ISO/TC 215/WG 4
Health Informatics/Security

Reference number of working document: **ISO/TC 215/WG4/N82**

Date: 2001-03-05

Reference number of document: **ISO/DTS 17090-1**

Committee identification: ISO/TC 215

Secretariat: ANSI

Health Informatics – Public Key Infrastructure - Part 1: Framework and overview

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Document type: Technical Specification
Document stage: (20) Preparation

Document language: E

This is a final working draft from the Task Force proposed to be approved by ISO/TC215/WG 4 on 2001-03-28 as the Draft Technical Specification to be submitted to ballot

International Standards Organisation Technical Committee 215, Health Informatics
Working Group 4: Security

Contact person

Convenor: Gunnar Klein, HSS
Box 70 487, S-107 26 Stockholm, Sweden
e-mail: wg4.isotc215@hss.se

Secretariat: Nagaki Ohyama, Tokyo Institute of Technology Imaging
Science and Engineering Laboratory
4259 Nagatsuta, Midori-ku, Yokahama 226-8503, Japan
e-mail: wg4kita@medis.or.jp

WG4/Task Force PKI. Managed by John Lewis

e-mail: jlewi@bigpond.com

Contents

Foreword

ISO (the International Standards Organisation) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organisations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2, Edition 4.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of normative document:

> an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/TS is reviewed every three years with a view to deciding whether it can be transformed into an International Standard.

Attention is drawn to the possibility that some elements of this Technical Specification/part of ISO/TS 17090 may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TS 17090 was prepared by Technical Committee ISO/TC 215, “Health informatics”, WG4 “Security”.

ISO/TS 17090 consists of the following parts, under the general title:

Health informatics - Public Key Infrastructure

Part 1: Framework and overview

Part 2: Certificate profile

Part 3: Policy Management of Certificate Authority

Introduction

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

Health care 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 unauthorised access (either inadvertent or deliberate) are increasing. It is essential to have available to the health care system reliable information security services which minimise the risk of unauthorised access.

How does the health care 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 health care 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) can 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 organisations 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 organisations and between jurisdictions in support of health care applications (for example between a hospital and a community physician working with the same patient).

Achieving interoperability between different PKI schemes, not only requires that technical interoperability be achieved, but most importantly, 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 public key infrastructures to support secure communications within their national boundaries. Inconsistencies will arise in policies and procedures between the Certification and Registration Authorities of different countries, if PKI standards development activity is restricted to within national boundaries.

Public Key Infrastructure technology is still rapidly evolving in certain aspects that are not specific to health care. Important standardization efforts and in some cases supporting legislation are ongoing. On the other hand health care 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. ISO/TC 215 intends to revise it into a full international standard after a three year period.

Health informatics – Public key infrastructure – Part 1: Framework and overview

1 Scope

This three-part ISO Technical Specification (ISO/TS) describes the common technical, operational and policy requirements that need to be addressed to enable Public Key Infrastructures (PKI) to be used in protecting the exchange of health care information within a single domain, between domains and across jurisdictional boundaries.

The purpose of this technical specification is to create a platform for global interoperability. It specifically supports PKI enabled communication across borders but the specification could also provide guidance for the establishment of health care PKIs nationally or regionally. The Internet is increasingly used as the vehicle of choice to support the movement of health care data between health care organisations and is the only realistic choice for cross-border communication in this sector.

This ISO/TS provides health care specific profiles of existing security standards from ISO/IEC and the Internet Engineering Task Force (IETF). The use of of this ISO/TS is not however restricted to Internet transport.

The specification addresses the following types of end-entity certificate holders:

Regulated health care professionals

Health care non-regulated employee

Sponsored health care providers (that are not regulated)

Patients/consumers

Health care organisations

Supporting organisations

Supporting organisation employee

Devices

Applications

These are defined further in Part 1, Section 5.2.

