

Translated English of Chinese Standard: YD/T2408-2013

www.ChineseStandard.net

Sales@ChineseStandard.net

YD

COMMUNICATIONS INDUSTRY STANDARD
OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 33.060

M 36

YD/T 2408-2013

Test methods for security capability of smart mobile terminal

移动智能终端安全能力测试方法

YD/T 2408-2013 How to BUY & immediately GET a full-copy of this standard?

1. www.ChineseStandard.net;
2. Search --> Add to Cart --> Checkout (3-steps);
3. No action is required - Full-copy of this standard will be automatically & immediately delivered to your EMAIL address in 0~25 minutes.
4. Support: Sales@ChineseStandard.net. Wayne, Sales manager

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	3
Introduction	4
1 Scope	5
2 Normative references	5
3 Terms, definitions and abbreviations	5
4 Test methods for security capability of smart mobile terminal.....	7
5 Test methods for functional restrictive requirements of smart mobile terminal	44
Reference	47

Foreword

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

This Standard is one of the smart mobile terminal's security series standards. The names and structure of this series of standards are expected to be as follows:

- a) *Design guidance 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;* and
- d) YD/T 1886-2009 *Security requirements and test specification for system on chip in mobile terminal.*

This Standard shall be used in conjunction with the *Technical requirements for security capability of smart mobile terminal.*

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

Drafting organizations of this Standard: China Academy of Telecommunication Research of MIIT, Spreadtrum Communications, Inc. (Beijing), and 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 and Li Xi.

Test methods for security capability of smart mobile terminal

1 Scope

This Standard specifies the test methods for security capability of smart mobile terminal, including the test methods for security capability of smart mobile terminal's hardware, the test methods for security capability of smart mobile terminal's operator system, the test methods for security capability of smart mobile terminal's peripheral interface, the test methods for security capability of smart mobile terminal's application layer, the test methods for security capability of smart mobile terminal's user data protection, etc.

This Standard **is applicable to** various types of smart mobile terminal. Individual terms do not apply to special industries and professional applications. Other terminals shall use this Standard for reference only.

2 Normative references

The following documents are essential to the application of this document. For dated references, only the editions with the dates indicated are applicable to this document. For undated references, only the latest editions (including all the amendments) are applicable to this document.

YD/T 1886 *Security requirements and test specification for system on chip in mobile terminal*

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

3 Terms, definitions and abbreviations

3.1 Terms and definitions

The following terms and definitions are applicable to this document.

3.1.1 Smart mobile terminal

It refers to the mobile terminal that has the ability to access a mobile communication network, an open operator system that is able to provide an

application development interface, and the ability to install and run the third-party applications.

3.1.2 Security capability

It refers to the technical means that can be achieved on smart mobile terminal and are able to prevent security threats.

3.1.3 User

An object that uses the smart mobile terminal resources, including the human beings or third-party applications.

3.1.4 User data

Personal user information stored on smart mobile terminal, including the data generated locally by the users, data generated locally for the users, data entering the user data area externally after approved by the users, etc.

3.1.5 Authorization

It refers to the process of granting the user the corresponding permissions in accordance with the preset security policy, after the user identity is authenticated.

3.1.6 Digital signature

It refers to the data attached to the data unit, or the data obtained by cryptographic transformation of the data unit. Data receivers are allowed to verify the source and integrity of the data, to protect data from being tampered with and forged, and to ensure the non-repudiation of the data.

3.1.7 Code signature

It refers to a mechanism that uses a digital signature mechanism to sign all or part of a code by an entity with signature authority.

3.1.8 Operator system of smart mobile terminal

It refers to the most basic system software of smart mobile terminal, which is able to control and manage various hardware and software resources of smart mobile terminal, and to provide the interface of application development.

3.2 Abbreviations

The following abbreviations are applicable to this document.

Test item: Controlled mechanism for short message sending
Item requirements: SEE Section 5.3.1.1.3 of YD/T 2407-2013.
Preconditions: The smart mobile terminal to be tested is under normal operating condition.
Test steps: Step 1: CHECK whether the operator system of the smart mobile terminal to be tested provides the development function of short message sending; Step 2: If the operator system of smart mobile terminal provides the development function of short message sending, USE this function to develop a short message sending application; Step 3: RUN this application to see whether the terminal requires the user to validate the short message sending.
Expected results: After Step 1, if the operator system of smart mobile terminal fails to provide the development function of short message sending, this item will be evaluated as “no abnormality”, and the evaluation will end; After Step 3, if smart mobile terminal requires the user to validate, this item will be evaluated as “no abnormality”, and the evaluation will end; After Step 3, if smart mobile terminal does not require the user to validate and successfully sends a short message, this item will be evaluated as “not satisfiable”, and the evaluation will end.

