

ICS 35.030  
CCS L 80

**GM**

**INDUSTRY STANDARD OF THE  
PEOPLE'S REPUBLIC OF CHINA**

**GM/T 0104-2021**

---

**Specifications of cloud host cryptographic server**

云服务器密码机技术规范

**(English Translation)**

**Issued on: October 18, 2021**

**Implemented on: May 1, 2022**

---

**Issued by: State Administration of Cryptography**

## Table of Contents

|                                                     |    |
|-----------------------------------------------------|----|
| Scope .....                                         | 1  |
| Normative references .....                          | 2  |
| Terms and definitions .....                         | 3  |
| Abbreviated terms .....                             | 4  |
| Device form .....                                   | 5  |
| Management requirements .....                       | 6  |
| Initialization .....                                | 7  |
| Registration, scheduling and monitoring .....       | 8  |
| Log audit .....                                     | 9  |
| Device self-checking .....                          | 10 |
| Device use .....                                    | 11 |
| Virtual security module life cycle management ..... | 12 |
| Key management function .....                       | 13 |
| Secure storage and destruction of keys .....        | 14 |
| Backup/Recovery .....                               | 15 |
| Access control and identity authentication .....    | 16 |
| Random number generation and verification .....     | 17 |
| Hardware security .....                             | 18 |
| Software security .....                             | 19 |
| External interface .....                            | 20 |
| Randomizer .....                                    | 21 |
| Environmental adaptability .....                    | 22 |
| Reliability .....                                   | 23 |
| Basic requirements .....                            | 24 |
| Service interface .....                             | 25 |
| Management interface .....                          | 26 |
| Service interface .....                             | 27 |
| Management interface .....                          | 28 |

## 1 Scope

This document defines the relevant terms of cloud cryptographic server, and specifies the overall structure, functional requirements, hardware requirements, software requirements, security requirements and testing requirements of cloud cryptographic server.

This document applies to the development and use of cloud cryptographic server, and can also be used to guide the testing of cloud cryptographic server.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the version corresponding to that date is applicable to this document; for undated references, the latest version (including all amendments) is applicable to this document.

GB/T 9813.3-2017, General specification for computer - Part 3: Server GB/T 31168-2014, Information security technology - Security capability requirements of cloud computing services GB/T 32915-2016, Information security technology - Binary sequence randomness detection method GB/T 35293-2017, Information technology - Cloud computing - General technical requirements of virtual machine management GB/T 36322-2018, Information security technology - Cryptographic device application interface specifications

## 3 Terms and definitions

For the purpose of this document, the following terms and definitions, as well as those given in GM/Z 4001, apply.

cloud computing

A model that accesses a scalable and flexible pool of physical or virtual resources through the network and can obtain and manage resources on demand by itself.

cloud-hosted hardware security module (CHSM) / cloud cryptographic server A cryptographic server that, in the cloud computing environment, provides cryptographic services for multiple tenants' application systems, in a network form, by using virtualization technology.

host

A physical device that provides a running environment and hardware resources for the virtual security module. Multiple virtual security modules in the same host share the cryptographic computing resources and key storage resources in the host.

single root I/O virtualization; SRIOV A specification that enables a single PCIe physical device under a single root port to display as multiple separate virtual PCIe devices (VFs) to

a hypervisor or guest operating system.

private key access password A passphrase used to verify access to the private key.

virtual security module; VSM A cryptographic service instance created on a cloud cryptographic server using virtualization technology that provides services similar to those of a physical cryptographic server.

## **4 Abbreviated terms**

For the purposes of this document, the following abbreviated terms apply.

CBC. Cipher Block Chaining

### **5.1 Device form**

The cloud cryptographic server is physically an independent cryptographic device, and logically consists of a host and several virtual security modules. The overall structure of the cloud cryptographic server is shown in Figure 1.

#### **5.2.1 Management requirements**

The host of the cloud cryptographic server is managed and used by the cloud platform or the owner of the cloud cryptographic server, and the virtual security module is managed and used by the tenant.

#### **5.2.2 Initialization**

The initialization of the cloud cryptographic server host mainly includes the generation (recovery) and installation of the host key, the generation of administrators, the secure storage and backup of the key according to the security mechanism, so that the device is in a ready state.

#### **5.2.3 Registration, scheduling and monitoring**

The cloud cryptographic server host should have the function of registering with the cloud platform management system, registering the physical resources of the host's physical device (processor, memory, network, cryptographic computing power, key storage capacity, etc.), and accepting the cloud platform management system's scheduling management and real-time monitoring of its operational state.

### **5.4 Log audit**

The cloud cryptographic server host and different virtual security modules shall provide log record, view and export functions.

## **5.5 Device self-checking**

The cloud cryptographic server host and virtual security module shall have the function of self-checking at startup and self-checking when receiving self-checking instructions, and should have the function of periodic self-checking.

## **5.6 Device use**

Tenants can use the virtual security module according to the following process.

### **5.7.1 Virtual security module life cycle management**

The cloud cryptographic server shall have virtualization function, to be able to accept external commands, as well as to create, start, stop and destroy virtual security modules.

#### **6.1.1 Key management function**

The host of the cloud cryptographic server shall have the functions of generating, installing, storing, using, destroying, backing up and restoring all the keys of the host;

the virtual security module of the cloud cryptographic server shall have the functions of generating, installing, storing, using, destroying, backing up and restoring all the keys of the virtual security module. The host cannot manage and access the keys of virtual security modules; the virtual security module cannot manage and access the keys of other virtual security modules other than itself and the host.

#### **6.1.4 Secure storage and destruction of keys**

Each virtual security module of the cloud cryptographic server shall be able to store at least 32 pairs of asymmetric keys and 100 symmetric keys.

#### **6.1.6 Backup/Recovery**

For persistently stored keys, the cloud cryptographic server shall have backup/recovery functions.

## **6.2 Access control and identity authentication**

The cloud cryptographic server shall have an identity authentication mechanism.

Bidirectional identity authentication shall be performed between the host and the administrator, between the virtual security module and the administrator, and between the tenant/application using the virtual security module and the virtual security module, and shall comply with the provisions for identity authentication of administrators and users at security level 2 and above in GB/T 37092.