This part, *Part 1:* "*Framework and overview*" of the ISO/TS defines the basic concepts needed to describe a health care PKI and provide a scheme of interoperability requirements to establish a PKI enabled secure communication of health information.

It starts with a model of the major stakeholders that are communicating in health with some detailed scenarios highlighting the need for PKI in an informative annex. This ISO/TC further describes the major security services required for health communication where PKI may be required. The document gives a brief introduction to public key cryptography and the basic components of a health care PKI. It further introduces different types of certificates, public key identity certificates and associated attribute certificates, for relying parties as described above, self-signed CA certificates, and CA hierarchies and bridging structures.

Part 2: "Certificate profile" specifies health care 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.

Part 3: "Policy management of certification authority" deals with management issues involved in implementing and operating a health care PKI. It defines a structure and minimum requirements for Certificate Policies 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 health care security policy for cross border communication. It also defines the minimum levels of security required, concentrating on the aspects unique to health care.

2 Normative references

This ISO Technical Specification incorporates by dated or undated reference, provisions from other publications. These normative references are cited in the appropriate places in the text, and the publications are listed hereafter. For dated references, subsequent amendments and revisions of any of these publications apply to this ISO Technical Specification only when incorporated in it by amendment and revision. For undated references, the latest edition of the publication referred to applies.

ISO/IEC 2382-8:1998	Information technology – Vocabulary -- Part 8: Security
ISO/IEC 7498-2	Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture
ISO/IEC 8824-1:1995	Information Technology - Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1). - Part 1: Specification of the basic notation
ISO/IEC 10181-1	Information technology – Open Systems Interconnection – Security frameworks for open systems – Overview.
ISO/IEC TR13335	Guidelines for management of IT Security – Part 1, Concepts and models for IT security.
ISO/IEC 14516	Information technology – Security techniques – Guidelines on the use and management of Trusted Third Party services
ISO/IEC 15945:	Information technology – Security techniques – Specification of TTP services to support the application digital signatures
ISO/IEC 17799:2000	Information technology -- Code of practice for information security management
ITU-T X.509:1997	Recommendation X.509: The Directory - Authentication Framework. Equivalent to ISO/IEC 9594-8
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
ENV 13608-1	Health informatics - Security for healthcare communication - Concepts and terminology

3 Terms and definitions

For the purposes of this ISO Technical Specification, the following definitions apply:

3.1 Health care context terms

Please note that there are many different terms used to describe these concepts for different purposes available from CEN, HL-7 and various national organisations. The following definitions are not meant to be universal in ISO work in health informatics, only to facilitate the understanding of this ISO/TS.

3.1.1

application
an identifiable computer running software process that is the holder of a private encipherment key

NOTE 1: in this context it may be any software process used in health care information systems including those without any direct role in treatment or diagnosis.

NOTE 2: in some jurisdictions including software processes may be regulated medical devices

3.1.2

device
an identifiable computer controlled apparatus or instrument that is the holder of a private encipherment key

NOTE: This includes the class of regulated medical devices that meet the above definition. Device in this context is any device used in health care information systems including those without any direct role in treatment or diagnosis

3.1.3

health care actor
health professional, health care employee, patient/consumer, sponsored health care provider, health care organisation, device or application that acts in a health related communication and requires a certificate for a PKI enabled security service

3.1.4

health care organisation
an officially registered organisation that has a main activity related to health care services or health promotion

NOTE 1: Examples include hospitals, Internet health care website providers, and health care research institutions.

NOTE 2: The organisation should be recognised to be legally liable for their activities but need not be registered for their specific role in health. An internal part of an organisation is here called organisational unit as in X.501.

3.1.5

health care non-regulated employee
person employed by a health care organisation that is not a health professional. Examples include a receptionist or secretary who organises appointments, or a business manager who is responsible for validating patient health insurance.

NOTE: The fact that the employee is not authorised by a body independent of the employer in his professional capacity does of course not imply that the employee is not professional in conducting his services.