4.3.1.1.4 Controlled mechanism for multimedia message sending

Test No.: 4.3.1.1.4
Test item: Controlled mechanism for multimedia message sending
Item requirements: SEE Section 5.3.1.1.4 of YD/T 2407-2013.
Preconditions: The smart mobile terminal to be tested is under normal operating condition.
Test steps: Step 1: CHECK whether the operator system of the smart mobile terminal to be tested provides the development function of multimedia message sending; Step 2: If the operator system of smart mobile terminal provides the development function of multimedia message sending, USE this function to develop a multimedia message sending application; Step 3: RUN this application to see whether the terminal requires the user to validate the multimedia message sending.
Expected results: After Step 1, if the operator system of smart mobile terminal fails to provide the development function of multimedia message sending, this item will be evaluated as “no abnormality”, and the evaluation will end; After Step 3, if smart mobile terminal requires the user to validate, this item will be evaluated as “no abnormality”, and the evaluation will end;

Expected results:

After Step 1, the ON / OFF switch for data connection in mobile communication network shall be able to be discovered on smart mobile terminal;

After Step 2, the data connection in mobile communication network of the smart mobile terminal to be tested will be successfully enabled;

After Step 3, the data connection in mobile communication network of the smart mobile terminal to be tested will be successfully disabled.

If smart mobile terminal meets the above expected results, this item will be evaluated as “no abnormality”, otherwise it will be evaluated as “not satisfiable”.

Test No.: 4.3.1.1.6.2

Test item: Controlled mechanism for enabling / disabling of data connection in mobile communication network

Item requirements: SEE Section 5.3.1.1.6 of YD/T 2407-2013.

Preconditions: The data connection in mobile communication network of the smart mobile terminal to be tested is in OFF state.

Test steps:

Step 1: CHECK whether the operator system of the smart mobile terminal to be tested provides the development function of data connection enabling / disabling in mobile communication network;

Step 2: If the operator system of smart mobile terminal provides the development function of data connection enabling / disabling in mobile communication network, USE this function to develop an application for enabling / disabling of data connection in mobile communication network;

Step 3: RUN this application to enable the data connection in mobile communication network, and to see whether the terminal requires the user to validate the enabling of data connection in mobile communication network.

Expected results:

After Step 1, if the operator system of smart mobile terminal fails to provide the development function of data connection enabling in mobile communication network, this item will be evaluated as “no abnormality”, and the evaluation will end;

After Step 3, if smart mobile terminal requires the user to validate the enabling of data connection in mobile communication network, this item will be evaluated as “no abnormality”, and the evaluation will end;

After Step 3, if smart mobile terminal does not require the user to validate and successfully enables the data connection in mobile communication network, this item will be evaluated as “not satisfiable”, and the evaluation will end.

Step 2: USE the switch on the operator system of smart mobile terminal to disable the WLAN connection;

Step 3: If the operator system of smart mobile terminal provides the development function of WLAN connection enabling, RUN the application for WLAN connection enabling developed in 4.3.1.1.6.2 [Translator note: 4.3.1.1.7.2?];

Step 4: RUN the application for WLAN connection disabling.

Expected results:

Before Step 1, smart mobile terminal shall provide the user with the status prompt for WLAN connection disabling on the main user interface;

After Step 1, smart mobile terminal shall provide the user with the status prompt for WLAN connection enabling on the main user interface;

After Step 2, smart mobile terminal shall provide the user with the status prompt for WLAN connection disabling on the main user interface;

After Step 3, smart mobile terminal shall provide the user with the status prompt for WLAN connection enabling on the main user interface;

After Step 4, smart mobile terminal shall provide the user with the status prompt for WLAN connection disabling on the main user interface.

If smart mobile terminal meets the above expected results, this item will be evaluated as “no abnormality”, otherwise it will be evaluated as “not satisfiable”.

