ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 28455-2026

Replacing GB/T 28455-2012

Cybersecurity technology - Entity authentication involving a trusted third party and access architecture specification

网络安全技术 引入可信第三方的实体鉴别及接入架构规范

Issued on: May 25, 2026 **Implemented on: December 1, 2026**

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

Table of Contents

5 Overall Architecture

5.1 General Rules This chapter describes the structural framework, control functions, and devices employing this mechanism in an entity authentication and access system that introduces a trusted third party. The relationship between the various operations performed. The entity authentication and access system that introduces a trusted third party adopts a three-element peer-to-peer architecture (TePA), as shown in Figure 1, which sets the entities participating in the authentication to... In a peer-to-peer manner, a trusted third party (authentication server system) is introduced, and logical port control methods are used to complete the authentication and endpoint verification between the two parties. Authorization via authentication. Authentication between the requester system and the authentication access controller system can be achieved through an authentication server acting as an intermediary, using an authentication protocol. It runs on three entities. the requester system, the authentication access controller system, and the authentication server.

5.2 Access Control Requirements In an entity authentication and access architecture that introduces a trusted third party, the system port should provide a point of contact between the requester and the authentication access controller. Connections to the point. The requester and the authentication access controller, and the authentication access controller and the authentication server, perform entity authentication protocol interactions and, according to... The result of the protocol execution determines the port status of the requester and the authentication access controller, thereby implementing access control.

5.3 System Roles and Port Technical Requirements

5.3.1 System Role Requirements A system port is a channel for service access and

provision. A port allows external systems to access the services provided by this system, and also allows internal systems to access the services provided by this system. The system provides services to the outside world through ports. A trusted third-party entity authentication and access architecture is introduced to ensure system port status by controlling the system's entity authentication and access architecture. Only authorized systems can access the services provided by this system, or access the services provided by authorized systems. The device's role should meet the requirements of the following three roles.

5.3.2 Technical Requirements for Controlled and Uncontrolled Ports

5.3.2.1 General Port Requirements The system introduces a trusted third-party entity authentication and access architecture. The connection point between the system and the link is a physical port or a logical port, and this port should provide... Provide one-to-one connections to other systems; two distinct access points should be established at the connection points between the system and the link. a controlled port and an uncontrolled end. The port should meet the following requirements.

a) The uncontrolled port and the controlled port are two parts of the same connection point, both receiving data frames from the physical connection point;

b) Uncontrolled ports, regardless of authorization status, allow uncontrolled exchange of data packets between systems on the link;

c) Controlled ports are only allowed to exchange data packets when they are in an authorized state.

Note. Although data packets can be obtained on both controlled and uncontrolled ports, a protocol entity can only be associated with one port at a time.

5.3.2.2 Port Control Technical Requirements Controlled and uncontrolled ports are logical concepts that categorize data flows. Management and control flows can be managed through uncontrolled ports. The information flow is controlled through a controlled port without affecting the system's communication management. The controlled port status parameter (AuthControledPortStatus) and the results of LAC control are shown in Figure

2.In System 1 of Figure 2... In System 1, because the LAC to the link connection point is operable, both controlled and uncontrolled ports can access the link; while in System 2, because... The LAC at the link connection point is inoperable; neither controlled nor uncontrolled ports can access the link. This inoperability of the LAC also leads to This causes the controlled port status of the system to be unauthorized.

5.3.2.3 Control Parameter Requirements for Controlled Ports In addition to the controlled port status parameters, administrators use the controlled port control parameter (AuthControledPortControl) to control... The port's authorization status. Controlled port

control parameters have three possible values. Force Authorized, Auto, and Force Not Authorized. The authorization setting (ForceUnauthorized) defaults to automatic. The relationship between controlled port status parameters and controlled port control parameters should meet the following requirements. The following requirements must be met.

a) When the controlled port control parameter value is "forced authorization", the authentication access controller or requester state machine will change the controlled port state. The value of the state parameter is set to authorized; that is, the controlled port is unconditionally set to authorized.

b) When the controlled port control parameter is set to automatic, the authentication access controller and requester state machine determine the requester and authentication access controller based on the requester and the authentication access controller. The result of the authentication exchange between the controller and the authentication server determines the value of the controlled port status parameter;

c) When the controlled port control parameter value is forced unauthorized, the authentication access controller or requester state machine will control the controlled port. The status parameter is set to unauthorized, meaning the controlled port is unconditionally set to unauthorized. In the three cases described above, the value of the controlled port state parameter directly reflects the port state in the authentication access controller and the requester state machine. The value of the (portStatus) variable.

5.3.2.4 Port Status Variable Requirements The value of the port status variable is affected by the following three factors, and the port status change should meet the following requirements.

a) Identify the authorized state of the access controller state machine. if no state machine is implemented on the port, it is considered "authorized".

b) Authorization state of the requester's state machine. If the port does not implement a state machine, it is considered "authorized".

5.4 Port Access Entity

5.4.1 Overview The Port Access Entity (PAE) operates on the protocols defined in Chapter

8.For systems that support port access control, regardless of... Whether the system acts as a requester or an authentication access controller, a PAE exists on each port.

a) The PAE that plays the role of the requester in the authentication exchange is called the requester PAE.

b) The PAE that plays the role of authentication access controller is called authentication access controller PAE. Both PAE roles control the authorized/unauthorized status of the controlled port based on the results of the authentication process.

5.4.2 Identifying Access Controller Role Requirements The authentication access controller should meet the following requirements.

a) The authentication access controller (PAE) should be responsible for authenticating requesting PAEs connecting to its controlled ports and for authenticating the controlled ports. The authorization status is controlled accordingly;

b) During the authentication process, the Authentication Access Controller (PAE) can use the authentication server;

c) The authentication server may be in the same system as the authentication access controller, or in a system that can be accessed via remote communication mechanisms, LAN, or other means. Other systems that access via other mechanisms;

d) Communication between the requester PAE and the authentication access controller PAE, and communication between the authentication access controller PAE and the authentication server (when authentication...). When the authentication server and the authentication access controller are not in the same system, communication should preferably be conducted through the procedures described in Chapter 8. Finish.

5.4.3 Requester Role Requirements The requester should meet the following requirements.

a) The requester PAE is responsible for sending the requester's authentication credentials to the authentication access controller PAE, as a confirmation of the authentication access control. The response to the PAE request;

b) The requesting PAE shall control the authorization of the controlled port based on the result of the authentication exchange with the authentication access controller PAE. state;

c) The requester PAE can initiate an authentication exchange to complete a specific deregistration exchange.

5.4.4 Port Access Restrictions Authentication is triggered during system initialization or when the requesting system connects to the authentication access controller system's port. Authentication is performed on each end. Ports are configured, and in some configurations, authentication of specific ports is not required. Port access should meet the following requirements.

5.4.5 TAEP Reuse Model

5.4.5.1 General Requirements The TAEP reuse model should conform to the requirements in Figure

4.The dashed line in Figure 4 indicates an optional part; whether this part is effective during operation is determined by... The TAEP identification method is determined.

5.4.5.2 Lower Layer and Transport Layer The underlying and transport layers are responsible for transmitting and receiving TAEP packets between the requester, the