3.1.6

health professional
person that is authorised by a nationally recognised body to be qualified to perform certain health services

NOTE 1: The types of registering or accrediting bodies differ in different countries and for different professions. Nationally recognised bodies include local or regional governmental agencies, independent professional associations and other formally and nationally recognised organisations. They may be exclusive or non-exclusive in their territory.

NOTE 2: A nationally recognised body in this definition does not imply one nationally controlled system of professional registration but in order to facilitate international communication it would be preferable that one nation-wide directory of recognised health professional registration bodies exists.

NOTE 3: Examples of health professionals are physicians, registered nurses and pharmacists.

3.1.7

patient/consumer
person that is the receiver of health related services and that is an actor in a health information system

3.1.8

privacy
freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual [ISO/IEC 2382-8]

3.1.9

sponsored health care provider
health services provider who is not a regulated professional in the jurisdiction of his/her practice but who is active in his/her health care community and sponsored by a regulated health care organisation

NOTE: Examples would be a drug and alcohol education officer who is working with a particular ethnic group, or a health care aid worker in a developing country

3.1.10

supporting organisation
an officially registered organisation that is providing services to a health care organisation but which is not providing health care services

NOTE : Examples include health care financing bodies such as insurance institutions, suppliers of pharmaceuticals and other goods

3.1.11

supporting organisation employee
person employed by a supporting organization

NOTE: Examples include medical records transcriptionists, health care insurance claims adjudicators and pharmaceutical order entry clerks.

3.2 Security services terms

3.2.1

access control
a means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways [ISO/IEC 2382-8]

3.2.2

accountability
the property that ensures that the actions of an entity may be traced uniquely to the entity [ISO 7498-2]

3.2.3

asymmetric cryptographic algorithm
an algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ [ISO 10181-1]

3.2.4

authentication
process of reliably identifying security subjects by securely associating an identifier and its authenticator. See also data origin authentication and peer entity authentication [ISO 7498-2]

3.2.5

authorization
the granting of rights, which includes the granting of access based on access rights [ISO 7498-2]

3.2.6

availability
property of being accessible and useable upon demand by an authorised entity [ISO 7498-2]

3.2.7

ciphertext
data produced through the use of encipherment. The semantic content of the resulting data is not available [ISO 7498-2]

3.2.8

confidentiality
the property that information is not made available or disclosed to unauthorised individuals, entities, or processes [ISO 7498-2]

3.2.9

cryptography
the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use [ISO 7498-2]

3.2.10

cryptographic algorithm
cipher
A method for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. [ISO 7498-2]

3.2.11

data integrity
the property that data has not been altered or destroyed in an unauthorised manner [ISO 7498-2]

3.2.12

data origin authentication
the corroboration that the source of data received is as claimed [ISO 7498-2]

3.2.13

decipherment
decryption
the process of obtaining, from a ciphertext, the original corresponding data [ISO/IEC 2382-8]

NOTE: a ciphertext may be enciphered a second time, in which case a single decipherment does not produce the original plaintext.

3.2.14

digital signature
data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient [ISO 7498-2]

3.2.15

encipherment
encryption
the cryptographic transformation of data (see cryptography) to produce ciphertext [ISO 7498-2]

3.2.16

identification
the performance of tests to enable a data processing system to recognize entities [ISO/IEC 2382-8]

3.2.17

identifier
piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator [ENV 13608-1]

3.2.18

integrity
proof that the message content has not altered, deliberately or accidentally in any way, during transmission [ISO/IEC 7498-2]

3.2.19

key
a sequence of symbols that controls the operations of encipherment and decipherment [ISO 7498-2]

3.2.20

key management
the generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy [ISO 7498-2]

3.2.21

non-repudiation
this service provides proof of the integrity and origin of data (both in an unforgeable relationship) which can be verified by any party [ASTM]

3.2.22

private key
a key that is used with an asymmetric cryptographic algorithm and whose possession is restricted (usually to only one entity) [ISO 10181-1]