Test No.: 4.3.1.1.7.4
Test item: Status prompt for data transmission via WLAN
Item requirements: SEE Section 5.3.1.1.7 of YD/T 2407-2013.
Preconditions: The WLAN connection of the smart mobile terminal to be tested is in ON state.
Test steps: Step 1: RUN the preset application software on smart mobile terminal for data transmission via WLAN; Step 2: DISABLE the running software; Step 3: RUN the third-party application software for data transmission via WLAN.
Expected results: Before Step 1, smart mobile terminal shall provide the user with the status prompt for data connection enabling in WLAN on the main user interface; After Step 1, smart mobile terminal shall provide the user with the status prompt for data transmission via WLAN on the main user interface; After Step 2, smart mobile terminal shall provide the user with the status prompt for data connection enabling in WLAN on the main user interface; After Step 3, smart mobile terminal shall provide the user with the status prompt for data transmission via WLAN on the main user interface.

Before Step 1, there shall be no status prompt of “positioning function has been called” on the main user interface of smart mobile terminal;
 After Step 1, smart mobile terminal shall present the user with the status prompt of “positioning function has been called” on the main user interface;
 After Step 2, there shall be no status prompt of “positioning function has been called” on the main user interface of smart mobile terminal.
 If smart mobile terminal meets the above expected results, this item will be evaluated as “no abnormality”, otherwise it will be evaluated as “not satisfiable”.

4.3.1.2.2 Controlled mechanism for the call recording function

Test No.: 4.3.1.2.2
Test item: Controlled mechanism for the enabling of the call recording function
Item requirements: SEE Section 5.3.1.2.2 of YD/T 2407-2013.
Preconditions: The smart mobile terminal to be tested is under normal operating condition.
Test steps: Step 1: CHECK whether the operator system of the smart mobile terminal to be tested provides the development function of call recording; Step 2: If the operator system of smart mobile terminal provides the development function of call recording, USE this function to develop a call recording application; Step 3: During calling, RUN this application for call recording, and SEE whether the terminal requires the user to validate to start the call recording.
Expected results: After Step 1, if the operator system of smart mobile terminal fails to provide the development function of call recording, this item will be evaluated as “no abnormality”, and the evaluation will end; After Step 3, if smart mobile terminal requires the user to validate to start the call recording, this item will be evaluated as “no abnormality”, and the evaluation will end; After Step 3, if smart mobile terminal does not require the user to validate and successfully performs the call recording, this item will be evaluated as “not satisfiable”, and the evaluation will end.

4.3.1.2.3 Controlled mechanism for the local recording function

Test No.: 4.3.1.2.3
Test item: Controlled mechanism for the enabling of the local recording function
Item requirements: SEE Section 5.3.1.2.3 of YD/T 2407-2013.
Preconditions: The smart mobile terminal to be tested is under normal operating condition.

After Step 4, if smart mobile terminal requires the user to validate the camera or filming operation, this item will be evaluated as “no abnormality”, and the evaluation will end;
After Step 3, if smart mobile terminal does not provide the user with any prompt, this item will be evaluated as “not satisfiable”, and the evaluation will end.

4.3.1.2.5 Controlled mechanism for the operations of user data

Test No.: 4.3.1.2.5.1

Test item: Controlled mechanism for the phonebook data write and delete operations

Item requirements: SEE Section 5.3.1.2.5 of YD/T 2407-2013.

Preconditions: The smart mobile terminal to be tested is under normal operating condition.

Test steps:

Step 1: CHECK whether the operator system of the smart mobile terminal to be tested provides the development function of phonebook data write and delete operations;

Step 2: If the operator system of smart mobile terminal provides the development function of phonebook data write and delete operations, USE this function to develop an application for the phonebook data write and delete operations;

Step 3: RUN the application for phonebook writing, and SEE whether the terminal requires the user to validate the write operation to the phonebook;

Step 4: RUN the application for phonebook delete, and SEE whether the terminal requires the user to validate the delete operation to the phonebook.

Expected results:

After Step 1, if the operator system of smart mobile terminal fails to provide the development function of phonebook data write and delete operations, this item will be evaluated as “no abnormality”, and the evaluation will end;

After Step 3, if smart mobile terminal requires the user to validate the write operation to the phonebook, this item will be evaluated as “no abnormality”, and the evaluation will end;

After Step 3, if smart mobile terminal does not require the user to validate and successfully performs the write operation to the phonebook, this item will be evaluated as “not satisfiable”, and the evaluation will end;

After Step 4, if smart mobile terminal requires the user to validate the delete operation to the phonebook, this item will be evaluated as “no abnormality”, and the evaluation will end;

After Step 4, if smart mobile terminal does not require the user to validate and successfully performs the delete operation to the phonebook, this item will be evaluated as “not satisfiable”, and the evaluation will end.

