GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80
RECORD NO.: 38311-2013

GM/T 0013-2012

Trusted computing - Trusted cryptography module interface compliance

可信计算　可信密码模块接口符合性测试规范

Issued on: November 22, 2012 **Implemented on: November 22, 2012**

Issued by: State Cryptography Management

Table of Contents

Foreword

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The issuer of this document shall not be held responsible for identifying any or all such patent rights.

This Standard was proposed by and shall be under the jurisdiction of the State Cryptography Management.

The drafting organizations of this Standard: Institute of Software Chinese Academy of Sciences, Nationz Technologies Co., Ltd., Legend Holdings Co., Ltd., Tongfang Co., Ltd., Beijing Information Science and Technology University.

The main drafters of this Standard: Qin Yu, Wu Qiuxin, Chang Dexian, Chu Xiaobo, Xu Zhen, Liu Xin, Ning Xiaokui, Zheng Bike, Liu Ren, Li Hao, Zhang Qianying, Wang Dan, Liu Ziwen, Yu AImin.

Trusted computing - Trusted cryptography module interface compliance

1 Scope

This Standard is based on GM/T 0011-2012, *Trusted computing - Functionality and interface specification of cryptographic support platform*; defines the command test vectors of trusted cryptography modules; and provides effective test methods and flexible test scripts.

This Standard applies to the compliance test of trusted cryptography modules, but it can not replace their security check. The security test of trusted cryptography modules shall be conducted in accordance with other specifications.

2 Normative references

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

GB/T 5271.8-2001, *Information technology - Vocabulary - Part 8: Security*

GB/T 16264.8-2005, *Information technology - Open systems interconnection - The directory - Part 8: Public-key and attribute certificate frameworks*

GB 17859-1999, *Classified criteria for security protection of computer information system*

GB/T 18336 (all parts), *Information technology - Security techniques - Evaluation criteria for IT security*

GM/T 0002-2012, *SM4 Block cipher algorithm*

GM/T 0003-2012, *Public key cryptographic algorithm SM2 based on elliptic curves*

GM/T 0004-2012, *SM3 password hashing algorithm*

GM/T 0011-2012, *Trusted computing - Functionality and interface specification of cryptographic support platform*

GM/T 0012-2012, *Trusted computing - Interface specification of trusted cryptography module*

3 Terms and definitions

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

3.1

trusted computing platform

The support system which is established in the computing system and used to implement the trusted computing function.

3.2

trusted cryptography module; TCM

The hardware module of the trusted computing platform, which provides the cryptographic operation function for the trusted computing platform and has a protected storage space.

3.3

platform configuration register; PCR

The storage unit inside the trusted cryptography module, which is used to store platform integrity measurement values.

3.4

TCM endorsement key; EK

The initial key of the trusted cryptography module.

3.5

storage master key; SMK

The master key which is used to protect platform identity keys and user keys.

3.6

hash-based message authentication mode; HMAC

This Standard adopts SM3 hash algorithm provided in GM/T 0004-2012 to generate message authentication codes.

3.7

This Standard only provides the test strategies and test methods for TCM compliance test, in which all the commands involved come from the standard GM/T 0011; and the optionality of the command input parameters and the randomization factors inside TCM enable manufacturers to implement command test by themselves. Therefore, the test vectors provided in this Standard are only for the reference of users only.

If manufacturers add a test process into TCM products regarding it as a mode, then when TMC is in such mode, it is deemed that TCM is in the test mode. The test mode requirements:

a) the TCM products in the test mode shall neither contradict with other information of TCM in work, nor disclose such information.

b) TCM manufacturers and system providers shall ensure that TCM only providing the compliance mode is not implanted into product systems.

c) when TCM is in the compliance test status, proof shall be provided to prove that TCM is in the compliance test status.

1) TCM can provide proof through a certain mechanism of manufacturers.

2) the already-known mechanisms include:

-- non-standard version information;

-- fixed EK.

4.2 Constant values

The examples in this Standard regarding test vectors and test scripts will involve some values; these values have the same functions and can be unified and reused, which is to be benefit of the unification of the whole standard. The following standard values will be applied in the examples of the digital computing TCM commands in the whole standards.