3.2.23

public key
a key that is used with an asymmetric cryptographic algorithm and that can be made publicly available [ISO 10181-1]

3.2.24

role
a set of behaviours that is associated with a task

3.2.25

security
the combination of availability, confidentiality, integrity and accountability [ENV 13608-1]

3.2.26

security policy
a plan or course of action adopted for providing computer security [ISO/IEC 2382-8]

3.2.27

security service
A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers [ISO 7498-2]

3.3 Public key infrastructure related terms

3.3.1

attribute authority
AA
An authority which assigns privileges by issuing attribute certificates [X.509]

3.3.2

attribute certificate
a data structure, digitally signed by an Attribute Authority, that binds some attribute values with identification about its holder [X.509]

3.3.3

authority certificate
a certificate issued to a Certification Authority or an Attribute Authority [adapted from X.509]

3.3.4

certificate
public key certificate

3.3.5

certificate distribution
act of publishing certificates and transferring certificates to security subjects

3.3.6

certificate extension

extension fields (known as extensions) in X.509 certificates that provide methods for associating additional attributes with users or public keys and for managing the certification hierarchy

NOTE: Certificate extensions may be either:

critical - a certificate using system MUST reject the certificate if it encounters a critical extension it does not recognize.

non-critical extension - may be ignored if it is not recognized.

3.3.7

certificate generation
act of creating certificates

3.3.8

certificate management
procedures relating to certificates: certificate generation, certificate distribution, certificate archiving and revocation

3.3.9

certificate profile
specifies the structure and permissible content of a certificate type

3.3.10

certificate revocation
act of removing any reliable link between a certificate and its related owner (or security subject owner), because the certificate is not trusted any more whereas it is unexpired

3.3.11

certificate holder
an entity that is named as the subject of a valid certificate

3.3.12

certificate verification
verifying that a certificate is authentic

3.3.13

certification
procedure by which a third party gives assurance that all or part of a data processing system conforms to security requirements [ISO/IEC 2382-8]

3.3.14

certification authority
CA
certificate issuer
an authority trusted by one or more relying parties to create and assign certificates. Optionally the certification authority may create the relying parties' keys [ISO 9594-8]

NOTE: Authority in the CA term does not imply any government authorisation only that it is trusted. Certificate issuer may be a better term but CA is used very broadly.

3.3.15

certificate policy
a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements[X.509]

3.3.16

certification practices statement
CPS
a statement of the practices which a certification authority employs in issuing certificates [RFC2527]

3.3.17

public key certificate
X.509 public key certificates (PKCs) [X.509], bind an identity and a public key. The identity may be used to support identity-based access control decisions after the client proves that it has access to the private key that corresponds to the public key contained in the PKC [RFC2459]

3.3.18

public key infrastructure

PKI
an infrastructure used in the relation between a key holder and a relying party that allows a relying party to use a certificate relating to the key holder for at least one application using a public key dependent security service. PKI includes a Certification Authority, a certificate data structure, means for the relying party to obtain current information on the revocation status of the certificate, a certification policy and methods to validate the certification practice

3.3.19

registration authority
RA
an entity which establishes the identities of relying parties and registers their certification requirements with a Certification Authority

3.3.20

relying party
a recipient of a certificate who acts in reliance on that certificate and/or digital signature verified using that certificate [RFC 2527]

3.3.21

third party
party other than data originator, or data recipient, required to perform a security function as part of a communication protocol.

3.3.22

trusted third party
TTP
a third party which is considered trusted for purposes of a security protocol [ENV 13608-1]

NOTE: This term is used in many ISO/IEC standards and other documents describing mainly the services of a CA. The concept is however broader and includes services like time stamping and possibly escrowing

4 Abbreviations

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
PKC	Public Key Certificate
PKI	Public Key Infrastructure
RA	Registration Authority
TTP	Trusted Third Party

5 Health care context

5.1 Health PKI Classes of Actors

For the purposes of facilitating the discussion on PKI requirements the following classes of actors are introduced. This does not imply that other classes and definitions are not more appropriate in other contexts.

