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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 1
5　统一身份认证与授权管理安全功能 …… 2
5.1　统一身份认证功能 …… 2
5.2　授权管理功能 …… 2
5.3　系统部署要求 …… 2
5.4　存储安全要求 …… 2
6　统一身份认证技术规范 …… 2
6.1　统一用户标识 …… 2
6.2　身份认证方式 …… 4
6.3　密码算法 …… 4
6.4　认证协议 …… 4
7　统一授权管理技术规范 …… 4
7.1　角色管理 …… 4
7.2　资源管理 …… 5
7.3　权限管理操作 …… 5
7.4　授权管理系统服务模式 …… 7
附录 A（资料性附录）　身份认证与授权管理系统应用示例 …… 9
附录 B（资料性附录）　授权管理系统策略表示方式 …… 11

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)

5 统一身份认证与授权管理安全功能

5.1 统一身份认证功能

统一身份认证系统要求域内统一部署，为多种应用系统提供认证服务：

a) 支持单点登录功能，避免重复认证，减少认证服务负担；

b) 根据应用的不同安全需求可采用不同的认证凭证以及多种凭证的组合，凭证的类型可分为口令、数字证书、生物特征等；

c) 对用户身份信息进行安全存储，能够有效防止用户敏感信息泄漏；

d) 认证协议安全，能够有效防止篡改、重放、假冒等攻击；

e) 支持统一的身份认证服务接口，便于与不同种类应用系统集成或二次开发。

5.2 授权管理功能

授权管理在用户管理的基础之上，对用户访问资源的权限进行统一的标识与管理，是基于互联网电子政务系统的必选配置。授权管理系统主要功能如下：

a) 授权管理系统支持物理分级部署，既可实现分布式授权管理，还可支持单域环境内集中式的授权管理；

b) 支持 PMS 内部的多管理员管理，通过为管理员划分管理范围，实现授权管理系统内部的分级管理；

c) 采用基于角色的授权管理方式，支持跨域授权，可通过推荐角色的方式，也可通过用户跨域申请授权的方式来实现跨域授权；

d) 为用户授权支持无属性证书方式，或属性证书方式，若采用属性证书方式，则提供属性证书的生成、更新、撤销、恢复等操作功能；

e) 提供人员信息同步接口、用户授权接口、角色授权接口等外部接口。

5.3 系统部署要求

统一身份认证系统由统一身份认证服务器和统一用户管理系统组成，统一身份认证服务器部署于互联网电子政务系统中的安全服务区域，统一用户管理系统部署于安全管理区域。统一授权管理系统作为安全管理中心的一部分，与统一用户管理系统一起部署于安全管理区域。系统的部署示例和工作流程参见附录 A。

5.4 存储安全要求

对统一用户管理系统中的用户的认证信息进行安全存储与管理，禁止明文存储，采用加密或哈希运算后存储，并使用数据库权限安全限制。统一授权管理系统中的授权信息存储于授权管理数据库中，与统一授权管理系统一起部署于安全管理区域，除管理员登录信息需加密或哈希后存放以外，其余信息可明文存放。

6 统一身份认证技术规范

6.1 统一用户标识

6.1.1 统一用户身份信息

基于互联网电子政务系统需要根据政府部门的实际情况将用户信息进行统一管理。统一用户身份

信息是指采用统一的用户身份信息规范，以记录、存储和描述每一个用户的身份信息。用户身份信息包括统一用户编码、用户名称、用户基本信息、用户身份认证信息、用户身份扩展信息等。

6.1.2 统一用户编码

统一用户编码根据政府部门、人员编制情况，通过为每一个用户、部门进行统一编码，使其在互联网电子政务的身份认证系统中具有唯一的标识。

系统利用树形结构组织部门与用户信息，对其进行分级管理。人员管理系统是树的根节点，下设的各一级部门是根节点的子节点；一级部门管理的用户和下级部门是其子节点；下级部门又可继续下设用户及子部门；以此类推，所有的部门节点与用户节点构成“用户树”，该树的非叶子节点（用户节点不能建立下级节点）构成“部门树”。