4.2.1 Keys

Asymmetric key: TCM adopts the SM2 asymmetric cipher algorithm provided by GM/T 0003-2012; and this Standard uses the following 4 named SM2 keys.

keyA: mainly in charge of relevant operations of keys themselves, such as obtaining public key, loading key, etc. and SM2 encryption and decryption. It is a SM2 asymmetric key which is imported from the outside.

keyB: signature key, mainly in charge of signature data. It is generated by command TCM_MakeIdentity.

4.4 Test method

The trusted cryptography module interface compliance test includes two parts, i.e. single command and functional tests. The single command test is used to test whether its implementation result complies with the Specification after the command receives input parameters; the functional test is used to test whether the implementation result of a set of commands fulfills a function specified in the Specification. Therefore, the two different test methods adopted: the single command test is implemented using test vectors; and the functional test is implemented using test scripts.

Many TCM commands are not isolated, and they have dependency relationships between them. Therefore, the compilation of test scripts or test vectors shall be based on the dependency relationships between commands. This Standard give the diagram of TCM command dependency relationships, in accordance with the dependency on the authorization relationships between TCM commands and the dependency on the data stream relationships. These dependency relationships ensure the correct compilation of test vectors and test scripts. The dependency relationships between data streams can be simply through the reference of command parameters, e.g. the input parameter of some command is the output of another command, then the command depends on another command on the data stream. However, the dependency on authorization relationships is obtained through the analysis of the multiple authorization methods of the commands in GM/T 0011. This Standard can reflect these dependency relationships correctly and uses solid arrows to indicate the dependency relationships which are generated by the other authorization methods of a command.

a) Test vectors

In accordance with the dependency relationships between commands, this Standard defines a set of test vectors for those TCM commands which are irrelevant to the implementation of manufacturers and can be tested independently. These test vectors show the bit combination format required for each command, other than all possible combination format. The commands do not require certain commands input and output by manufacturers, which are tested directly using test vectors. Test vectors are generally implemented by manufacturers as a mode of TCM products, in a static way. But this is not necessary, test vectors may also be developed independently by assessors during test.

The object of test vectors is to ensure a correct format of command parameters, ensure correct structural explanation and ensure the compliance of the implementation of operation with the Specification. In TCM products, TCM does not need to support the use of test vectors, but these test vectors are recommended for use during the self-test of TCM. Test vectors requires minimum interaction between commands. The command of

using authorization sessions requires the successful output of AP sessions, which will be the default preconditions for its implementation of test vectors.

b) Test scripts

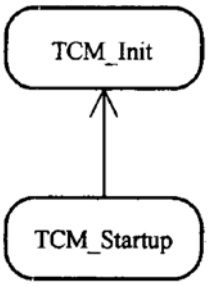
For a command requiring special decisions of manufacturers or a command requiring a set of command sequences, the compliance test will be conducted using the test script method. These test scripts can be provided by manufacturers and can also be developed by assessors in accordance with the information and data of manufacturers. TCM shall provide the capability to implement these scripts dynamically. In brief, the test of the commands is completed using test scripts, which cannot be tested simply using test vectors because of the above-mentioned reasons. This Standard will give some example data of TCM commands which requires being tested in test scripts. The specific scripts need to be compiled further in accordance with the implementation of manufacturers and the specification description.

5 Command dependency relationships

The establishment of command dependency relationships is the fundamental assurance of the correct implementation of test vectors and test scripts. Only when the command implementation preconditions are met in accordance with command dependency relationships, can the successful implementation of test scripts be ensured. Because of the large number and complexity of command dependency relationships, see GM/T 0011 and GM/T 0012 for the classification of TCM of this Standard; and in accordance with the statuses after TCM successfully implement different commands, several similar commands are classified into one command set. There are dependency relationships between commands within a set and there are also dependency relationships between sets. This Standard describes all dependency relationships between commands using this method and uses solid arrows to indicate such dependency relationships. The arrowtail commands depend on the commands pointed to by arrowheads. The details are shown as follows.

5.1 Startup command set

There are two commands, TCM_Init and TCM_Startup, whose dependency relationship is as shown in Figure 2.



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

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