The focus here is on actors that are directly involved in a health related communication and may require a certificate for a PKI enabled security service. The following actors were defined in Section 3.1.

Persons

health professional

health care non-regulated employee

patient/consumer

sponsored health care provider

supporting organisation employee

Organisations

health care organisation

supporting organisation

Other entities

devices

regulated medical devices

applications

In addition to these actors, the PKI requires certification authorities and registration authorities to be part of the total system and these organisations are important certificate holders in this infrastructure.

Some health care workers are associated with multiple health care organisations. There is a primary need in health care to avoid duplicate or redundant registration with its inherent costs and multiplicity of certificates.

Within the health care context the role of registration authorities is to identify the actors as either a valid health professional performing a given role, or to identify a consumer as the person with rights to his or her own information. There also needs to be a way of registering support staff for physicians in private practice (medical receptionists, billing clerks, file clerks, etc.). Such individuals are not associated with institutions such as hospitals that are covered by national, state or provincial health authorities.

5.2 Examples of actors

5.2.1 Health professional

Examples of health professionals are: physicians, dentists, registered nurses and pharmacists. There are many different classifications of officially regulated/accredited professions in health care in different countries. It is an

important task for future ISO standardisation to create a global mapping between this but for the purposes of this technical specification it is assumed that only very broad classes can be recognised internationally. In part 2 of this ISO/TS a data structure is presented that allows a broad international classification to be used in parallel with a more detailed defined classification that may be national or follow other jurisdictions since health professionals are regulated in provinces or states in some countries.

5.2.2 Health care non-regulated employee

Examples of persons who are employed by a health care organisation but who are not regulated health professionals include medical secretaries and record assistants, transcription clerks (i.e., those who type from a dictated voice recording), billing clerks, and assistant nurses. For the purpose of this technical specification it is important to include the relationship between the employing health care organisation and the employee in a certificate for security services. For the health care professionals it is important to include the relationship with the professional registration body in the PKI structure but a possible employment or other affiliation of e.g. a physician may also be important.

There are many different types of roles or occupations of health care employees and this international technical specification makes not attempt to provide a classification scheme.

NOTE: The fact that the employee is not registered by a body independent of the employer in his professional capacity does of course not imply that the employee is not professional in conducting his services

5.2.3 Patient/consumer

The person who receives health related services is, in most cases called the patient but in some situations it is more appropriate for a healthy person and when considering the contractual relations with the health care providers to call such a person a consumer of health services. Only the patient/consumer who is also a direct user of a health information system is considered in this context.

5.2.4 Sponsored health care provider

There are some types of persons who are providers of health services that are not regulated in the jurisdiction but are active in a community and where their professional role may be certified and sponsored by a registered health care organisation. Examples are in some countries midwifes (who may be sponsored by obstetricians or other physician), physiotherapists of different types, various persons active in community care for disabled and elderly (who may be sponsored by a General Practitioner or a Hospital).

5.2.5 Supporting organisation employee

A person working for an organisation that is a supporting organisation and who is not a health professional.

5.2.6 Health care organisation

Examples of officially registered organisations that have a main activity related to health care services or health promotion are health care providers, health care financing bodies (insurance companies or administrators of governmental public health financing) and health care research institutions

5.2.8 Supporting organisation

These are organisations that are performing services for health care organisations but these do not perform direct health care services

5.2.9 Devices

Devices are equipment such as ECG machines, laboratory automation equipment and different portable diagnostic aids that measure various physiological parameters of a patient. They also include computer devices such as e-mail servers, web servers and application servers.

5.2.10 Applications

Applications are computer software programs running on individual machines and/ or networks. Within the health care context applications which may be part of a PKI could include integrated clinical management systems, electronic health record (E.H.R) applications, emergency department information system, imaging system, prescribing , drug profiling and medication management systems.