Step 3: INSTALL and RUN an application that is able to read the phonebook data, and CHECK whether any prompts are provided for the user during the program installation or first run.

Expected results:

After Step 1, if the operator system of smart mobile terminal fails to provide the development function of phonebook data read operations, this item will be evaluated as “no abnormality”, and the evaluation will end;

After Step 3, if smart mobile terminal provides the user with the prompt that this program will access to the user’s phonebook data, this item will be evaluated as “no abnormality”, and the evaluation will end;

After Step 3, if smart mobile terminal does not provide the user with any prompts, and if the program is able to perform the read operation to the user’s phonebook, this item will be evaluated as “not satisfiable”, and the evaluation will end.

Test No.: 4.3.1.2.5.6

Test item: Controlled mechanism for the call record read operations

Item requirements: SEE Section 5.3.1.2.5 of YD/T 2407-2013.

Preconditions: The smart mobile terminal to be tested is under normal operating condition.

Test steps:

Step 1: CHECK whether the operator system of the smart mobile terminal to be tested provides the development function of call record read operations;

Step 2: If the operator system of smart mobile terminal provides the development function of call record read operations, USE this function to develop an application for the call record read operations;

Step 3: INSTALL and RUN an application that is able to read the call records, and CHECK whether any prompts are provided for the user during the program installation or first run.

Expected results:

After Step 1, if the operator system of smart mobile terminal fails to provide the development function of call record read operations, this item will be evaluated as “no abnormality”, and the evaluation will end;

After Step 3, if smart mobile terminal provides the user with the prompt that this program will access to the user’s call records, this item will be evaluated as “no abnormality”, and the evaluation will end;

After Step 3, if smart mobile terminal does not provide the user with any prompts, and if the program is able to perform the read operation to the user’s call records, this item will be evaluated as “not satisfiable”, and the evaluation will end.

Step 3: INSTALL and RUN an application that is able to read the multimedia message data, and CHECK whether any prompts are provided for the user during the program installation or first run.

Expected results:
 After Step 1, if the operator system of smart mobile terminal fails to provide the development function of multimedia message data read operations, this item will be evaluated as “no abnormality”, and the evaluation will end;
 After Step 3, if smart mobile terminal provides the user with the prompt that this program will access to the user’s multimedia message data, this item will be evaluated as “no abnormality”, and the evaluation will end;
 After Step 3, if smart mobile terminal does not provide the user with any prompts, and if the program is able to perform the read operation to the user’s multimedia message data, this item will be evaluated as “not satisfiable”, and the evaluation will end.

4.3.1.3 Updates of the operator system

Test No.: 4.3.1.3.1
Test item: Updates of the operator system - Authorization update
Item requirements: SEE Section 5.3.2 of YD/T 2407-2013.
Preconditions: The smart mobile terminal to be tested is under normal operating condition.
Test steps: Step 1: CHECK whether the operator system of the smart mobile terminal to be tested provides the ability to update the operator system; Step 2: If the operator system of smart mobile terminal provides the ability of authorization update of the operator system, USE the authorized operator system for system update; Step 3: USE the unauthorized operator system for system update.
Expected results: After Step 1, if the operator system of smart mobile terminal fails to provide the ability to update the operator system, this item will be evaluated as “no abnormality”, and the evaluation will end; After Step 2, smart mobile terminal successfully performs the updates of the operator system; After Step 3, if smart mobile terminal cannot normally perform the updates of the operator system, this item will be evaluated as “no abnormality”; if smart mobile terminal successfully performs the updates of the operator system, this item will be evaluated as “not satisfiable”.

Test No.: 4.3.1.3.2
Test item: Updates of the operator system - Risk prompt
Item requirements: SEE Section 5.3.2 of YD/T 2407-2013.

If smart mobile terminal meets the above expected results, this item will be evaluated as “no abnormality”, otherwise it will be evaluated as “not satisfiable”.

Test No.: 4.1.1.1.2 [Translator note: 4.4.1.1.2]

Test item: Controlled mechanism for the enabling of the Bluetooth interface

Item requirements: SEE Section 5.4.1.1 of YD/T 2407-2013.

