GM

CRYPTOGRAPHIC INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.030

CCS L 80

GM/T 0011-2023

Replacing GM/T 0011-2012

Trusted computing - Trusted computing functionality and interface specification of cryptographic support platform

可信计算 可信密码支撑平台功能与接口规范

Issued on: December 04, 2023 **Implemented on: June 01, 2024**

Issued by: State Cryptographic Administration

Table of Contents

Trusted computing - Trusted computing functionality and interface specification of cryptographic support platform

1 Scope

This document gives the system framework and functional principles of the trusted computing cryptographic support platform; specifies the interface specifications of the trusted cryptographic module; describes the corresponding verification methods.

This document is applicable to the research, production, evaluation and application development of products related to the trusted computing cryptographic support platform.

2 Normative references

The contents of the following documents constitute the essential terms of this document through normative references in the text. Among them, for referenced documents with dates, only the version corresponding to that date applies to this document; for referenced documents without dates, the latest version (including all amendments) applies to this document.

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

GB/T 25069 Information security techniques - Terminology

GB/T 32905 Information security techniques - SM3 cryptographic hash algorithm

GB/T 32907 Information security technology - SM4 block cipher algorithm

GB/T 32915 Information security technology - Randomness test methods for binary sequence

GB/T 32918.2 Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves - Part 2: Digital signature algorithm

GB/T 32918.3 Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves - Part 3: Key exchange protocol

GB/T 32918.4 Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves - Part 4: Public key encryption algorithm

GB/T 35276 Information security technology - SM2 cryptography algorithm usage specification

GM/T 0012 Trusted computing - Trusted computing interface specification of trusted cryptography module

GM/T 0058 Trusted computing - TCM service module interface specification

GM/Z 4001 Cryptographic terminology

3 Terms and definitions

The terms and definitions defined in GB/T 25069 and GM/Z 4001, as well as the following terms and definitions, apply to this document.

3.1

Storage master key

The primary key used to protect operating system keys and user keys.

3.2

Trusted computing platform

A support system built in a computing system to implement trusted computing functions.

3.3

Cryptographic support platform for trusted computing

An important component of a trusted computing platform, including cryptographic algorithms, key management, certificate management, cryptographic protocols, cryptographic service content, providing cryptographic support for the integrity, identity authenticity, data confidentiality of the trusted computing platform itself.

3.4

Root of trust for measurement

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

Note: The root of trust for measurement is implemented or composed of hardware, firmware, software, etc.

3.5

SRTM: Static Root of Trust Measurement

TBB: Trusted Building Block

TCB: Trusted Computing Base

TCM: Trusted Cryptography Module

TSM: TCM Service Module

UEFI: Unified Extensible Firmware Interface

5 Overview of trusted computing cryptographic support platform

5.1 Trusted computing

Trusted computing is a comprehensive information security technology, which is designed to enhance the trustworthiness of computer systems. Trusted technology establishes a trusted root in a computer system, starting from the trusted root to the hardware platform, to the operating system, then to the application, measures, authenticates, trusts step by step, extending this trust to the entire computer system, taking protective measures to ensure the integrity of computing resources and the predictability of computing behavior, thereby improving the trustworthiness of the computer system.

5.2 Trusted components

A trusted component consists of one or a group of components that can complete the instantiation of a trusted root.

5.3 Trusted computing base

The trusted computing base (TCB) is the system hardware and software resources responsible for maintaining the system security policy. An important attribute of the TCB is that it shall prevent itself from being damaged by any hardware or software that does not belong to the TCB.

5.4 Trusted boundary

The trusted component (TBB) and the trusted root constitute the trusted boundary,

which includes entities that measure, store, and report the integrity of the computer's minimum configuration. In more complex systems, trust shall be extended to other code by measuring other code based on the Core root of trust for measurement (CRTM) and recording the measurement results in the Platform Configuration Register (PCR).

5.5 Trusted Transfer

Trusted transfer is the process of measuring the measured modules one by one based on the Trusted Root and extending the trust chain.

Trusted transfer shall be achieved by TCM supporting one of the following two methods:

a) An operation performed in accordance with the security policy to allow subsequent operations to obtain control of the TCB;

b) For the measurement of subsequent operations, an independent evaluation of the trust relationship is established.

5.6 Trusted authorization

When the root of trust for measurement (RTM) begins to execute the core root of trust for measurement (CRTM), its correctness is guaranteed by the producer of the trusted component.

When the system executes code outside the core root of trust for measurement, the trust chain can be maintained by measuring the trust of the code. If the execution of code depends on its trust measurement, the execution authorization of the code will remain unchanged.

The following are two different methods that allow the evaluation of the trust rights of the platform.

a) Measure the code (hash calculation) and record the measurement value in the root of trust for storage (RTS). If the code does not consider its measurement value when running, its trust authorization comes from the digest value provided by the root of trust for reporting (RTR).

b) Sign the code and determine whether the code is trustworthy by verifying the signature. If its identity is recorded in the RTS, then this assessment can be modified.

6 Functions of trusted computing cryptographic support

reports to it. The only interaction between TCM and the system is through the interface defined in this document.