5.3 Communication requirements for health care actors and applicability

This Technical Specification for a health care public key infrastructure applies to the health care industry both within and between national boundaries. It is intended to cover public (government) health authorities, private health care providers across the entire range of settings including hospitals, community health and general practice. The technical specification also applies to health insurance organisations, health care educational institutions and health related activities (such as home care).

While the primary aim is to develop a framework where health professionals, health care organisations and insurers can securely exchange health information, the technical specification is also intended to provide consumers with the ability to securely access their own health care information. Transactions can take place with CAs and RAs acting as trusted third parties to enable providers, insurers and consumers to exchange information, safe in the knowledge that it is secure, protected and if integrity is breached it will quickly become known.

Suitable applications within the Health Care Public-Key Infrastructure are:

1 Secure electronic mail
2 Access requests by applications used by community based health professionals for patient information in hospital based information systems.
3 Access requests by applications used within hospital based information systems. Systems would include patient administration, clinical management, pathology, radiology, dietary and other related information systems.
4 Other systems in accordance with local policies

5 Billing applications which require authentication for patients, health service providers and health insurers, together with non repudiation, message integrity and confidentiality.

6 Tele-imaging applications which require a reliable binding between an image and a patient identity, together with authentication of the health professional.

7 Remote access control applications which have a particular need to verify authenticity, confidentiality and integrity.

8 Electronic prescription applications which require all of the security services of a PKI – authenticity to verify the prescription is verified as having originated from a particular health professional, and is being filled for the correct patient. Ensuring there are no errors in transmission requires the integrity service and auditability requires the service of non repudiation.

9 Digitally signed patient consent documents.

10 Transcription services across national boundaries.

A set of scenarios where PKI could be applied is detailed in Annexure B.

Local policies may exclude one or more of the above applications from participation in a PKI.

6 Requirements for security services in Health Care Applications

The health care industry has particular security needs that require special interpretation, which is the reason why this Technical Specification has been developed. Particular characteristics of the health care are:

1 Health information is reusable and can exist for as long as (and longer than) the person it whom it refers;

2 There are significant health consumer and health service provider concerns to ensure health information collected is used for health purposes and not for something else, unless the patient has given their explicit consent to the use of such information (e.g. anonymised patient data may be used for training and planning purposes .

3 There is a need to improve the health consumer confidence in the ability of the health system to manage their information

4 There is a need for health professionals and organisations to meet security obligations in the context of health strategies

5 The need exists to ensure health professionals, trading partners and relying parties in a health care PKI have confidence in measures to ensure privacy and security of patient information

The security issue in the health care becomes more visible as personal health information is being increasingly stored using electronic information systems instead of paper files. The first concern of the health care industry is to protect the privacy and safety of the patient. In particular this concern extends to the need to comply with relevant privacy legislation, in respect of trans-border health information flows. If an information system is going to be used by both health care professionals and consumers/patients, it must be trusted. For this reason, meeting the need for privacy and security is critical for health care information systems.

6.1 Health Care PKI Technical Requirements

Major security threats that need to be addressed in health care information and communication systems are unauthorised access gained through stealing the private key of a legitimate relying party and then masquerading as that relying party. Such unauthorised access can lead to the health care information itself being altered, lost or replicated. A PKI used in combination with a security standard like ISO17799-1 can significantly reduce the risk of unauthorised access.

A PKI is the only combination of policy, procedures and technology which offers the services of authentication, integrity, confidentiality and digital signature. Within the health care context a PKI enables health care providers and consumers who may not know each other to communicate securely and with confidence, by electronic means, through a chain of trust.

A PKI can offer services the health industry has a particular need for. These services and their application to health care are described in more detail below:

Authentication.
Health care is a multi-disciplinary endeavour and health professionals routinely rely upon the judgment of other health care providers when reviewing patient records, consultation reports, and other documents containing personal health information. When these documents and records are accessed and updated electronically, it is essential that the information contained within be reliably attributable to its authors.

