

ICS 35.040
CCS L80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/Z 24294.3-2017

Replacing GB/Z 24294-2009

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

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

Issued on: May 31, 2017

Implemented on: May 31, 2017

**Issued by: State Administration for Market Regulation;
Standardization Administration of China**

Table of Contents

Foreword	III
Introduction	IV
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviations	1
5 Security functions of unified identity authentication and authorization management	2
5.1 Unified identity authentication function	2
5.2 Authorization management function	2
5.3 Requirements on system deployment	2
5.4 Requirements on storage security	2
6 Technical specification for unified identity authentication	2
6.1 Unified user identifier	2
6.2 Modes of identity authentication	4
6.3 Cryptographic algorithms	4
6.4 Authentication protocol	4
7 Technical specification for unified authorization management	4
7.1 Role management	4
7.2 Resource management	5
7.3 Privilege management operations	5
7.4 Service modes of the authorization management system	7
Annex A (informative) Examples of application of the identity authentication and authorization management system	9
Annex B (informative) Ways of expressing the policy of the authorization management system	11

Foreword

GB /Z 24294 "Information Security Technology Internet-based e-government information security implementation guidelines" is divided into four parts.

--- Part 1. General principles;

--- Part 2. Access control and security exchange;

--- Part 3. Identity and authorization management;

--- Part 4. Terminal Security. This section GB /Z 24294 Part 3. This section drafted in accordance with GB/T 1.1-2009 given rules. Part of this section instead of GB /Z 24294-2009 "Information Security Technology Internet-based e-government information security implementation guidelines," and GB /Z 24294-2009 compared to the main technical changes are as follows:

--- Added a unified authentication and authorization management of security features;

--- Added unified authentication technology requirements;

--- Added a unified licensing management technical requirements;

--- For the construction of the trust system, complemented the authentication and authorization management system deployment examples. This part of the National Information Security Standardization Technical Committee (SAC/TC260) and focal point. This part of the drafting unit. People's Liberation Army Information Engineering University, China Electronics Standardization Institute, Beijing Tian Rong Xin Technology Co., Ltd. Zheng Dazhou Great Information Technology Co., Ltd. The main drafters of this section. Chen Xingyuan, Du Xuehui, Sun Yi, Xia Chuntao, Cao Li-feng, Zhang Dongwei, Ren Zhiyu, Luo Feng surplus, Shangguan Xiao Li, Dong Guohua. This part replaces the standards previously issued as.

--- GB /Z 24294-2009.

Because of the open nature of internet e-government, e-government system is faced with identity fraud, information leakage, non-teaching Security of access and other security threats, the use of authentication, authorization management and other technologies can effectively improve the safety of Internet e-government system. In order to promote the application of the Internet in China's e-government and to guide the technical specifications based on Internet e-government identity authentication and authorization management Work, specially formulated in this section. This part of the Internet first of all e-government identity authentication and authorization management of security features to regulate, respectively, after the identity Certificate and license management in the process of implementation of technical specifications for a detailed description of the Internet and e-government security interface to regulate. This part of the main norms in the Internet-based e-government system implementation of identity authentication and authorization of the technical activities carried out by the phase Guan management activities. Information Security Technology Internet-based e-government information security implementation guidelines Part 3. Identity and authorization management

1 Scope

GB/Z 24294.3-2017 is the Chinese national standard on information security technology -

guide of implementation for internet-based e-government information security - part 3: identity authentication and authorization, in the field of information technology. The /Z suffix marks it as a guiding technical document: it does not prescribe requirements that can be certified against, but sets out the technique, the method or the state of the art that the standards bodies recommend following. It was issued on 31 May 2017 by the State Administration for Market Regulation; Standardization Administration of China. As a guiding technical document it carries no separate date of entry into force: it applies from publication. Classification: ICS 35.040, CCS L80. This page is published from the official record of the standard held by the Chinese standards administration: the identification, the dates, the classification and the issuing body are taken from there. The clause text, the tables and the numeric limits are in the document itself, which is delivered complete in English translation.

This part of GB /Z 24294 gives the implementation guide of identity authentication and authorization management in Internet e-government, clarifying its functional requirements And install the deployment requirements, define the authentication and authorization management technical specifications. To rely on the Internet to build a credible government service platform as the goal Establish a credible, manageable and controllable Internet-based e-government information system to provide technical guidance. This section applies to Internet-based e-government system authentication and authorization management system design, development and construction, as managers Members, engineers, information security product providers to build a unified authentication and authorization management system to provide management and technical reference. Involved State secrets, or the state secrets that may be involved after the information stored, processed and transmitted are collected, shall be subject to the provisions of state secrets and standards.

2 Normative references

The following documents for the application of this document is essential. For dated references, only the dated version applies to this article Pieces. For undated references, the latest edition (including all amendments) applies to this document. Digital Certificate Format Specification Based on SM

3 Terms and definitions

The following terms and definitions apply to this document.

3.1 Attribute Authorities attributeauthority A certification authority that distributes permissions by publishing a certificate of attributes, also known as a property management agency.

3.2 Attribute certificate attributecertificate Attribute Authorities digitally sign a data structure

that binds the holder's identity information to some attribute value.

3.3 Specific rights management infrastructure privilegemanagementinfrastructure A comprehensive infrastructure that supports authorized services is closely linked to public key infrastructure.

4 Abbreviations

The following abbreviations apply to this document. LDAP Lightweight Directory Access Protocol (LightweightDirectoryAccessProtocol) PMS authorization management system (PrivilegeManagementSystem)