ICS 35.040
L 80
备案号:44633—2014

GM

中华人民共和国密码行业标准

GM/T 0032—2014

基于角色的授权与访问控制技术规范

Specifications for role based privilege management and access control

2014-02-13 发布　　2014-02-13 实施

国家密码管理局　　发 布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：长春吉大正元信息技术股份有限公司、无锡江南信息安全工程技术中心、成都卫士通信息产业股份有限公司、山东得安信息技术有限公司、上海格尔软件股份有限公司、北京数字证书认证中心有限公司、上海市数字证书认证中心有限公司、万达信息股份有限公司、兴唐通信科技有限公司。

本标准起草人：刘平、李伟平、赵丽丽、何长龙、徐强、李元正、高志权、谭武征、李述胜、崔久强、周栋、王妮娜。

基于角色的授权与访问控制技术规范

1 范围

本标准规定了基于角色的授权与访问控制框架结构及框架内各组成部分的逻辑关系，定义了各组成部分的功能、操作流程及操作协议，定义了访问控制策略描述语言、授权策略描述语言的统一格式和访问控制协议的标准接口。

本标准适用于公钥密码技术体系下基于角色的授权与访问控制系统的研制，并可指导对该类系统的检测及相关应用的开发。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 20519 信息安全技术 公钥基础设施 特定权限管理中心技术规范

GM/T 0019 通用密码服务接口规范

3 术语和定义

以下术语和定义仅适用于本文件。

3.1

访问控制判定 access control decision

访问控制决策部件对访问请求的评估结果。

3.2

访问控制决策部件 access control decision function

负责对访问请求做出判定功能的部件。

3.3

访问控制执行部件 access control enforcement function

执行访问控制策略功能的部件。

3.4

访问控制策略 access control policy

由应用确定的角色与资源的绑定关系。

3.5

访问控制策略证书 access control policy certificate

承载应用访问控制策略的属性证书。

3.6

上下文信息 contextual information

访问发生时与访问判定结果相关的环境信息。

3.7

授权管理 privilege management

对主体与角色间的分配关系的管理。