ICS 35.030
CCS L 80



# NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

# GB/T 43696-2024

## Cybersecurity technology - Zero trust reference architecture

网络安全技术 零信任参考体系架构

**Issued on: April 25, 2024** **Implemented on: November 1, 2024**

**Issued by: State Administration for Market Regulation;**
**Standardization Administration of the PRC**

# Table of Contents





## 1 Scope

The document specifies the zero trust reference architecture and describes the subject, the resource, the core components and the supporting components, together with the relations among them.

It applies to the planning, design, development, application and evaluation of information systems that adopt a zero trust architecture.

## 2 Normative references

One normative reference is listed: GB/T 25069, Information security technology - Terminology. For dated references only the edition corresponding to that date applies; for undated references the latest edition, including all amendments, applies.

## 3 Terms and definitions

The terms and definitions given in GB/T 25069 and the following ones apply to the document.

3.1 zero trust: a cybersecurity concept whose core is the protection of resources. Note: the concept holds that when a subject accesses a resource, whether or not the subject and the resource are trustworthy, the trust relation between the subject and the resource has to be built from zero through continuous state awareness and dynamic trust evaluation, so as to carry out end-to-end secure access control.

3.2 zero trust architecture: the information system architecture built on the basis of zero trust. Note: it includes the system components that make up the architecture and the relations among the components.

3.3 subject: the entity that initiates an access request.

3.4 resource: the object available for a subject to access.

## 4 Typical features

A zero trust architecture has the following typical features.

a) Continuous state awareness: the relevant information of the subject, the resource and the environment is collected continuously and the security posture is analysed.

b) Dynamic trust evaluation: while a subject accesses a resource, trust evaluation is carried out continuously on the basis of the changes in the security posture of the subject, the resource and the environment that are continuously perceived, and the policy decision is maintained or changed.

c) Least privilege: according to the task requirements and the policy decision, and taking into account the time window and the granularity of the accessed resource, the least privilege is granted to the accessing subject.

d) Encrypted transmission: cryptographic technology is used to set up an end-to-end secure data channel for the subject to access the resource.

## 5 Reference architecture

The zero trust reference architecture is made up of the subject, the resource, the core components and the supporting components, as shown in Figure 1. Figure 1 places the supporting components - task management, identity management, resource management, environment awareness and cryptographic service - on the left, supplying supporting services to a block divided into a control layer and a data layer; the control layer holds the core components, that is the policy decision component with its policy engine and policy manager, and the data layer holds the policy enforcement component between the subject and the resource. The legend distinguishes control information from the secure data channel.

The core components comprise the policy decision component and the policy enforcement

component; the supporting components comprise the task management component, the identity management component, the resource management component, the environment awareness component and the cryptographic service component.

The subject is one or a combination of several of the following: user, device, information system and application software.

The resource is chiefly data, and usually also includes devices, information systems, application software, services and functional interfaces.

When a subject accesses a resource, state awareness is carried out on the basis of the demand submitted by the task management component and using the state information supplied by the identity management component, the resource management component and the environment awareness component; the policy decision component generates the policy decision through trust evaluation; the policy enforcement component enforces the policy decision and carries out least privilege access control. Throughout the access, the protection of the accessed resource is put into effect through the cyclical process of continuous state awareness, dynamic trust evaluation and least privilege control. The cryptographic service component provides cryptographic support over the whole process.

The control layer and the data layer are two logical layers: control information is transmitted and processed at the control layer, and data are securely transmitted and processed at the data layer.



## 6 Core components

6.1 Policy decision component. The policy decision component consists of the policy engine and the policy manager; its main functions are the following. a) Policy engine: it decides on the access rights of the subject to the resource; on the basis of the security policy and the information supplied by the supporting components it carries out trust evaluation continuously and makes the access control decision to permit, refuse or revoke. b) Policy manager: it issues the control instructions for the connection between the subject and the resource; relying on the access control decision made by the policy engine, it issues to the policy enforcement component the instructions to set up, maintain or block the secure data channel.

6.2 Policy enforcement component. Under the management of the policy decision component, the policy enforcement component carries out identity authentication and controls the secure data channel between the subject and the resource. a) Identity authentication: following the instructions of the policy decision component, and in cooperation with the supporting components, it carries out identity authentication on the subject. b) Control of the secure data channel: following the instructions issued by the policy manager, it starts, monitors and terminates the secure data channel between the subject and the authorized resource.

## 7 Supporting components

7.1 Task management component. It coordinates the grounds on which the subject seeks access, drives the task by which the subject accesses the resource - including the task objective, the task responsibility and the task flow - and connects to the entity rights. It provides the subject, the resource, the core components and the other supporting components with the associated task lifecycle management service, the task and resource rights coordination service, the task approval service, the task authentication service and the task audit service, as well as the task-related information, including subject task attribute information, resource task attribute information, task state information, task approval information and task audit information.

7.2 Identity management component. It provides the subject, the resource, the core components and the other supporting components with the entity identity management service, the entity identity attribute association service, the personal entity identity authentication service, the device identity authentication service and the entity rights management service, as well as the identity-related information, including entity identity, entity identity information, entity attribute information and entity rights information.

7.3 Resource management component. It provides the subject, the resource, the core components and the other supporting components with the data resource management service, the device resource management service, the network resource management service, the computing resource management service, the application resource management service, the resource entity identity authentication service, the resource attribute association service and the resource business coordination management service, as well as the resource-related information, the resource grading and classification information, the device configuration information, the resource identity information, the resource access rights information and the resource access context information. Resource management takes the resource unit as the smallest unit, and several resource units combine into the accessed resource. Resource units associated with the same resource identity have unified resource attributes and enforce a common security policy.

7.4 Environment awareness component. While a subject accesses a resource, it collects network traffic, asset information, logs, vulnerability information, user behaviour, threat information and similar data, and analyses the network behaviour and the user behaviour during the access, so as to let the subject, the resource, the core components and the other supporting components obtain, understand, trace back and display the state changes and the change trends of the subject, of the resource and of the access environment.

7.5 Cryptographic service component. It secures the authenticity of the entity identity of the subject, the resource, the core components and the other supporting components, the confidentiality and integrity of the data, and the non-repudiation of the operating behaviour. It provides the subject, the resource, the core components and the other supporting