

ICS 35.240.80
CCS C 07



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

GB/Z 21716.2-2008

**Health informatics -- Public Key Infrastructure (PKI) -- Part 2:
Certificate profile**

健康信息学 公钥基础设施 (PKI) 第2部分: 证书轮廓
(English Translation)

Issued on: April 11, 2008

Implemented on: September 1, 2008

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine of People's Republic of China, China National Standardization
Administration**

Table of Contents

Foreword
Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviations
5 Health Care Certificate Strategy
5.1 Type of health certificate
5.2 CA certificate
5.3 Cross/Bridge Certificate
5.4 end entity certificate
6 General Certificate Requirements
6.1 Certificate Compliance
6.2 Common fields of various types of certificates
6.3 General Field Specification
6.4 Requirements for various types of health care certificates
7 the use of certificate extensions
7.1 Introduction
7.2 General Extensions
7.3 Dedicated Subject Directory Attributes
7.4 Certificate Declaration Expansion
7.5 Requirements for each type of medical profession certificate
Appendix A A. 1 Introduction
References

Foreword

GB /Z21716 "Health Informatics Public Key Infrastructure (PKI)" is divided into three parts.

--- Part 1. Overview of Digital Certificate Services;

--- Part 2. Certificate outline;

--- Part 3. Strategic Management of Certification Bodies. This section GB /Z21716 Part 2.

This section with reference to ISO 17090-2 (DIS) "Health Informatics Public Key Infrastructure (PKI) Part 2. Certificate Outline" formulation, its The main technical content is consistent with ISO 17090-2 (DIS). Relative to the original text, this section with only minor changes, including.

--- According to China's national conditions, the text included in the example of the country name, unit name, etc. into Chinese name in China;

--- Do not change the technical content of the editorial changes. Appendix A of this section is informative appendix. This section proposed by the China National Institute of Standardization. This part of China Institute of Standardization centralized. This section drafted by. China National Institute of Standardization.

Introduction

To reduce costs and costs, the health industry is facing the challenge of shifting from paper processing to automated electronic processing. New medical insurance The health paradigm increases the need to share patient information among professional healthcare providers and to break the boundaries of traditional institutions.

In general, each citizen's health information can be accessed by e-mail, remote database access, electronic data interchange, and others Used to exchange. The Internet provides an economical and easily accessible means of information exchange, but it is also an unsafe medium, which requires Take certain measures to protect the privacy and confidentiality of information. Unauthorized visits, whether intentional or unintentional, will increase Threat to health information security. It is necessary for health care systems to use reliable information security services to reduce the risk of unauthorized access.

How can the health care industry provide an affordable and affordable way to properly protect the data transmitted over the Internet? for this problem, At present, people are trying to meet this challenge by using public key infrastructure (PKI) and digital certificate technology.

Correctly configuring digital certificates requires that technologies, policies, and management processes be tied together and that "public-key cryptography" be used to protect the information.

Use "certificates" to confirm the identity of individuals or entities to enable the secure exchange of sensitive data in an insecure environment. In the area of health, This technique uses methods of authentication, encryption, and digital signatures to ensure secure access and transmission of personal health records to meet clinical And management needs. The services provided by digital certificate configuration, including encryption, message integrity, and digital signatures, address the More security issues. To this end, many organizations in the world have started using digital certificates. A typical situation is the digital certificate and A well-established standard for information security.

If you need to exchange health between different organizations or between jurisdictions (such as hospitals and community doctors serving the same patient)

Information, the digital certificate technology and its support strategy, procedures, operational interoperability is the most important.

Achieving interoperability between different digital certificate implementations requires building a trust framework. In this framework, responsible for the protection of personal letters The parties to the entitlement rely on specific tactics and practices and even rely on the validity of digital certificates issued by other established institutions.

Many countries are using digital certificates to support domestic secure communications. If standard development activities are limited to countries, There will be inconsistencies and even inconsistencies in the tactics and procedures of the certification bodies (CAs) and registries (RAs) in different countries.

There are many aspects of digital certificates not dedicated to healthcare and they are still at a developmental stage. In addition, some important standardization Work and legislative support are also under way. On the other hand, healthcare providers in many countries are using or getting ready for use Digital certificate Therefore, the purpose of this guidance document is to provide guidance for these rapidly evolving international applications.

This guidance document describes the general technical, operational, and policy requirements to be able to use digital certificates to protect health Kang information exchange within the field, between different areas and between different jurisdictions. The ultimate goal of this technical guide is to build Establish a platform that enables global interoperability. This guidance document mainly supports cross-border communications using digital certificates, but also for distribution Provide national or regional health care digital certificate to provide guidance. The Internet as a transmission medium is increasingly being used in Medicare The delivery of health data among health organizations is also the only option for cross-border communication.

The three parts of this guidance document as a whole define how to use digital certificates in the health sector to provide safety clothing Services, including authentication, confidentiality, data integrity, and technical capabilities that support the quality of digital signatures.

Part 1 of this guidance document prescribes the basic concepts of using digital certificates in the field of health and gives guidance on the use of digital certificates Interoperability programs required for health information security communications.

This guidance document, Part 2, is based on international standard X. 509 digital certificates for health-specific profiles as well as for no The same type of certificate IETF/RFC3280 outlined in the health care profile.

This guidance document, Part 3, addresses management issues related to the

implementation and use of digital certificates of health care, provides evidence The structure and minimum requirements of the book strategy (CP) and the structure of the associated certification operation statement. This section is based on IETF/RFC3647 recommendations As the basis for identifying the principles needed in the security strategy for cross-national communications of health information and also setting the minimum level of security required for health Full. Health Informatics Public Key Infrastructure (PKI) Part 2. Certificate Outline

1 Scope

This section specifies the certificates required for the exchange of health care information within and between individual organizations and across regulatory boundaries contour. This section also details the applications of PKI digital certificates in the medical industry and focuses on the use of Certificate outline related to health care issues.

2 Normative references

The provisions of the following documents through the GB /Z21716 of this part of the reference and become the provisions of this section. Any reference to the date of the citation All subsequent amendments (not including errata content) or revisions do not apply to this section, however, encouraged to be reached under this section The parties to the agreement examine whether the latest versions of these documents are available. For undated references, the latest version applies to this book section.

GB /Z21716.1-2008 Health Informatics Public Key Infrastructure (PKI) Part 1. Overview of Digital Certificate Services GB /Z21716.3-2008 Health Informatics Public Key Infrastructure (PKI) Part 3. Strategic Management of Certification Bodies IETF/RFC3280 InternetX. 509 Public Key Infrastructure Certificate and CRL Profile IETF/RFC3281 Internet profile for agency profile IETF/RFC3739 Internet X. 509 Public Key Infrastructure Certificate of Eligibility

3 Terms and definitions

GB /Z21716.1 given terms and definitions apply to this section.

4 Abbreviations

The following abbreviations apply to this section.

AA Attribute Agency attributeauthority AC attribute certificate attributecertificate CA certification authority certificationauthority CP certificate policy certificatepolicy CPS certification operating statement certificationpracticestatement CRL certificate revocation list certificaterevocationlist PKC public key certificate publickeycertificate PKI public key infrastructure publickeyinfrastructure RA registration authority registrationauthority TTP