6.1.4 TCM service module

The trusted cryptographic module defines a subsystem with storage protection and execution protection, which will establish a trusted root for the computing platform; its independent computing resources will establish a strictly isolated security protection mechanism. The functions that need to be executed and those that do not need to be executed in the subsystem shall be separated; the functions that do not need to be executed shall be executed by the main processor of the computing platform; these supporting functions constitute the TCM service module.

Note: This document only describes the functional principle of the TCM service; it does not involve the TCM service module interface specification. The TCM service module interface specification can be found in GM/T 0058.

The TCM service mainly provides support for users to use TCM basic resources. It consists of multiple parts; the interface definition between each part shall be interoperable. The TCM service shall provide a standardized function interface.

The design goals of the TCM service are as follows:

a) Provide an entry point for applications to call TCM security protection functions;

b) Provide synchronous access to TCM;

c) Hide the complexity of TCM function commands from applications;

d) Manage TCM resources.

6.2 Platform interface functions

6.2.1 Trusted root

The trusted root is the trusted base point of the trusted computer and the base point for implementing security controls. The trusted root provides the minimum functions required to describe the characteristics of the platform's trustworthiness.

There are three trusted roots in the trusted computing cryptographic support platform: the root of trust for measurement (RTM), the root of trust for storage (RTS), the root of trust for reporting (RTR).

a) RTM is the base point for trusted measurement of the platform. RTM sends integrity information to RTS. When a new trust chain is established, the first set of instructions executed is the core root of trust for measurement (CRTM). When the system is reset, the CPU starts executing CRTM. Then, CRTM sends a

measurement value indicating its identity to RTS. This establishes the starting point of the trust chain.

b) RTS is the base point for secure storage of trusted measurement values. TCM internal storage cannot be unauthorizedly accessed by external entities; TCM can serve as RTS. TCM can prevent unauthorized access to sensitive information; TCM can also store some non-sensitive information.

c) RTR is the base point for the platform to provide platform credibility status reports to access objects. RTR reports on RTS content; RTR reports are signed reports of selected content in TCM.

TCM contains an encrypted identity that can be verified by RTR. This identity is expressed in the form of an endorsement key or an endorsement certificate. The seed generated by the endorsement key is bound to each chip, so two TCMs will not have the same endorsement key.

The trusted computing platform provides at least three trusted roots described above: RTM, RTS, RTR. All three roots use authentication and proof to provide evidence of information. The trusted computing platform will also provide protected storage for trusted keys and data objects. The trusted computing platform can provide integrity measurements to ensure the trustworthiness of the platform.

6.2.2 Attestation and certification

6.2.2.1 Attestation methods

6.2.2.1.1 Classification

The trusted computing platform provides the following attestation methods.

a) In the first category, an external entity attests to the TCM, which shall comply with this document. This attestation is based on the endorsement key in the TCM.

b) In the second category, an external entity authenticates the platform to ensure that the platform contains the RTM, the authentic TCM.

c) In the third category, the "certifying CA" attests to the asymmetric key pair in the TCM, to ensure that the key is protected by the TCM and has specific intrinsic properties. This attestation takes the form of a certificate, to provide guarantees for information including the public key of the key pair.

d) In the fourth category, the trusted computing platform attests to the asymmetric key pair, to ensure that the key pair is protected by the TCM and has specific intrinsic properties. This authentication method takes the form of signing the information describing the key pair in the platform's TCM, using the authentication key protected by the TCM, and a type authentication that provides

a guarantee for the authentication key.

e) Category 5, the trusted computing platform attests the measurement to ensure that a specific software/firmware state exists in the platform. This attestation method uses the authentication key protected by the TCM, to sign the software/firmware measurement value in the PCR.

f) Category 6, the external entity attests the software/firmware measurement. This authentication takes the form of a credential that signs the information including the measurement value and state.

6.2.2.1.2 Attestation key and attestation key identity certificate

The authentication of categories 3 and 4 above requires the use of a key to sign the content of the TCM shielded location.

a) Attestation key (AK) is the platform identity key. The AK is a special type of signing key, whose use is restricted to prevent forgery (the signature of external data has the same format as the real authentication data). When the TCM is to create a signed message, a special value is used from within the TCM as the message header. When using AK to sign a digest, the caller provides a ticket so that TCM shall determine that the message used to create the digest cannot be forged TCM authentication data. The value signed by AK can be guaranteed to reflect the TCM state, but AK can also be used for general signing purposes.

b) Proof of key identity certificate. TCM users can create limited-use signing keys based on TCM and require a third-party CA to provide them with a key identity certificate. The CA can require the caller to provide some evidence to prove that the authenticated key is a TCM resident key, before providing an identity certificate.

6.2.2.2 Platform identity

The trusted computing cryptographic support platform uses an endorsement key (EK) to identify its identity. Under the authorization of EK, an asymmetric key pair is generated inside TCM as AK, which is used to digitally sign information inside TCM, realize platform identity authentication and platform integrity report, thus proving the credibility of the platform's internal data to the outside.