It is of paramount importance that health professionals be able to access sensitive personal health information from a variety of clinical settings and at the same time protect this information from access or alteration by unauthorised persons.
Integrity.
Maintaining the integrity of personal health information can literally become a life-or-death issue when such

information is relied upon in the course of providing emergency health care. Moreover, strong incentives exist to corrupt the integrity of some forms of personal health information (for example, narcotics prescriptions).

Confidentiality.
Personal health information is often regarded as the most confidential information in common use. Unlike information communicated electronically for the purposes of e-commerce, the confidentiality of personal health information cannot readily be assigned a monetary value, and a patient's right to privacy, once abrogated, cannot readily be restored.

Digital Signature
Digital signatures used in health care, and the policies and practices to confirm their integrity may ultimately be the subjects of considerable interest during inquest hearings, medical malpractice litigation, professional disciplinary hearings, and other legal or quasi-legal forums where electronically signed documents will be entered as evidence.

A PKI also supports authorization and role based access control services. These services are vital in health care as there are many specializations and many situations that require different levels of access to parts of a personal health information depending on the situation and the role of the health professional involved.

Authorisation

It is essential in health care to only grant rights for personal health information access to those entities, who require them for providing care to the patient/ consumer, or to other entities where the patient has explicitly consented.

Access Control

In health care it is essential that means are in place to ensure that the resources of a data processing system can only be accessed by authorised entities in authorised ways and for authorised purposes/functions, as the consequence of unauthorised access can be impossible to remedy.

When used in conjunction with an appropriate security standard, PKI can significantly reduce the risk of unauthorised disclosure of patient health information.

The purpose of this technical specification is to define the common elements of a PKI which will ensure the chain of trust for communicating health information extends beyond national boundaries.

6.2 Separation of Authentication from Encipherment

There is a particular health industry need to separate the signing from the encipherment function. The reason for this is that authorised health professionals may need to access a patient's record in emergency or special situations when the health professional for whom the message was intended for is not physically present or contactable. It is common practice in health care security to have an individual identity certificate used for authentication and an organisation unit certificate used for encipherment.

This specification advocates that separate certificates and associated keys be used for the purpose of authentication and other for encipherment (ensuring confidentiality). It also recognises the need to have separate certificates to establish identity and others to manage access control, that are bound to the subject's authentication key.

6.3 Health Industry PKI Security Management Framework

The Public-Key Infrastructure required to support the secure movement of health care related information and access to data within and across national boundaries needs to be supported by a framework of generic security management policies To achieve some assurance that the infrastructure operates securely, there is a need to establish codes of practices for its management.

There are already in existence "codes of practice" standards for the management of information security, which are commonly accepted. They include practices for the identification of security risks as well as the application of the

appropriate controls to manage those risks. Three such standards and publicly available specifications are:

- ISO 17799 Part 1 (2000): Code of Practice for Information Security Management
- ISO TR 13335: Guidelines for the Management of Information Technology Security-GMITS
- COBIT (Control Objectives for Information and Related Technologies) specification produced by the Information Systems Audit and Control Foundation.

Such codes of practice place little or no constraint on the services that can be offered by a health care Public-Key Infrastructure and give the signer and verifier a degree of assurance that the electronic signature is not weakened by poor security management.

Consequently this specification will refer to ISO17799 2000 to address the security issues presented in the IETF PKIX RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

6.4 Policy Requirements for a Health Care PKI

The policy requirements and associated practices for a health care PKI are defined in Part 3 of this Technical Specification

7 Public key cryptography

7.1 Symmetric vs asymmetric cryptography

With symmetric cryptography a secret key is used to encipher plain text into a cryptogram that is not readable. Such enciphered information can be deciphered with the same secret key by reversing the encipherment algorithm. This type of cryptosystem is widely used to ensure confidentiality and is called *symmetric or secret key.*

Public key cryptography was first described by Whitfield Diffie and Martin Hellman in 1976. The approach uses two different keys, one public and the other private. (suggest removing this sentence as it conflicts somewhat with the last sentence). Anyone with the public key can encipher a message but not decipher it. Only the person with the private key can decipher the message. It is not possible to deduce the private key from knowledge of the public key alone and the public key can thus made widely known without confidentiality concerns.

