in 5.5.1, 5.5.2 and 5.5.3 are non-preset.

5.2 Hardware security capability requirements of smart mobile terminal

If the smart mobile terminal’s hardware provides a remote operation means, the smart mobile terminal shall protect its remote operation means so as to prevent the remote operation from malicious use.

5.3 Operating system security capability requirements of smart mobile terminal

5.3.1 Security call control capability

5.3.1.1 Communication function control mechanism

The operating system of smart mobile terminal shall provide user data protection function to protect the phone book data, call records, SMS data, MMS data. The specific requirements are as follows:

a) when the application software calls to write user data, the smart mobile terminal shall execute it after it is confirmed by user;

b) when the application software needs to call the user data read operation, the application software shall prompt the user that the application is going to read these user data during download, installation or the first run.

5.3.2 Operating system update

The smart mobile terminal usually performs the authorized operating system update. When it cannot guarantee the update of the operating system security, the possible security risks to the user shall be indicated in the instructions for use.

5.4 Peripheral interface security capability requirements of smart mobile terminal

5.4.1 Security capability requirements for wireless peripheral interface

5.4.1.1 Wireless peripheral interface on / off controlled mechanism

The smart mobile terminal with Bluetooth, NFC functions shall have a switch that can turn on / off the wireless connection supported by Bluetooth, NFC or other terminal.

When the application software calls to open the wireless peripheral interface, the smart mobile terminal shall give user the corresponding prompt. It shall start the connection after it is confirmed by user.

5.4.1.2 Confirmation mechanism established by wireless peripheral interface connection

When the first connection is made via a wireless peripheral interface (Bluetooth only) with different devices, the smart mobile terminal shall be able to discover the connection and give the user a corresponding prompt. The connection shall be established after user confirms.

Example: Bluetooth pairing mechanism.

5.4.1.3 Wireless peripheral interface connection state prompt

mode), it shall provide access control mode.

5.5 Application layer security requirements of smart mobile terminal

5.5.1 Security configuration capability requirements for application software

The smart mobile terminal can provide the mechanism to configure the calling behavior of the installed third-party application software, including the controls of making calls, initiating the three-way call, sending SMS, sending MMS, calling the mobile communication network data connection, calling the positioning function, local recording, photographing / camera shooting, access to phone book, access to call records, access to SMS and access to MMS.

The controls of the above calling behaviors shall at least have two states: allowing and prohibiting. It is recommended to use three states: allowing, asking the user for each call and prohibiting. If the smart mobile terminal can support the configurations of the above three or more call behaviors, it shall be regarded as meeting the application software security configuration requirements.

5.5.2 Security authentication mechanism requirements for application software

5.5.2.1 Noncertified signature requirements

If the smart mobile terminal supports software downloading and application for unauthorized signatures, the smart mobile terminal shall be able to recognize the signature status of the application software during the installation of the application software and be able to give the user a corresponding prompt according to the signature status.

5.5.2.2 Certified signature requirements

If the smart mobile terminal adopts the authentication signature mechanism, in this case, the application software without the authentication signature shall only perform the next operation after it is confirmed by user.

5.5.3 Mobile communication network boot self-start program monitoring capability

If the smart mobile terminal has capability of a third-party application boot self-start program, it shall be able to browse and configure whether the application boots self-start.

5.6 Requirements for security protection capability of smart mobile terminal user data

5.6.1 Password protection of smart mobile terminal

The smart mobile terminal shall support password protection during power-on and password protection during boot-up, such as passwords, patterns, biometrics, and other forms of password. And the password is a required form of protection, and the other forms are optional. See 5.5.2.1 of YD/T 1699-2007 for password certification requirements. See 5.5.2.3 of YD/T 1699-2007 for biometric certification requirements.

5.6.2 Authorization access for user data in file

The smart mobile terminal provides authorized access to user data in file. When a third-party application accesses to the protected user data, it shall be confirmed by user. User data in file includes pictures, videos, audios and documents.

5.6.3 Encrypted storage of user data

Any unauthorized entity shall not be able to restore the actual content of the user's private data from the data of the encrypted storage area of the smart mobile terminal.

5.6.4 Complete removal of user data

The smart mobile terminal provides a function to completely delete data so as to ensure that the deleted user data cannot be restored. The general delete function shall only delete the index for data placed in the storage device location. But the data that is actually stored in this area is not completely emptied. After the data is deleted, it is still possible for an illegal program to restore the deleted private data it reads through reading the contents of this area. The complete deletion function shall completely eliminate the actual stored data in this area. For example, when the end user data is deleted, multiple padding shall be performed by using the full "0" or full "1" in the memory area corresponding to the data.

5.6.5 Remote protection of user data

The smart mobile terminal shall provide remote protection of user data so that the user's data in the terminal shall not be disclosed when the user’s cell phone is lost or in any other cases. Remote protection capability includes remote locking of smart mobile terminal and remote destruction of user data. The remote protection provided by the smart mobile terminal shall also have

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

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