AS ISO 17090.2—2003
ISO/TS 17090-2:2002

Australian Standard™

Health informatics—Public key infrastructure

Part 2: Certificate profile

Standards Australia

This Australian Standard was prepared by Committee IT-014, Health Informatics. It was approved on behalf of the Council of Standards Australia on 30 March 2003 and published on 16 May 2003.

The following are represented on Committee IT-014:

Australian and New Zealand College of Anaesthetists
Australian Association of Pathology Practices
Australian Health Insurance Association
Australian Heathcare Association
Australian Institute of Health and Welfare
Australian Medical Association
Australian Private Hospitals Association
Central Queensland University
Commonwealth Department of Health and Aged Care
Consumers Federation of Australia
Consumers Health Forum of Australia
Department of Health Services, South Australia
Department of Human Services, Victoria
Health Department of Western Australia
Health Informatics Society of Australia
Health Information Management Association of Australia
Health Insurance Commission
Institution of Engineers Australia
Medical Software Industry Association
National Health Information Management Group
New Zealand Health Information Foundation
New South Wales Health Department
Queensland Health
Royal Australasian College of Radiologists
Royal Australian and New Zealand College of Obstetricians and Gynaecologists
Royal Australian College of General Practitioners
Royal Australian College of Medical Administrators
Royal College of Nursing, Australia
Society of Hospital Pharmacists of Australia

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about Standards can be found by visiting the Standards Australia web site at www.standards.com.au and looking up the relevant Standard in the on-line catalogue.

Alternatively, the printed Catalogue provides information current at 1 January each year, and the monthly magazine, *The Australian Standard*, has a full listing of revisions and amendments published each month.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.com.au, or write to the Chief Executive, Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001.

This Standard was issued in draft form for comment as DR 01183.

Australian Standard™

Health informatics—Public key infrastructure

Part 2: Certificate profile

First published as AS ISO 17090.2—2003.

COPYRIGHT

© Standards Australia

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Published by Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001

ISBN 0 7337 5190 3

PREFACE

This Standard was prepared by the Australian members of the Joint Standards Australia/Standards New Zealand Committee IT-014, Health Informatics. After consultation with stakeholders in both countries, Standards Australia and Standards New Zealand decided to develop this Standard as an Australian Standard rather than an Australian/New Zealand Standard.

This Standard is identical with, and has been reproduced from, ISO/TS 17090-2:2002, *Health informatics—Public key infrastructure*—Part 2: *Certificate profile*.

Committee IT-014 provided input to the International Organization for Standardization (ISO) Committee, ISO/TC 215 on Health Informatics, in the preparation of the ISO 17090 family of International Standards.

The objective of this Standard is to specify the certificate profiles required to interchange healthcare information within a single organization, between different organizations and across jurisdictional boundaries. It details the use made of public key infrastructure (PKI) digital certificates in the health industry and focuses, in particular, on specific healthcare issues relating to certificate profiles.

This Standard is Part 2 of AS ISO 17090, *Health informatics—Public key infrastructure*, which is published in parts as follows:

Part 1: Framework and overview
Part 2: Certificate profile (this Standard)
Part 3: Policy management of certification authority

The terms 'normative' and 'informative' are used to define the application of the annex to which they apply. A normative annex is an integral part of a standard, whereas an informative annex is only for information and guidance.

As this Standard is reproduced from an international standard, the following applies:

(a) Its number appears on the cover and title page while the international standard number appears only on the cover.

(b) In the source text 'this part of ISO/TS 17090' should read 'this Australian Standard'.

(c) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

Reference to International Standard		*Australian or Australian/New Zealand Standard*	
ISO/TS		AS ISO	
17090	Health informatics—Public key infrastructure	17090	Health informatics—Public key infrastructure
17090-1	Part 1 : Framework and overview	17090.1	Part 1 : Framework and overview
17090-3	Part 3: Policy management of certification authority	17090.3	Part 3: Policy management of certification authority

CONTENTS

Page

Introduction ... **iv**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Abbreviations ... **2**

5 Healthcare CPs ... **2**
5.1 Certificate types required for healthcare ... **2**
5.2 CA certificates ... **2**
5.3 Cross/Bridge certificates ... **3**
5.4 End entity certificates ... **3**

6 General certificate requirements ... **6**
6.1 Certificate compliance ... **6**
6.2 Common fields for each certificate type ... **7**
6.3 Specifications for common fields ... **8**
6.4 Requirements for each healthcare certificate type ... **10**

7 Use of certificate extensions ... **13**
7.1 Introduction ... **13**
7.2 General extensions ... **13**
7.3 Special subject directory attributes ... **14**
7.4 Qualified certificate statements extension ... **16**
7.5 Requirements for each health industry certificate type ... **16**

Annex A (informative) **Certificate profile examples** ... **18**

Bibliography ... **25**

INTRODUCTION

The healthcare industry is faced with the challenge of reducing costs by moving from paper-based processes to automated electronic processes. New models of healthcare delivery are emphasizing the need for patient information to be shared among a growing number of specialist healthcare providers and across traditional organizational boundaries.