Preconditions: The Bluetooth interface of the smart mobile terminal to be tested is in OFF state.

Test steps:

Step 1: CHECK whether the operator system of the smart mobile terminal to be tested provides the development function of Bluetooth interface enabling;

Step 2: If the operator system of smart mobile terminal provides the development function of Bluetooth interface enabling, USE this function to develop an application for Bluetooth interface enabling;

Step 3: RUN this application to enable the Bluetooth interface, and SEE whether the terminal requires the user to validate the enabling of Bluetooth interface.

Expected results:

After Step 1, if the operator system of smart mobile terminal fails to provide the development function of Bluetooth interface enabling, this item will be evaluated as “no abnormality”, and the evaluation will end;

After Step 3, if smart mobile terminal requires the user to validate the enabling of Bluetooth interface, this item will be evaluated as “no abnormality”, and the evaluation will end;

After Step 3, if smart mobile terminal does not require the user to validate and successfully enables the Bluetooth interface, this item will be evaluated as “not satisfiable”, and the evaluation will end.

Test No.: 4.4.1.1.3

Test item: ON / OFF switch of the NFC interface

Item requirements: SEE Section 5.4.1.1 of YD/T 2407-2013.

Preconditions: The NFC interface of the smart mobile terminal to be tested is in OFF state.

Test steps:

Step 1: CHECK whether the smart mobile terminal to be tested provides the ON / OFF switch of the NFC interface;

Step 2: If smart mobile terminal provides a switch, USE this switch to enable the NFC interface;

Step 3: USE the switch to disable the NFC interface.

Expected results:

After Step 2, smart mobile terminal prompts to the user, then starts the file transmission.
If smart mobile terminal meets the above expected results, this item will be evaluated as “no abnormality”, otherwise it will be evaluated as “not satisfiable”.

Test No.: 4.4.1.4.2
Test item: Controlled mechanism for the data transmission via NFC interface
Item requirements: SEE Section 5.4.1.4 of YD/T 2407-2013.
Preconditions: The NFC interface of the smart mobile terminal to be tested is in ON state, and smart mobile terminal has established data connection with the PC for testing.
Test steps: Step 1: USE the data transmission method provided by the terminal to send data from the smart mobile terminal to be tested to the PC for testing; Step 2: USE the data transmission method provided by the terminal to send data from the PC for testing to the terminal to be tested.
Expected results: After Step 1, smart mobile terminal prompts to the user, then starts the file transmission; After Step 2, smart mobile terminal prompts to the user, then starts the file transmission. If smart mobile terminal meets the above expected results, this item will be evaluated as “no abnormality”, otherwise it will be evaluated as “not satisfiable”.

4.4.2 Security capability of the wired peripheral interface

4.4.2.1 Validation mechanism for the establishment of the connection with the wired peripheral interface

Test No.: 4.4.2.1
Test item: Validation mechanism for the establishment of the connection with the wired peripheral interface
Item requirements: SEE Section 5.4.2.1 of YD/T 2407-2013.
Preconditions: The smart mobile terminal to be tested is under normal operating condition.
Test steps: Step 1: CHECK the number of wired peripheral interfaces on smart mobile terminal; Step 2: CARRY out the following tests to each wired peripheral interface; Step 3: VALIDATE the purposes of such wired peripheral interfaces: for charging only, for data connection only, for charging and data connection;

If smart mobile terminal meets the above expected results, this item will be evaluated as “no abnormality”, otherwise it will be evaluated as “not satisfiable”.