EK shall be stored in TCM and used only when obtaining endorsement key authorization operations and applying for platform identity certificates; it shall not be exported outside TCM.

The endorsement key certificate is signed by a trusted party before the platform is used to establish a one-to-one correspondence between EK and trusted cryptographic module instances.

A trusted computing cryptographic support platform can generate multiple AKs, each of which is bound to EK and represents the platform identity to the outside world.

6.2.3 Protected locations

6.2.3.1 Overview

The protected location uses multiple seeds and keys for encryption, which never leave the TCM. One of them is the context key. It is a symmetric key used to encrypt data when it is temporarily exchanged out of the TCM, in order to load a different set of working objects. Other sensitive values that never leave the TCM are primary seeds, which are the roots of the storage hierarchy that protects objects retained by the application. The primary seed is used to generate random numbers for protection keys for other objects: these objects may be storage keys containing protection keys. The primary seeds may be changed; when they are changed, the objects derived from them will no longer be available.

6.2.3.2 Key management functions

Key management includes the following functions.

a) Key generation: Key generation refers to the application layer software setting the key attributes, key use authorization, key migration authorization, key protection operation key of the required generated key, sending them to the TCM to generate the specified key. In the TCM, the private key part of the generated key is encrypted by the protection operation key, then the generated key data structure is returned to the application layer software. For various types of keys in the TCM, the generation methods include:

- EK is generated by the manufacturer and is an asymmetric key;
- When the platform owner generates the storage master key, it shall be generated inside the trusted cryptographic module;
- The platform identity key is an asymmetric key and shall be generated inside the TCM. The trusted party shall apply for the corresponding platform identity certificate and activate the key;
- The user key can be generated inside the trusted cryptographic module or imported after being generated outside the trusted cryptographic module. The user key can be a symmetric key or an asymmetric key.

b) Key loading: After the key is generated, when the application layer software uses the key for data security protection operations, if the private key of the key is used, the key data shall be loaded into the TCM and can only be used after being decrypted by the protection operation key. If the public key of the key is used, it can be used directly in the application layer software. The loading methods of

various keys in the trusted cryptographic module include:

- When using the TCM key public key, the authorization shall not be verified before setting the platform owner. After setting the platform owner, the owner authorization shall be verified; the cryptographic algorithm operation process shall be performed inside the TCM;

- When using the storage master key, the storage master key authorization shall be verified; the cryptographic algorithm operation process shall be performed inside the TCM;

- When using the platform identity key AK, the platform identity key authorization and storage master key authorization shall be verified; the private key of the platform identity key shall be loaded into the TCM for cryptographic algorithm operation; the cryptographic algorithm operation process of the public key shall be performed outside the TCM;

- When using the platform encryption key, the platform encryption key authorization and storage master key authorization shall be verified; the private key of the platform encryption key shall be loaded into the trusted cryptographic module for cryptographic operation; the cryptographic operation process of the public key shall be performed outside the module;

- When using the user key, the user key authorization shall be verified; the private key of the user key shall be loaded into the TCM for cryptographic operation.

c) Key destruction: After the key is generated, the application layer software can destroy the specified key. For various keys in TCM, the destruction method is as follows:

- Destroying EK is completed by revoking revocable EK. Irrevocable EK cannot be destroyed;

- Destroying the storage master key shall verify the storage master key authorization before executing it in TCM;

- Destroying the platform identity key shall verify the platform identity key authorization and storage master key authorization, before executing it in the trusted cryptographic module;

- Destroying the platform encryption key shall verify the platform encryption key authorization and storage master key authorization, before executing it in the trusted cryptographic module;

- Destroying the user key needs to verify its protection operation key authorization, before executing it in the TCM service module.

After the integrity measurement value storage operation of the last component is completed, the value obtained is the integrity measurement value of the component sequence stored in the PCR.

6.2.4.3 Integrity report

Integrity report refers to the process of the platform providing the integrity measurement value of the platform or some components to the verifier. The integrity report shall meet the following requirements:

a) The platform shall provide the verifier with the specified PCR value without any authorization;

b) The platform shall provide the verifier with the specified PCR value and the signature of the PCR value; the signature shall use the platform identity key;

c) The platform can provide the verifier with the associated event log information of the specified PCR;

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

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

6.2.4.4 Trust chain

The trust chain is used to ensure the integrity of the platform. The establishment of the platform trust chain starts with the root of trust for measurement.

First, measure the integrity of other components of BIOS; store the measurement values in the PCR of the trusted cryptographic module. According to the selected judgment mechanism, judge the integrity of BIOS. If the integrity is not damaged, run BIOS; measure the integrity of the initialization program loader (IPL)/master boot record (MBR). The integrity of IPL/MBR can also be judged, based on the judgment mechanism. If the integrity of IPL/MBR is not damaged, run MBR; then measure the integrity of OS kernel by IPL/MBR; after OS kernel is started, detect the integrity of OS service based on the same mechanism. Through the transmission of trust relationship, it can be ensured that the started system is trustworthy. If the integrity of a component is found to be damaged in the above process, report the problem and perform operations according to the specified policy.

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

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