依据上述树形结构，将信任域内的部门、人员身份按照统一的编码方案进行编码，树中每一节点由根开始编码。

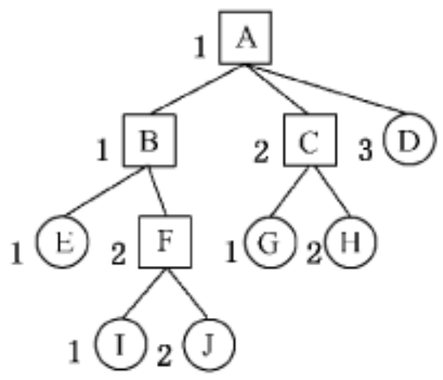

图 1 统一用户编码方式

统一用户编码方式的示意图如图 1 所示的树形结构中，节点编号是由一个整数序列组成，代表部门或用户身份，整数之间以圆点分割，整数的个数决定了该节点的深度。例如根结点 1 代表用户管理中心 A，1.1 代表 A 下设的一级部门 B，1.1.2 代表 B 的下级部门 F，1.1.2.1 代表部门 F 的负责人，而 1.1.2.2 可表示该部门的第一副职领导。根据编码也可解析出对应节点的编号。

在添加部门或用户时，编码由系统根据当前编码情况自动生成，编码一经生成，不能再修改，删除的编码不再重用。当编码空间加入到其他编码空间中时，为该编码空间加上统一前缀以实现扩展。

6.1.3 用户名称

用户名称表示此用户在互联网电子政务系统中的唯一名称。

6.1.4 用户基本信息

用户基本信息表示用户个人基本情况信息。用户基本信息主要包括用户姓名、性别、年龄、民族、籍贯、出生日期、工作日期、政治面貌、入党（团）时间、职务、级别、职称、类别、证件类别、证件号码、住址、电话号码、邮箱等。

6.1.5 用户身份认证信息

用户身份认证信息表示此用户在互联网电子政务系统中用于身份认证的相关特征信息。用户身份认证信息主要包括此用户的认证方式和每种认证方式对应的特征信息。认证方式包括口令认证、证书认证、指纹认证、人脸影像认证等多种认证方式，其中，口令认证、证书认证是较常用的认证方式，指纹认证、人脸影像认证等方式属于生物特征认证方式，用于安全级别较高的应用场景。认证方式对应的特征信息包括用户口令、证书信息、生物特征值等信息。

6.1.6 用户身份扩展信息

用户身份扩展信息表示此用户在互联网电子政务系统中与身份相关的扩展信息。用户身份扩展信息包括用户简历、工作履历、奖惩情况等信息。

6.2 身份认证方式

6.2.1 口令认证

口令认证适用于基于互联网电子政务系统中政务服务应用。口令认证的基本过程是认证系统通过比较用户输入的口令与系统内部存储的口令是否一致来判断用户的身份。

口令不能以明文形式传输和存储，必须以口令的散列值或加密后的密文传输和存储。用户进行口令方式认证时，除需要输入用户名和口令之外，还要输入校验码进行登录。

6.2.2 数字证书认证

数字证书认证通过数字证书获取用户的公钥信息，并利用公钥验证用户提交的消息签名值是否合法以鉴别用户身份。数字证书认证适用于互联网电子政务系统中政务办公应用。

6.2.3 生物特征识别

生物特征认证利用人类本身所拥有且能标识其身份的生物特征进行身份认证。生物特征认证方式主要包括指纹鉴别、虹膜兼备、影像鉴别等，用于互联网电子政务系统中政务办公应用。

6.2.4 面向信息分类防护的认证方式选择

用户在进行访问时，认证服务器需根据用户所访问的资源类型，强制用户采用与其资源类别相适应的认证方式。

6.3 密码算法

密码安全产品的使用以及产品所使用的密码算法应符合国家密码管理的有关规定。

6.4 认证协议

认证协议是通信参与者为完成相互的身份认证或识别而采用的规程、约定、约束和交换信息的总和。在认证系统对用户、终端、设备、装置等进行身份认证的过程中，应选用安全的认证协议，为其提供机密性、完整性、不可否认性保护，抵御消息重放、第三方假冒等攻击。

7 统一授权管理技术规范

7.1 角色管理

7.1.1 角色的层次结构

互联网电子政务系统中，角色可根据组织结构中的岗位职责进行定义，也可根据应用系统中的功能划分来进行定义。角色层次组织成树形结构，允许一个角色拥有多个子角色和至多一个父角色。

