GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80
File No.: 44633-2014

GM/T 0032-2014

Specifications for role based privilege management and access control

基于角色的授权与访问控制技术规范

Issued on: February 13, 2014 **Implemented on: February 13, 2014**

Issued by: State Cryptography Administration

Table of Contents

Foreword

This Standard was drafted in accordance with the rules given in GB/T 1.1-2009.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The issuing authority shall not be held responsibility for identifying any or all such patent rights.

This Standard was proposed by and shall be under the jurisdiction of Code Industry Standardization Technical Committee.

Drafting organizations of this Standard: Changchun Jida Zhengyuan Information Technology Co., Ltd., Wuxi Jiangnan Information Security Engineering Technology Center, Chengdu Westone Information Industry Co., Ltd., Shandong De'an Information Technology Co., Ltd., Shanghai Koal Software Co., Ltd., Beijing Digital Certificate Certification Center Co., Ltd., Shanghai Digital Certificate Certification Center Co., Ltd., Wanda Information Co., Ltd., Xingtang Communication Technology Co., Ltd.

Drafters of this Standard: Liu Ping, Li Weiping, Zhao Lili, He Changlong, Xu Qiang, Li Yuanzheng, Gao Zhiquan, Tan Wuzheng, Li Shusheng, Cui Jiuqiang, Zhou Dong, Wang Nina.

Specifications for role based privilege management and access control

1 Scope

This Standard specifies the role-based privilege and access control framework structure and the logical relationship between the various components within the framework, defines the functions, operating procedures and operating protocols of each component, and defines the uniform format of access control policy description language and privilege policy description language, and the standard interface for access control protocols.

This Standard is applicable to the development of role-based privilege and access control systems under the public key cryptography technology system, and may guide the detection of such systems and the development of related applications.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the dated edition cited applies. For undated references, the latest edition of the referenced document (including all amendments) applies.

GB/T 20519 Information security technology - Public key infrastructures - Privilege Management Center technical specification

GM/T 0019 Universal cryptography service interface specification

3 Terms and definitions

For the purpose of this document, the following terms and definitions apply.

3.1

access control decision

Evaluation result of the access control decision function to the access request.

3.2

access control decision function

Component responsible for making the decision on the access request.

3.3

access control enforcement function

Component that performs the access control policy function.

3.4

access control policy

Binding relationship, determined by the application, between roles and resources.

3.5

access control policy certificate

Attribute certificate that carries the application access control policy.

3.6

contextual information

Environmental information related to the access decision result when the request is happening.

3.7

privilege management

Management of the distribution relationship between subjects and roles.

3.8

privilege information

Information that identifies the distribution relationship between subjects and roles.

3.9

privilege certificate

Attribute certificate that carries the privilege information.

to complete the binding of subjects and roles, roles and resources, such as using privilege certificates and access control policy certificates. When using the attribute certificate to carry the binding relationship, the system shall follow the requirements of GB/T 20519.

5.4 Access control enforcement function (AEF)

The AEF receives the access request, encapsulates the access request according to the access control protocol and controls the access to the resource based on the decision result.

When the decision result is “permit”, the AEF authorizes the initiator's access to the resource; if the decision result is “deny”, the AEF shall block the initiator's access to the resource.

The use mode of the AEF includes share and non-share. In the share mode, multiple applications use one AEF; in the non-share mode, each application uses its own AEF.

5.5 Access control decision function (ADF)

The ADF makes the decision on the access request based on the privilege information, the access control policy and other information.

The input of the ADF includes the access request, the privilege information, the access control policy and the ADF retention information. The output of the ADF is the access control decision result.

The ADF decision result includes “permit” and “deny”. “Permit” means that the access request meets the resource's access control policy constraints; “deny” means that the access request does not meet the access control policy constraints.

The input and output information of the ADF is shown in Figure 3.

1) Initiator identity:

The initiator identity includes three types, which are:

- simple string;

- signature certificate serial number + signature certificate issuer subject;

- signature public key.

2) Resource information:

The resource information is the resource identity string carried in the access request.

3) Contextual information:

The contextual information is the information related to the access request and capable of identifying the environment characteristics of the access request. It may need this information when making access request decisions. They are, respectively:

- time: the time when the access request is initiated;

- location: the source address where the access request is initiated;

- type of initiator identity;

- custom information: the information defined by the application, participating in the access decision.

4) Role identity:

The role identity is the role information that the subject shall use to access resources in the current scenario when an access occurs.

See Clause 8 for detailed access request formats.

5.5.2 Privilege information

The privilege information in the role-based privilege and access control model refers to the binding relationship between subjects and roles.

See Clause 7 for a detailed description of privilege information.