4.5 Security of smart mobile terminal’s application layer

4.5.1 Security configuration capability of application software

Test No.: 4.5.1
Test item: Security configuration capability of application software
Item requirements: SEE Section 5.5.1 of YD/T 2407-2013.
Preconditions: The smart mobile terminal to be tested is under normal operating condition.
<p>Test steps:</p> <p>Step 1: CHECK whether the operator system of the smart mobile terminal to be tested provides the development functions of dialing, initiating the third-way calling, sending the short messages and multimedia messages, calling the data connection in mobile communication network, calling the positioning function, call recording, local recording, camera / filming, accessing the phonebook, accessing the call records, accessing the short messages and multimedia messages;</p> <p>Step 2: DEVELOP the corresponding application for providing the calling of the development functions;</p> <p>Step 3: RUN this application, and CHECK whether the corresponding call has configurable capability;</p> <p>Step 4: DISABLE all calls, RUN again, and CHECK the application for actual running status;</p> <p>Step 5: Gradually ENABLE each call, RUN afterwards, and CHECK the application for actual running status.</p>
<p>Expected results:</p> <p>After Step 3, if you can find the application’s security configuration menu containing the configuration options for calling with the development functions, and the configuration includes at least two options of “allow calls” and “no calls”, CONTINUE to perform Step 4, otherwise this evaluation will be evaluated as “not satisfiable”, and the evaluation will end;</p> <p>After Step 4, if the application cannot call all functions, CONTINUE to perform Step 5; if the application can call some of the functions, this evaluation will be evaluated as “not satisfiable”, and the evaluation will end;</p> <p>After Step 5, if the application can only call the allowed call(s) and cannot perform other calls every time when a call is enabled, this item will be evaluated as “no abnormality”, otherwise it will be evaluated as “not satisfiable”, and the evaluation will end.</p>

4.5.2 Security authentication mechanism for the application software

Step 5: DEVELOP an application whose signing certificate is revoked, with a certified code signature that has not been tampered with; INSTALL this application on the smart terminal to be tested;

Step 6: DEVELOP an application with no certified code signature. INSTALL this application on the smart terminal to be tested.

Expected results:

After Step 1, if the smart mobile terminal to be tested is checked to provide the certified signature mechanism for the application software, CONTINUE to perform Step 2;

In Step 2, if the smart mobile terminal to be tested supports OCSP or CRL protocol to perform online check for the effectiveness of the Code Signing Certificate, CONTINUE to perform Step 3, otherwise this evaluation will be evaluated as “not satisfiable”, and the evaluation will end;

In Step 3, the application can be successfully installed on the smart terminal to be tested;

In Steps 4, 5 and 6, if the smart mobile terminal to be tested prohibits the application installation or reminds the user of the installation risks, this item will be evaluated as “no abnormality”, otherwise it will be evaluated as “not satisfiable”.

4.5.3 Monitoring capability of the self-triggered program

Test No.: 4.5.3

Test item: Monitoring capability of the self-triggered program

Item requirements: SEE Section 5.5.3 of YD/T 2407-2013.

Preconditions: The smart mobile terminal to be tested is under normal operating condition.

Test steps:

Step 1: SEE the self-triggered program of smart mobile terminal;

Step 2: INSTALL an application that is able to perform self-starting, and CHECK whether it is identified as the self-triggered program;

Step 3: CONFIGURE the application added in Step 2 to be unable to perform self-starting;

Step 4: RESTART the smart mobile terminal, and CHECK whether the application configured to be unable to perform self-starting in Step 3 is under operation, after smart mobile terminal enters normal operating condition.

Expected results:

After Step 1, RECORD the program that is able to perform self-starting;

After Step 2, CHECK whether the installed application is configured as self-starting;

After Step 3, it shall be able to configure the application to be unable to perform self-starting;

After Step 4, smart mobile terminal shall not run the application that has been configured to be unable to perform self-starting.

phonebook data, call records, short message data, multimedia message data, call recording, local recording, pictures, videos, audios and positioning information in the absence of a user's confirmation) without giving a clear indication to the user and user consent.

Expected results:

If the preset application software's information security testing system displays that the preset application software of the smart mobile terminal to be tested has no unauthorized calling of terminal communication leading to user's information disclosure, this item will be evaluated as "no abnormality", otherwise it will be evaluated as "not satisfiable".

4.6 Security protection capability of user data on smart mobile terminal

4.6.1 Password protection for smart mobile terminal

Test No.: 4.6.1.1
Test item: Boot password protection
Item requirements: SEE Section 5.6.1 of YD/T 2407-2013.
Preconditions: The smart mobile terminal to be tested is turned off, and smart mobile terminal enables the user identity authentication.
<p>Test steps:</p> <p>Step 1: START up the smart mobile terminal, and smart mobile terminal prompts for user login password;</p> <p>Step 2: ENTER the correct user password;</p> <p>Step 3: ENTER the user login password modification menu via the man-machine interface of smart mobile terminal;</p> <p>Step 4: MODIFY the user login password to 3 digits;</p> <p>Step 5: MODIFY the user login password to 4 digits or above;</p> <p>Step 6: SHUT down, and START up afterwards;</p> <p>Step 7: ENTER the old password;</p> <p>Step 8: ENTER the new password;</p> <p>Step 9: ENTER the user login password menu via the man-machine interface of smart mobile terminal, and DISABLE the user identity authentication;</p> <p>Step 10: SHUT down, and START up afterwards;</p> <p>Step 11: MODIFY the user login password to normal value via the man-machine interface of smart mobile terminal;</p> <p>Step 12: SHUT down, and START up afterwards;</p> <p>Step 13: Continuously ENTER wrong user password.</p>
<p>Expected results:</p> <p>After Step 2, smart mobile terminal shall prompt that the login password entered is correct, and the terminal starts up normally;</p> <p>In Step 4, smart mobile terminal shall prompt the user that the user login password is too short and shall ask the user to re-enter, or smart mobile terminal cannot modify the password to 3 digits;</p>