7.1.2 角色的编码原则

根据角色的层次关系，授权管理系统对角色进行统一的编码。角色的编码应遵循以下原则：

a) 在角色层次中，每一个角色的编码都是唯一的；

b） 子角色的编码应以其父角色的编码为前缀，体现角色的层次结构；

c） 根据角色的编码，能求出其父角色及所有祖先角色的编码。

7.1.3 基于信息分类防护的角色分类

按照信息分类防护要求，将角色分为公开角色、内部共享角色和内部受控角色3种类型。

7.1.4 角色的权限类型

角色的权限可分为公开权限、私有权限和继承权限：

a） 公开权限：直接分配给角色的可被上级角色继承的权限；

b） 私有权限：直接分配给角色的但不可被任何角色继承的权限；

c） 继承权限：从下级角色继承而来的可继续被上级角色继承的权限。

角色之间的权限继承关系是可选的。当角色之间没有权限继承关系时，上级角色不继承下级角色的权限，角色的所有权限均为私有权限。

当角色之间存在权限继承关系时，上下级角色之间的权限继承仅限于在一个授权管理系统内部，不允许跨授权管理系统的权限继承。

7.2 资源管理

7.2.1 资源分类

资源分类是互联网电子政务系统中资源种类的划分，主要包括：网页、文件系统、数据库、功能模块，其中网页中包含了HTML代码段和脚本程序段，通常在脚本程序段中会包含应用组件，HTML代码段中可嵌套HTML代码段和脚本程序段，并使用相关控件资源，控件之间有时也存在嵌套关系；文件系统中通常包含文件和文件夹，文件夹中又包含文件资源；数据库资源由数据表组成，数据表由数据字段构成。

根据信息分类防护要求，基于互联网电子政务系统中的信息资源可按其重要程度将其分为：敏感信息、内部公开信息和公开信息3种类型。

7.2.2 资源操作

互联网电子政务系统中资源操作是指用户对系统中资源的操作权限，根据资源的类型不同，操作种类也不相同。网页资源操作包括：读、写、本级读、本级写、遍历、拥有。文件系统操作包括：读、写、本级读、本级写、遍历、拥有。数据库操作包括：数据库的创建、修改、删除，数据表的创建、修改、删除，数据项查询、修改、删除、添加。功能模块操作包括：加载、删除、调用接口等操作。

7.2.3 资源编码

互联网电子政务系统中所有资源均有一个唯一编码，编码由系统自动生成，不能重复使用、重复分配和修改。

7.3 权限管理操作

7.3.1 角色操作流程

7.3.1.1 添加下级角色

添加下级角色操作流程如下：

a） 获得当前进行操作的角色节点位置；

b） 添加角色信息，包括角色名称、限制用户数、角色类型，并自动为新添加角色生成角色编号、建立日期、子角色数、是否授权等信息，更新对应父角色的子角色个数。

7.3.1.2 修改角色

修改角色的流程如下：

a） 获得当前进行操作的角色节点位置；

b） 对角色名称、限制用户数进行修改。

本操作仅允许对角色名称、限制用户数进行修改，其余角色信息不允许修改。

7.3.1.3 删除角色

删除角色的流程如下：

a） 获得当前进行操作的角色节点位置，若为根节点，则退出，否则进行下一步；

b） 删除该角色及其所有子角色，以及它们所对应的所有权限，同时删除所有上级角色中从该角色处继承的权限，更新对应父角色的子角色个数，并从相关用户的权限中删除该角色，从相关互斥角色集中删除该角色。

