

ICS 35.020
CCS A 90

GA

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

GA 611-2006

**Information service system of internet -- Security protection
technology controls -- Technology requirement
(English Translation)**

Issued on: April 27, 2006

Implemented on: June 1, 2006

Issued by: Ministry of Public Security

Table of Contents

- Foreword
- 1 Scope
- 2 Normative references
- 3 Terms and definitions
- 4 Technical requirements
- 4.1 System Security

Foreword

4.2.2.4, 4.3.2.2.1(?), 4.3.3) are recommended terms, others are mandatory.

GA 611-2006 is one of the series of standards for "Technical Measures for Security Protection of Internet Information Service Systems". The structure of this series of standards as follows.

--- Internet information service system security protection technical measures information code;

---Data format of the technical measures for security protection of Internet information service systems;

---Technical requirements for technical measures for security protection of Internet information service systems;

--- Internet information service system security protection technical measures communication standards.

This standard was proposed by the Public Information Network Security Supervision Bureau of the Ministry of Public Security.

This standard is under the jurisdiction of the Information System Security Standardization Technical Committee of the Ministry of Public Security.

This standard was drafted. Ministry of Public Security Computer Information System Security Product Quality Supervision and Inspection Center.

1 Scope

This standard specifies Internet peer-to-peer file transmission services, electronic bulletin services, and e-commerce services in the Internet information service system.

Technology, email service, short message service, instant messaging service, chat room service, search engine service, website service, game service technology Claim.

This standard applies to Internet information service systems. Other types of systems that provide Internet information services may be implemented with reference to this standard.

2 Normative references

The terms in the following documents become the terms of this standard by reference to this standard. All dated references, followed by all Modifications (not including errata content) or revisions do not apply to this standard, however, parties to agreements based on this standard are encouraged to study it is possible to use the latest version of these files? For undated references, the latest edition applies to this standard.

GB/T 2260 Administrative division code of the People's Republic of China GB 2312-1980 Basic set of Chinese character coded character set for information exchange GB 18030-2000 Extension of the basic set of Chinese character coded character sets for information technology information exchange GA 609-2006 Internet Information Service System Security Protection Technical Measures Information Code GA 610-2006 Internet Information Service System Security Protection Technical Measures Data Format GA/Z02-2005 Public Security Business Basic Data Element Code Set

3 Terms and definitions

The following terms and definitions established by GA 609-2006 apply to this standard.

Based on instant messaging software, users are provided with a multi-party information exchange function.

In the information system, the identity authentication method of the user proves that the identity of a person is called single factor recognition only through the conformation of one condition.

Certificate, for example. the traditional "user + password". To prove the identity of a person by combining two different conditions, called two-factor authentication, for example, in addition to the traditional "user + password", it also uses a hardware-based U disk, using PIN password to protect user information.

4.1.1 Management Authority Identification

- a) The system should provide administrator management functions, including querying, adding, modifying, and deleting administrators;
- b) The system shall provide the identity authentication function to authenticate the authorized administrator. Identification is done in the form of a password, and in each the secondary user authenticates when logging in to the system. The password is invisible and

is secure when stored;

c) The system should have and only authorized administrators can perform system security management;

d) The system should set a separate audit administrator role, and only the administrator of this role can set the audit policy event library, check