The privilege information of the initiator may be carried by using the privilege certificate, or may be carried by other methods, but the authenticity and integrity of the privilege information shall be ensured.

see the definition of access request carrying protocol. For example, the HTTP protocol defines the GET, POST and other actions.

6.1.2 Rules

The rule is the criteria for controlling access to the resource, including four elements: roles, resources, actions and conditions, among which conditions are optional factors. The evaluation result may be “permit” or “deny”. Multiple rule evaluation results for the same resource shall be combined into a single evaluation result using the merge algorithm.

The ADF selects appropriate rules based on the role of the access request initiator and resources, actions and related environmental factors of the request.

For unconditional rules, the access request initiator may perform corresponding actions on the resource as long as it is the role specified in rules. For conditional rules, the access request initiator shall be the role specified in rules and meet the requirements of the conditions before performing corresponding actions on the resource.

For conditional rules, the evaluation result of rules depends on the evaluation result of conditions. The ADF evaluates each condition and combines multiple condition evaluation results into a logical expression through the logical combination algorithm, which finally forms the evaluation result for all conditions.

6.1.3 Conditions

The condition is the contextual restriction (such as the time limit of actions) that shall be satisfied when performing the specified action on the resource. The evaluation result is TRUE or FALSE.

The condition is a relational expression consisting of one of four kinds of contextual information: time, location, initiator identity type and custom information. Multiple conditions may be connected by using logical operators and form a logical expression.

This Standard defines conditional relational operations and logical operations. Table 1 is a list of relational operators and their meanings; it gives the operation rules with results TRUE and FALSE. Table 2 is a list of logical operators and their meaning; it gives the logical operation rules.

control decision result to the AEF in the form of the access control response message (Response).

The access control request consists of Version, Subject, Resources, Actions, Environment and Role, which represent the version number of the protocol, the initiator of the access request, the access target (resource), the actions, the contextual information of the access request and the role identity. This information comes from the environment of the access request message and the AEF.

This Standard specifies that the version (Version) defaults to the integer 1.

The attribute DomainCode is the code of the application that identifies the application that the initiator will access.

For definitions of the Subject, Resources, Actions and Environment, see 8.2.3, 8.2.6, 8.2.7 and 8.2.8.

8.2.3 Initiator (Subject)

```
<xs:element name = "Subject" type = "SubjectType"/>
  <xs:complexType name = "SubjectType">
    <xs:sequence>
      <xs:element ref = "entityNameType"/>
      <xs:element ref = "baseCertificateIDType"/>
    </xs:sequence>
</xs:complexType>
```

The initiator carries the access initiator identity information. This Standard supports two kinds of initiator representation forms, namely entity name type (EntityNameType) and basic certificate binding type (baseCertificateIDType). However, the initiator identity in access control request messages shall not occur at the same time with more than one representation form. When the AEF constructs the access control request message, it shall decide which initiator identifier representation form to choose.

8.2.4 Entity name type (entityNameType)

```
<xs:element name = "entityNameType" type = "xs:string"/>
```

The entity name type (entityNameType) is a representation form of the initiator identity. The entity name type uses simple strings to represent the initiator identity, such as "entity A" or "cn = entity name, o = organization name, c = cn" and other forms. The ADF shall use the entirety of the entity name type value as the initiator identity. This Standard does not specify the internal grammar of the entity name type value, which may be freely defined as needed by the

2) when the access control request does not comply with the access control policy constraint, the decision result shall be “Deny”, meaning that the AEF shall prohibit the access to the resources by the request;

3) when an exception occurs in the ADF, the decision result shall be “Exception”, and the ADF’s exception information is placed in the decision status (Status).

8.3.5 Decision status (Status)

```
<xs:element name = "Status" type = "StatusType"/>
<xs:complexType name = "StatusType">
  <xs:sequence>
    <xs:element name = "StatusCode" type = "xs:string"/>
    <xs:element name = "StatusMessage" type = "xs:string"/>
  </xs:sequence>
</xs:complexType>
```

The type of decision status (Status) is the decision status type (StatusType). It consists of StatusCode and StatusMessage, which respectively represent the code of the decision status and the detailed information of the decision status type.

See Annex A for the code and detailed information of the decision status.

9 Requirements for application systems

9.1 AEF implementation

In addition to being implemented as a stand-alone service as shown in Figure 2, AEF can also be implemented directly by the application system.

9.2 Expression of roles

The expression of roles includes the determination of the role name and the role value. The role name is to provide an understandable symbol for privilege management to facilitate human-computer interaction. The role value is a code that uniquely represents the role that is different from other roles and is suitable for computer processing.

The expression of roles determines the number of roles that can be assigned, the range of values for the role and their internal relationships. In general, the role expression shall be relatively stable after the application function is determined.

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

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