7.3.2 互斥角色集管理流程

7.3.2.1 新建互斥角色集

新建互斥角色集流程如下：

a） 为新建互斥角色集自动生成编号；

b） 在角色树中选择角色，添加到互斥角色集，查看已有互斥角色集，若已存在与新建互斥角色集中的角色完全相同的互斥角色集，则退出，否则进行下一步；

c） 设置互斥角色集的基数；

d） 检查所有已授权用户，如存在违反新建互斥角色集的授权，则自动撤销用户角色集中存在互斥关系的角色，并提示授权管理员调整用户授权。

7.3.2.2 修改互斥角色集

修改互斥角色集流程如下：

a） 获得需进行修改操作的互斥角色集；

b） 对互斥角色集中的角色进行添加或删除，若修改后的互斥角色集中的角色个数为 0，则删除该互斥角色集并退出；

c） 修改互斥角色集的基数；

d） 检查所有已授权用户，如存在违反当前互斥角色集的授权，则自动撤销用户角色集中存在互斥关系的角色，并提示授权管理员调整用户授权。

7.3.2.3 删除互斥角色集

删除互斥角色集流程如下：

a） 获得需进行删除操作的互斥角色集；

b） 删除互斥角色集。

7.3.3 角色权限管理流程

7.3.3.1 为角色分配权限

为角色分配权限的流程如下：

a) 获得当前角色，按照信息分类保护要求，为其授予相应的权限集合，公开角色可被授予公开的信息资源，内部共享角色可被授予内部共享和公开的信息资源，内部受控角色可被授予公开、内部共享、内部受控的信息资源；

b) 指定所授权限的类别为公开权限或私有权限；

c) 权限继承深度策略所允许的上级角色可继承该角色的公开权限，并标记这些权限为继承权限。

7.3.3.2 撤销角色权限

撤销角色权限的流程如下：

a) 获得当前角色和要撤销的权限，从当前角色的权限集中删除要撤销的权限；

b) 若要撤销的权限已被上级角色继承，则从上级角色的继承权限中删除这些权限。

7.3.4 用户角色管理流程

7.3.4.1 为用户分配角色

为用户分配角色的流程如下：

a) 获得当前用户和将分配的角色；

b) 获得当前用户的已有角色集，若该角色已存在于用户的已有角色集中，则退出；

c) 将该角色与用户已有角色集形成并集，若该并集与某一互斥角色集相交，并且交集的元素个数大于该互斥角色集的基数，则退出；

d) 若该角色的用户数已达到最大值，则退出；

e) 将该角色加入当前用户的角色集中。

7.3.4.2 撤销用户已有角色

撤销用户已有角色的流程如下：

a) 获得当前用户及其要撤销的角色，更新该角色对应的用户数；

b) 从当前用户的角色集中删除该角色。

7.4 授权管理系统服务模式

7.4.1 用户授权服务方式

授权管理系统对用户的授权可提供两种服务方式，对未包含在下列内容中的服务方式，是否可以开启，应根据实际网络环境和服务的功能、性质进行处理：

a) 属性证书方式：以属性证书作为用户的权限载体，授权管理系统将用户的权限即角色信息写入属性证书中。属性证书可上传至 LDAP 服务器，认证服务器或应用系统通过拉模式获得属性证书；也可直接交给用户，用户在进行访问时通过推模式提交给认证服务器或应用系统。

b) 在线查询方式：由授权管理系统向认证服务器提供在线权限查询服务，授权管理系统权限策略的表示方式参见附录 B。无须生成属性证书，认证服务器在验证用户身份后，由认证服务器向授权管理系统查询用户的权限，生成票据后交给用户，作为访问应用系统的凭证。

7.4.2 角色授权服务方式

授权管理系统对角色的授权可提供两种服务方式，对未包含在下列内容中的服务方式，是否可以开

启，应根据实际网络环境和服务的功能、性质进行处理：

a） 权限裁决服务方式：由授权管理系统向应用服务器提供在线的权限裁决服务，当用户进行访问时，应用系统获得用户的角色和访问目标等信息，向授权管理系统发起权限裁决请求，授权管理系统根据请求信息和角色权限作出裁决，将裁决结果返回给应用系统。

