ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 47697-2026

Cybersecurity technology - Authentication and authorization - Specification for the attribute-based access control model and its management

网络安全技术 鉴别与授权 基于属性的访问控制模型与管理规范

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

Foreword

6.1 Overview ABAC defines and implements access control policies based on attributes. ABAC attributes reflect subject identity, object characteristics, and operations. Information such as type and environment status are used as attributes in access control decisions. ABAC introduces more discrete input variables into the access control decision-making process by using attributes, thus defining richer and more explicit strategies. Express.

6.2 Attribute Classification

6.2.1 Main Attributes A subject refers to the initiator of an access control action, which can be a natural person or a non-natural person entity. Each subject is assigned a set of subject attributes. Subject attributes are a collection of characteristic information describing a subject, and can be divided into two categories. natural subject attributes and authorized subject attributes.

a) Natural Subject Attributes. These describe attributes inherent to a subject that do not change with the context of access control operations. For example, an individual. Identity information, personal biometric information, etc.

b) Authorized Subject Attributes. A set of attributes describing the access permissions assigned to a subject in a given access control operation context, along with the permissions granted... It changes dynamically depending on the context. For example, the role, job function, employee number, domain name, or URL assigned to the subject. Authorizing the subject... Subject attributes reflect a subject's role, permission level, and temporary state within a specific access control environment. These attributes change with the subject's characteristics and access permissions. The system is dynamically adjusted in response to changes in the environment and business needs.

6.2.2 Object Attributes An object is the target of access control behavior, and each object is

assigned a set of object attributes. Object attributes are a collection of characteristic information describing an object, and can be divided into two categories. natural object attributes and authorized object attributes.

a) Natural object attributes. Describe attributes that are inherent to the object after its creation and do not change or change infrequently with a given access control operation context. Attributes typically describe basic information or physical characteristics of an object. Examples include database primary keys, timestamps, file extensions, and encoding methods. And digital fingerprints, etc.

b) Authorized Object Attributes. Describes a set of attributes assigned to an object for access within a given access control context, depending on the given context. These parameters change dynamically depending on the object. Examples include the object's assigned number, owner, creation and deletion dates and times, and authorization level. These attributes reflect the state, permission settings, and temporary characteristics of objects under different access control environments, and are typically based on management systems. It is set according to the degree and business needs.

6.2.3 Environmental Attributes Environmental attributes refer to access environment status information that is independent of any specific subject or object and participates in determining access control operations. For example... Current date, time, location, threat type, and system status, etc. Environmental attributes are not passively created and managed, but are intrinsic and can be... ABAC system detection. When an authorized access request is made, the environment attributes are evaluated based on the currently matched environment variables. The environment attribute is access control. The definition of special or dynamic rules specified in the strategy provides a basis for this.

Note. When environment attributes are used to form access control rules, the environment attribute variables and their values are tamper-proof.

6.3 Attribute Metadata Before implementing access control, ABAC identifies, defines, and describes a standardized set of metadata. The metadata for an attribute is the metadata for each attribute. Basic information elements mainly include attribute value information, attribute creation information, and attribute source information.

a) Attribute value information. such as update frequency, validity period, etc.

b) Property creation information. For example, whether the property is self-asserted or retrieved from the property authorization system.

c) Attribute source information. such as the identifier of the attribute source. In the access control decision-making process, standardized attribute metadata is used to assess the credibility of attributes by evaluating the authority of the attribute's source. Metadata of attributes such as sex, timeliness of attribute information, and accuracy of attribute information verification frequency are used to score the credibility of attributes, defining

attributes. The authenticity, security, and timeliness of attributes. The assessment results of attribute credibility can be used as part of the input for access control decisions, enabling fine-grained decision-making. Access control. In attribute management, attribute metadata is used to group and classify attributes, avoiding the need to assign a specific attribute to each subject or object. Similar attributes can be used to improve the flexibility of access control and the convenience of attribute management. For example, based on the common characteristics of subjects or objects in the system, Subjects or objects are divided into different groups, and each "group" is the metadata of the attribute.

7 Strategies

7.1 Strategy Formulation In ABAC, policies are attribute-based rules or sets of rules used to determine whether access control is authorized. Policy formulation... The principles are as follows:

a) The strategy is formulated according to condition-outcome logic, that is, under certain attribute combinations, a subject is allowed or denied access to a certain object. What operation should be performed?

b) In the process of defining the strategy, pre-determine the subject attributes, object attributes, and environmental attributes;

c) In defining policies, the access control operations described by the policies originate from the organization's internal business processes, management systems, etc.

7.2 Strategy Expression

7.2.1 Strategy Expression Form Strategy expression is the process of transforming natural language, which is understandable to humans from a business and management perspective, into a formal language that can be executed by machines. The forms of expression include two types. natural language strategies and digital strategies.

a) Natural language policies are the natural language expression of access control policies and should conform to the principles of policy definition. For example, condition-result logic... It describes access control policies, but cannot be directly executed by the machine.

b) A numeric policy is an access control policy expression that can be directly encoded into machine-readable and executable code. Numeric policy statements It consists of subject and object attributes, as well as environmental attributes that satisfy the access control operation. The transition from natural language strategies to digital strategies involves two stages.

a) Phase One. Transform the natural language policy into a set of access control rules that are still described in natural language and are deployable and enforceable. In this phase, the combination of subject attributes and object attributes in the strategy and the permitted

operations should be determined.

b) Phase Two. Using technical means, convert access control rules into machine-executable digital policies.

7.2.2 Strategy Expression Language A policy expression language is a programming language used to describe access control policies. The basic requirements of ABAC for a policy expression language are primarily... include.

a) Provide a method for making authorization decisions based on the attributes of the subject and the object;

b) Provides a set of logical and mathematical operators to handle the attributes of subjects, objects, and environments;

c) Provide a method to combine individual rules and policies into a policy set so that it can be applied to a given decision request;

d) Provide a method for defining the process of combining strategies and rules;

e) Provide a method for handling multivalued attributes.

8 ABAC Engine

The ABAC engine is the core component of the ABAC model. The ABAC engine combines policy, subject attributes, object attributes, and environment attributes. They are put together, and then strategy matching and logical calculations are performed to execute the strategy decision. An ABAC engine typically includes four functions. policy determination, policy execution, policy management, and attribute provision. The system components of this engine are referenced below. See Appendix A for the architecture. The ABAC engine should be able to manage the decision-making and execution process of strategies, including the retrieval strategy and the order in which different types of attributes are retrieved. And the determination of attribute sources, etc. 9.ABAC Management Requirements

9.1 Attribute Management

9.1.1 General Requirements The general requirements for attribute management include the following.

a) Authorized attributes should be provided by an attribute licensing authority. In scenarios where multiple attribute licensing authorities coexist, each authority should provide the attributes it needs. Subjective attributes and object attributes each possess authority;

b) The attribute authorization body should identify all attribute information and compile it into an attribute list so that when defining each access control policy, it can be used to identify all attributes. It has corresponding attributes;