ICS 35.040
L 80

中华人民共和国国家标准化指导性技术文件

GB/Z 24294.3—2017
部分代替 GB/Z 24294—2009

信息安全技术 基于互联网电子政务信息安全实施指南 第3部分:身份认证与授权管理

**Information security technology—
Guide of implementation for Internet-based e-government information security—
Part 3:Identity authentication and authorization**

2017-05-31 发布　　2017-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/Z 24294《信息安全技术　基于互联网电子政务信息安全实施指南》分为4个部分：

——第1部分：总则；

——第2部分：接入控制与安全交换；

——第3部分：身份认证与授权管理；

——第4部分：终端安全防护。

本部分为GB/Z 24294的第3部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分部分代替GB/Z 24294—2009《信息安全技术　基于互联网电子政务信息安全实施指南》，与GB/Z 24294—2009相比，主要技术变化如下：

——新增了统一身份认证与授权管理的安全功能；

——新增了统一身份认证技术要求；

——新增了统一授权管理技术要求；

——针对信任体系建设，补充了身份认证与授权管理系统的部署示例。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位：解放军信息工程大学、中国电子技术标准化研究所、北京天融信科技有限公司、郑州信大捷安信息技术股份有限公司。

本部分主要起草人：陈性元、杜学绘、孙奕、夏春涛、曹利峰、张东巍、任志宇、罗锋盈、上官晓丽、董国华。

本部分所代替标准的历次版本发布情况为：

——GB/Z 24294—2009。

引　言

由于基于互联网电子政务具有网络开放性的特点，电子政务系统面临着身份假冒、信息泄漏、非授权访问等安全威胁，利用身份认证、授权管理等技术可有效提高互联网电子政务系统的安全性。

为推进互联网在我国电子政务中的应用，指导基于互联网电子政务身份认证与授权管理技术规范工作，特制定本部分内容。

本部分首先对互联网电子政务中身份认证与授权管理的安全功能进行规范，之后分别针对身份认证和授权管理实施过程中的技术规范进行详细描述，并对互联网电子政务安全接口进行规范。

本部分主要规范在基于互联网电子政务系统中实施身份认证和授权管理所进行的技术活动及其相关的管理活动。

信息安全技术
基于互联网电子政务信息安全实施指南
第3部分:身份认证与授权管理

1 范围

GB/Z 24294的本部分给出了互联网电子政务中身份认证与授权管理的实施指南,明确其功能要求和安装部署要求,定义身份认证与授权管理技术规范。以依托互联网构建可信政务服务平台为目标,为建立可信、可管、可控的基于互联网电子政务信息系统提供技术指导。

本部分适用于基于互联网电子政务系统中身份认证与授权管理系统的设计、研发与建设,为管理人员、工程技术人员、信息安全产品提供者构建统一身份认证与授权管理系统提供管理和技术参考。涉及国家秘密,或所存储、处理、传输信息汇聚后可能涉及国家秘密的,按照国家保密规定和标准执行。

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。

GM/T 0015—2012 基于SM2密码算法的数字证书格式规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

属性授权机构 attribute authority

通过发布属性证书来分配权限的认证机构,也称属性管理机构。

3.2

属性证书 attribute certificate

属性授权机构进行数字签名的数据结构,把持有者的身份信息与一些属性值绑定。

3.3

特定权限管理基础设施 privilege management infrastructure

支持授权服务的综合基础设施,与公钥基础设施有着密切的联系。

4 缩略语

下列缩略语适用于本文件。

LDAP 轻量级目录访问协议(Lightweight Directory Access Protocol)

PMS 授权管理系统(Privilege Management System)