b） 应用系统自主裁决方式：授权管理系统将角色的权限信息实时同步给应用系统，由应用系统进行访问控制的裁决。

附　录　A
（资料性附录）
身份认证与授权管理系统应用示例

A.1　身份认证与授权管理系统的示例部署

身份认证与授权管理系统的应用部署示例如图 A.1 所示。

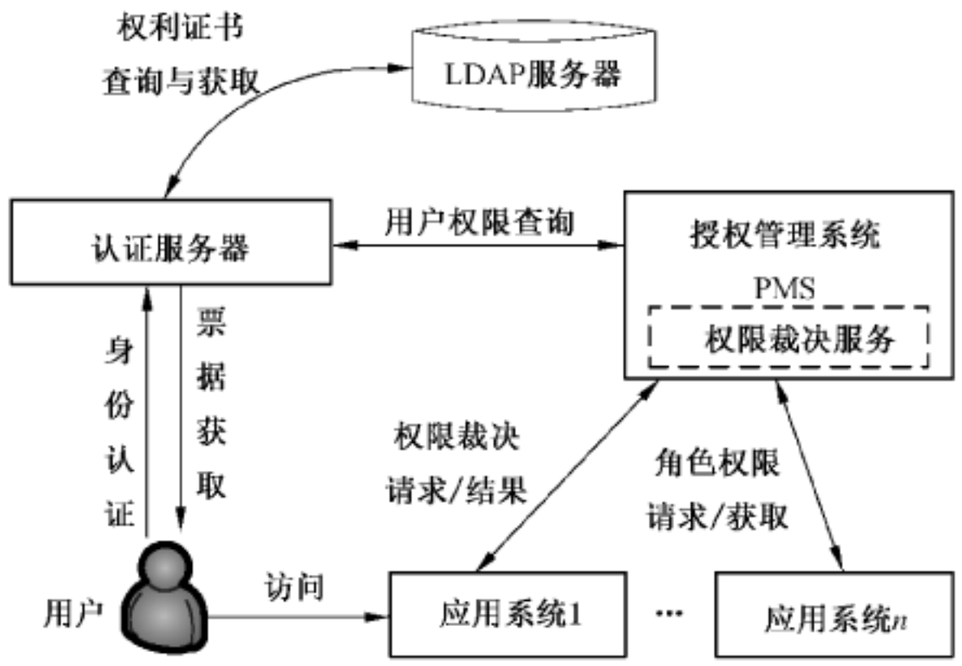

图 A.1　身份认证与授权管理系统的应用部署示例

在图 A.1 中包含以下实体：

a）　用户：对应用系统进行访问的实体；

b）　认证服务器：负责对用户的身份进行鉴别，保证对应用系统进行访问的用户均是合法用户；

c）　授权管理系统：在本例中，PMS 负责用户的授权和角色的授权，以及用户属性证书的管理；

d）　LDAP 服务器：证书目录服务器，可提供属性证书的在线查询服务；

e）　应用系统：用户访问的目标。

A.2　身份认证与授权管理系统工作流程示例

如图 A.1，基于角色的权限管理应用流程如下：

a）　PMS 为用户分配角色，并为角色分配访问应用系统资源的权限；也可根据用户角色信息为用户签发属性证书并发布到目录服务器中；

b）　PMS 启动权限裁决服务；

c）　用户访问应用系统，若用户未登录，则自动跳转到用户登录页面；

d）　用户在客户端登录，认证服务器验证用户身份，验证通过进行下一步，验证失败则中止用户访问；

e）　若采用属性证书方式，认证服务器从 LDAP 上获得用户属性证书，或由用户直接提交属性证书，验证属性证书的合法有效性，并从属性证书中获得用户角色信息；若不采用属性证书方式，直接根据用户身份信息向 PMS 查询用户角色信息；

f）　用户访问应用系统资源时，应用系统根据步骤 g）和 h）对用户访问进行控制；

g）　对每个访问请求，应用系统根据用户角色和对目标资源的访问需求，生成权限裁决请求，向

PMS 发出权限裁决请求，PMS 根据角色权限信息对请求进行判断，角色的类型与资源的类型应满足信息分类防护要求，PMS 将判决结果返回应用系统，应用系统根据判决结果决定是否允许用户的访问；

h) 应用系统根据用户的访问请求从 PMS 得到的同步授权信息，进行访问控制裁决，由应用系统自行决定是否允许用户对目标资源的访问，用户访问请求中的角色类型与目标资源类型应满足信息分类防护要求。