In Step 2, smart mobile terminal shall enter the screensaver state, after exceeding the waiting time;
In Step 3, smart mobile terminal shall be able to answer the phone normally;
In Step 4, smart mobile terminal shall enter the screensaver state immediately after the call ends;
In Step 5, smart mobile terminal shall prompt the user to enter the password for the identity authentication via screensaver activation;
In Step 6, smart mobile terminal shall prompt that the password is wrong;
In Step 7, smart mobile terminal shall prompt that the password is correct; smart mobile terminal is activated and enters the normal operating condition;
In Step 8, smart mobile terminal shall prompt to enter the password;
In Step 9, smart mobile terminal shall prompt that the identity authentication via screensaver activation is successfully disabled.
If smart mobile terminal meets the above expected results, this item will be evaluated as “no abnormality”, otherwise it will be evaluated as “not satisfiable”.

4.6.2 Authorized access for user data in files

Test No.: 4.6.2
Test item: Authorized access for user data in files
Item requirements: SEE Section 5.6.2 of YD/T 2407-2013.
Preconditions: The smart mobile terminal to be tested is under normal operating condition.
Test steps: Step 1: PROTECT the pictures, videos, audios and files by smart mobile terminal’s authorized access for user data in files; Step 2: DEVELOP a third-party application to try to access the pictures, videos, audios and files under protection.
Expected results: In Step 2, the third-party application can access the pictures, videos, audios and files under protection after user validation. If smart mobile terminal meets the above expected results, this item will be evaluated as “no abnormality”, otherwise it will be evaluated as “not satisfiable”.

4.6.3 Encrypted storage of user data

Test No.: 4.6.3
Test item: Encrypted storage of user data
Item requirements: SEE Section 5.6.3 of YD/T 2407-2013.
Preconditions: The smart mobile terminal to be tested is under normal operating condition.
Test steps:

Step 1: USE the triggering conditions for remote locking of the smart mobile terminal to be tested to perform remote locking of smart mobile terminal.

Expected results:

After Step 1, the smart mobile terminal to be tested is remotely locked.

If smart mobile terminal meets the above expected results, this item will be evaluated as “no abnormality”, otherwise it will be evaluated as “not satisfiable”.

Test No.: 4.6.5.2

Test item: Remote deletion of user data

Item requirements: SEE Section 5.6.5 of YD/T 2407-2013.

Preconditions: The smart mobile terminal to be tested is under normal operating condition.

Test steps:

Step 1: USE the triggering conditions for remote deletion of the smart mobile terminal to be tested to perform remote deletion of smart mobile terminal. CHECK whether the user data in the smart mobile terminal to be tested is deleted.

Expected results:

After Step 1, the user data is remotely deleted.

If smart mobile terminal meets the above expected results, this item will be evaluated as “no abnormality”, otherwise it will be evaluated as “not satisfiable”.

4.6.6 Transfer backup of user data

Test No.: 4.6.6.1

Test item: Local backup of user data

Item requirements: SEE Section 5.6.6 of YD/T 2407-2013.

Preconditions: The smart mobile terminal to be tested is under normal operating condition.

Test steps:

Step 1: ESTABLISH data connection between the smart mobile terminal and the PC for testing via a peripheral interface;

Step 2: USE the function of user data backup to perform the backup of user data. CHECK whether the backup contents include the phonebook, short message, multimedia message, email and multimedia data. CHECK whether the corresponding prompts are provided for the user during backup.

Expected results:

In Step 2, smart mobile terminal can perform local backup of the phonebook, short message, multimedia message, email and multimedia data;

In Step 2, smart mobile terminal shall prompt the user that data backup is in progress.