Healthcare information concerning individual citizens is commonly interchanged by means of electronic mail, remote database access, electronic data interchange and other applications. The Internet provides a highly cost-effective and accessible means of interchanging information, but is also an insecure vehicle that demands additional measures be taken to maintain the privacy and confidentiality of information. Threats to the security of health information through unauthorized access (either inadvertent or deliberate) are increasing. It is essential to have available to the healthcare system reliable information security services that minimize the risk of unauthorized access.

How does the healthcare industry provide appropriate protection for the data conveyed across the Internet in a practical, cost-effective way? Public key infrastructure (PKI) technology seeks to address this challenge.

PKI is a blend of technology, policy and administrative processes that enable the exchange of sensitive data in an unsecured environment by the use of “public key cryptography” to protect information in transit and “certificates” to confirm the identity of a person or entity. In healthcare environments, PKI uses authentication, encipherment and digital signatures to facilitate confidential access to, and movement of, individual health records to meet both clinical and administrative needs. The services offered by a PKI (including encipherment, information integrity and digital signatures) are able to address many of these security issues. This is especially the case if PKI is used in conjunction with an accredited information security standard. Many individual organizations around the world have started to apply PKI for this purpose.

Interoperability of PKI technology and supporting policies, procedures and practices is of fundamental importance if information is to be exchanged between organizations and between jurisdictions in support of healthcare applications (for example between a hospital and a community physician working with the same patient).

Achieving interoperability between different PKI schemes requires the establishment of a framework of trust, under which parties responsible for protecting an individual’s information rights may rely on the policies and practices and, by extension, the validity of digital certificates issued by other established authorities.

Many countries are adopting PKIs to support secure communications within their national boundaries. Inconsistencies will arise in policies and procedures between the certification authorities (CAs) and registration authorities (RAs) of different countries if PKI standards development activity is restricted to within national boundaries.

PKI technology is still rapidly evolving in certain aspects that are not specific to healthcare. Important standardization efforts and, in some cases, supporting legislation are ongoing. On the other hand, healthcare providers in many countries are already using or planning to use PKI. This Technical Specification seeks to address the need for guidance of these rapid international developments.

This three-part document is being issued in the Technical Specification series of publications (according to the ISO/IEC Directives, Part 1, 3.1.1.1) as a prospective standard for the use of PKI in the field of healthcare because there is an urgent need for guidance on how standards in this field should be used to meet an identified need. This document is not to be regarded as an International Standard. It is proposed for provisional application so that information and experience of its use in practice may be gathered. ISO/TC 215 intends to revise it into a full International Standard after a three-year period.

This Technical Specification describes the common technical, operational and policy requirements that need to be addressed to enable PKI to be used in protecting the exchange of healthcare information within a single domain, between domains and across jurisdictional boundaries. Its purpose is to create a platform for global interoperability.

It specifically supports PKI enabled communication across borders, but could also provide guidance for the establishment of healthcare PKIs nationally or regionally. The Internet is increasingly used as the vehicle of choice to support the movement of healthcare data between healthcare organizations and is the only realistic choice for cross-border communication in this sector.

This Technical Specification should be approached as a whole, with the three parts all making a contribution to defining how PKIs can be used to provide security services in the health industry, including authentication, confidentiality, data integrity and the technical capacity to support the quality of digital signature.

ISO/TS 17090-1 defines the basic concepts of a healthcare public key infrastructure (PKI) and provides a scheme of interoperability requirements to establish a PKI enabled secure communication of health information.

ISO/TS 17090-2 provides healthcare specific profiles of digital certificates based on the International Standard X.509 and the profile of this specified in IETF/RFC 2459 for different types of certificates.

ISO/TS 17090-3 deals with management issues involved in implementing and operating a healthcare PKI. It defines a structure and minimum requirements for certificate policies (CPs) and a structure for associated certification practice statements. This part is based on the recommendations of the IETF/RFC 2527 *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* and identifies the principles needed in a healthcare security policy for cross border communication. It also defines the minimum levels of security required, concentrating on the aspects unique to healthcare.

Comments on the content of this document, as well as comments, suggestions and information on the application of these technical specifications may be forwarded to the ISO/TC 215 secretariat: tsandler@astm.org and the WG4 secretariat w4sec215@medis.or.jp.

NOTES

AUSTRALIAN STANDARD

Health informatics — Public key infrastructure —

Part 2:
Certificate profile

1 Scope

This part of ISO/TS 17090 specifies the certificate profiles required to interchange healthcare information within a single organization, between different organizations and across jurisdictional boundaries. It details the use made of public key infrastructure (PKI) digital certificates in the health industry and focuses, in particular, on specific healthcare issues relating to certificate profiles.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/TS 17090. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO/TS 17090 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/TS 17090-1:2002, *Health informatics — Public key infrastructure — Part 1: Framework and overview*

ISO/TS 17090-3:2002, *Health informatics — Public key infrastructure — Part 3: Policy management of certification authority*

IETF/RFC 2459, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*

IETF/RFC 2527, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*

IETF/RFC 3039, *Internet X.509 Public Key Infrastructure Qualified Certificates Profile*

INTERNET-DRAFT October 1999 4.1, *X.509 Attribute Certificate*

3 Terms and definitions

For the purposes of this part of ISO/TS 17090, the terms and definitions given in ISO/TS 17090-1:2002 apply.

© Standards Australia