附 录 B
（资料性附录）
授权管理系统策略表示方式

策略表示方式需采用标准格式进行定义，建议采用 XML 文件格式表示。

用户权限查询结果格式定义方法如下：

```
〈? xml version = "1.0" encoding = "utf-8"?〉
    〈xs:schema id = "XMLSchema" targetNamespace = http://tempuri.org/XMLSchema.xsd
    elementFormDefault = "qualified"
    xmlns = "http://tempuri.org/XMLSchema.xsd"
    xmlns:mstns = http://tempuri.org/XMLSchema.xsd xmlns:xs = " http://www.w3.org/2001/
XMLSchema"〉
      〈xs:simpleType name = "char"〉
        〈xs:restriction base = "xs:string"〉
          〈xs:length value = "1" /〉
        〈/xs:restriction〉
      〈/xs:simpleType〉
      〈xs:element name = "用户标识" type = "xs:string" /〉
      〈xs:element name = "资源根" type = "xs:string" /〉
      〈xs:element name = "搜索深度" type = "xs:int" /〉
      〈xs:element name = "操作名称" type = "xs:string" /〉
      〈xs:element name = "资源"〉
        〈xs:complexType〉
          〈xs:sequence〉
            〈xs:element name = "资源编码" type = "xs:ID" /〉
            〈xs:element name = "资源名称" type = "xs:string" /〉
            〈xs:element name = "资源" type = "xs:string" /〉
            〈xs:element name = "资源属性" type = "xs:string" /〉
            〈xs:element name = "资源类型" type = "xs:string" /〉
          〈/xs:sequence〉
        〈/xs:complexType〉
      〈/xs:element〉
      〈xs:element name = "资源-操作列表" minOccurs = "0" maxOccurs = "unbounded"〉
        〈xs:complexType〉
          〈xs:sequence〉
            〈xs:element ref = "资源" /〉
            〈xs:element ref = "操作名称" minOccurs = "0" maxOccurs = "unbounded"/〉
          〈/xs:sequence〉
        〈/xs:complexType〉
      〈/xs:element〉
      〈xs:element name = "用户权限集"〉
        〈xs:complexType〉
```

```
        〈xs:sequence〉
          〈xs:element ref = "用户标识" /〉
          〈xs:element ref = "资源根" /〉
          〈xs:element ref = "搜索深度" /〉
          〈xs:element ref = "资源-操作列表" /〉
        〈/xs:sequence〉
      〈/xs:complexType〉
    〈/xs:element〉
  〈/xs:schema〉
```

角色权限查询结果格式定义方法如下：

```
〈? xml version = "1.0" encoding = "utf-8"?〉
〈xs:schema id = "XMLSchema" targetNamespace = http://tempuri.org/XMLSchema.xsd
elementFormDefault = "qualified"
xmlns = "http://tempuri.org/XMLSchema.xsd"
xmlns:mstns = http://tempuri.org/XMLSchema.xsd xmlns:xs = " http://www.w3.org/2001/
XMLSchema"〉
  〈xs:simpleType name = "char"〉
    〈xs:restriction base = "xs:string"〉
      〈xs:length value = "1" /〉
    〈/xs:restriction〉
  〈/xs:simpleType〉
〈xs:element name = "角色编码" type = "xs:string" /〉
〈xs:element name = "资源根" type = "xs:string" /〉
〈xs:element name = "搜索深度" type = "xs:int" /〉
〈xs:element name = "操作名称" type = "xs:string" /〉
〈xs:element name = "资源"〉
  〈xs:complexType〉
    〈xs:sequence〉
      〈xs:element name = "资源编码" type = "xs:ID" /〉
      〈xs:element name = "资源名称" type = "xs:string" /〉
        〈xs:element name = "资源" type = "xs:string" /〉
        〈xs:element name = "资源属性" type = "xs:string" /〉
        〈xs:element name = "资源类型" type = "xs:string" /〉
      〈/xs:sequence〉
  〈/xs:complexType〉
〈/xs:element〉
〈xs:element name = "资源-操作列表" minOccurs = "0" maxOccurs = "unbounded"〉
  〈xs:complexType〉
    〈xs:sequence〉
      〈xs:element ref = "资源"/〉
      〈xs:element ref = "操作名称" minOccurs = "0" maxOccurs = "unbounded"/〉
    〈/xs:sequence〉
  〈/xs:complexType〉
```

```
〈/xs:element〉
〈xs:element name="角色权限集"〉
  〈xs:complexType〉
    〈xs:sequence〉
      〈xs:element ref="角色编码"/〉
      〈xs:element ref="资源根"/〉
      〈xs:element ref="搜索深度"/〉
      〈xs:element ref="资源-操作列表"/〉
    〈/xs:sequence〉
  〈/xs:complexType〉
 〈/xs:element〉
〈/xs:schema〉
```

中 华 人 民 共 和 国
国家标准化指导性技术文件

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

GB/Z 24294.3—2017

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)

网址:www.spc.org.cn
服务热线:400-168-0010
2017年6月第一版

*

书号:155066·1-55839

GB/Z 24294.3-2017