GM

CRYPTOGRAPHIC INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

CCS L 80

GM/T 0012-2020

Replacing GM/T 0012-2012

Trusted computing - Trusted computing interface specification of trusted cryptography module

可信计算 可信密码模块接口规范

Issued on: December 28, 2020 **Implemented on: July 01, 2021**

Issued by: National Cryptography Administration

Table of Contents

Trusted computing - Trusted computing interface specification of trusted cryptography module

1 Scope

This document describes the functions of the trusted cryptographic module; defines the command interface of the trusted cryptographic module in detail.

This document is applicable to the research, production, evaluation, application development of products related to trusted cryptographic modules.

2 Normative references

The contents of the following documents constitute the essential provisions of this document through normative references in the text. Among them, for dated references, only the version corresponding to the date applies to this document; for undated references, the latest version (including all amendments) applies to this document.

GB/T 20518 Information security technology - Public key infrastructure - Digital certificate format

GB/T 29829 Information security techniques - Functionality and interface specification of cryptographic support platform for trusted computing

GB/T 32905 Information security technology SM3 cryptographic hash algorithm

GB/T 32907 Information security techno1ogy--SM4 b1ock cipher algorithm

GB/T 32915 Information security technology - Binary sequence randomness detection method

GB/T 32918 (all parts) Information security technology -- Public key cryptographic algorithm SM2 based on elliptic curves

3 Terms and definitions

The following terms and definitions apply to this document.

3.1

Trusted computing platform

A supporting platform, which is built in the computing system, to realize the trusted computing function.

[GB/T 29829-2013, 3.1.1]

3.2

Cryptographic support platform for trusted computing

An important part of a trusted computing platform, including cryptographic algorithms, key management, certificate management, cryptographic protocols, cryptographic services, which provides cryptographic support for the integrity, identity credibility, data security of the trusted computing platform itself. Its product forms are mainly manifested as trusted cryptographic modules and trusted cryptographic service modules.

[GB/T 29829-2013, 3.1.2]

3.3

Integrity measurement

The process of calculating the hash value of the measured object, using a cryptographic hash algorithm.

[GB/T 29829-2013, 3.1.3]

3.4

Root of trust for measurement

A trusted integrity measurement unit, which is the basis for trusted measurement in a trusted computing platform.

[GB/T 29829-2013, 3.1.4]

3.5

Root of trust for storage

It refers to storing the master key, which is the basis for trusted storage in the trusted computing platform.

[GB/T 29829-2013, 3.1.5]

3.6

Root of trust for reporting

Refers to the cryptographic module key, which is the basis for trusted reporting in the trusted computing platform.

[GB/T 29829-2013, 3.1.6]

3.7

Trusted cryptography module

It is a hardware module of the trusted computing platform, which provides cryptographic operation functions for the trusted computing platform AND has a protected storage space.

[GB/T 29829-2013, 3.1.7]

3.8

TCM service module

A software module inside the trusted computing cryptography supporting platform, which provides software interfaces for accessing trusted cryptography modules outside the platform.

[GB/T 29829-2013, 3.1.8]

3.9

Component

A hardware and/or software module, in a computing system, that can be measured.

[GB/T 29829-2013, 3.1.9]

3.10

Platform configuration register

A storage unit, which is used inside the trusted cryptographic module, to store platform integrity metrics.

[GB/T 29829-2013, 3.1.10]

3.11

Integrity measurement value

The hash value, which is obtained after the component is measured.

[GB/T 29829-2013, 3.1.11]

a) The process of calculating the measurement value shall be the process of performing hash operation;

b) The input data of the hash operation shall be the data, which is specified by the measurer that can characterize the characteristics of the measurement-object;

c) The hash value output by the hash operation is the integrity measurement value of the measurement-object;

d) The measurer shall enter the measured value into the designated PCR. The way to write in is: new PCR value = password hashing algorithm (former PCR value || measurement value);

e) Measuring process information shall be recorded in the platform event log. At least it shall be recorded: Measurer information, measurement-object information, original PCR value, measurement value, new PCR value, completion time, etc.;

f) If the integrity measure of each component in a component sequence is stored in the same PCR, then a special compression storage method is adopted, that is, starting from the first component, the integrity measure of the component is concatenated with the target PCR's existing stored values, to perform the hash operation; THEN, the result obtained is stored in the PCR, and so on. After the integrity measurement value storage operation of the last component is completed, the obtained value is the integrity measure of this component sequence, as stored in the PCR.

Integrity reporting refers to the process, by which the platform provides integrity measurements of the platform or components of the platform to the prover.

The integrity report shall meet the following requirements:

a) The platform can provide the specified PCR value to the prover, without any authorization;

b) The platform can provide the prover with the specified PCR value and the signature of the PCR value. It can sign using the platform identity key;

c) The platform can provide relevant event log information of the specified PCR to the prover;

d) The prover can judge whether the PCR value comes from the correct measurement process, by analyzing the integrity measurement event log information;

e) The prover shall use the platform identity key, to verify the PCR value signature and obtain the platform integrity report result.

6 Functional interface of trusted cryptographic module

6.1 General requirements

This chapter specifies the specific commands of the functional interface of the trusted cryptographic module. The trusted cryptographic module, which is defined in this document, shall satisfy all command interfaces in this chapter.

6.2 Startup command

6.2.1 TCM2_Startup

This command is used for TCM initialization. When the command is executed successfully, it is no longer allowed to execute the command successfully.

When TCM needs TCM2_Startup command, if it receives other commands, OR receives this command when it does not need this command, TCM will return TCM2_RC_INITIALIZE.

The shutdown/startup sequence is as follows, which defines the operation method of the TCM after receiving the TCM2_Startup() command.

a) TCM reset: Send Shutdown (CLEAR) or do not send TCM2_Shutdown () command to close, send Startup (CLEAR) when startup. When the TCM is reset, all variables are restored to the initial state.

b) TCM restart: Send Shutdown (STATE) command to shut down, send Startup (CLEAR) when startup. In this state, the following values will be restored to their initial state:

- The control switch status of PCR and platform domain;
- The remaining TCM status values will be saved.

c) TCM wake-up: Send Shutdown (STATE) command to shut down, send Startup (STATE) when startup. In this state, the following states will be saved:

- S-RTM;
- PCR;
- Platform control switches, except phEnable, phEnableNV.

For the command codes, return codes commonly used and data structures involved in all interfaces in this document, please refer to Appendix A.

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

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