Such a cryptosystem is called *asymmetric.* The RSA asymmetric algorithm named after the three inventors (Rivest, Shamir and Adelman) is widely used, either alone or in combination with symmetric cryptosystems. In such hybrid systems, the asymmetric algorithm is used to protect the secret key of the symmetric cryptosystem.

Asymmetric cryptosystems can add value to symmetric cryptosystems or virtual private networks by enabling relying parties to be authenticated, by guaranteeing communication integrity and also by enabling authorisation and access control.

Some public key algorithms such as RSA can be used to recover a message and are therefore suitable for confidentiality protection using encipherment as described above. This algorithm can also be used in the inverse direction where a text enciphered by the private key can be deciphered using the public key. This principle is not suitable for confidentiality protection but for authentication purposes. Only the holder of the private key could produce a cryptogram that can be deciphered using the corresponding private key. This quality can be used to authenticate the origin of messages to someone in possession of the private key.

7.2 Digital Certificates

A digital certificate is a software data structure that binds an entity's public key and one or more attributes relating to that entity's identity - the public keys of an entity, together with other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it [ISO 9594-8]

The entity can be a person, an organisational unit, an application, a server or a hardware device. The purpose of a digital certificate is to provide some level of confidence that the public key belongs to the identified entity and that the entity possesses the corresponding private key.

The level of confidence is provided by the Certification Authority signing the digital certificate with their own private key. By signing the digital certificate, the Certification Authority is taking responsibility for information contained in the digital certificate and providing the certificate holder with some level of authentication.

A Certification Authority publishes certificates, maintains a directory of certificates (together with their public keys). revokes any certificates that may become invalid and ensures all relevant relying parties are promptly informed of any revocation of certificates. The process of managing certificates is described in Part 3 of this technical specification. Part 3 also specifies the role of the Registration Authority and specifies restrictions on who can perform the role of a Registration Authority.

7.3 Digital signatures

A digital signature is data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient [ISO 7498-2]

The digital signature is generated by using the sender's private key to perform a mathematical operation on the message being sent. The method is to use the private key and a one way mathematical function known as a hashing algorithm, to produce a hash (a number) from the original message. The hash function has the property of being one way, in that it is computationally infeasible to produce the original message or private key from the hash. This hash is appended to the message and sent with the message. The recipient then uses the sender's public key to perform the same operation on the message and then compares the resultant hash with the one that has been sent with the message. If the two are identical then the recipient can have a level of confidence that the message was sent by the source that claimed to have sent it.

Since the private key is part of a key pair in which the public key is bound to an identity in a Digital Certificate, the identity of the sender can be verified to a level of confidence previously not possible. The level of confidence is provided by the Certification Authority signing the digital certificate with its own private key. By signing the digital certificate, the Certification Authority is taking responsibility for information contained in the digital certificate and providing the certificate holder with some level of authentication.

The level of confidence achieved is dependent upon the Certification Authority's policies and practices and the key management of the relying parties.

Besides providing a level of confidence about authentication of senders, the use of a digital signature can provide a level of confidence about the integrity of the communication, as identical hash results can only be obtained if the communication used to produce it is the same at the source and at the destination.

7.4 Protecting the private key

Competent key management is critical to the successful functioning of any Public Key Infrastructure within the health industry. If the private key is compromised the PKI is no longer effective in protecting information communicated and stored using that particular key pair. More seriously if the private key of a CA is compromised, the domain of that CA can no longer rely on the PKI for protection.

Protecting the private key requires a combination of management processes and technical methods. Whatever technical option is used, key protection must be managed within an overall Information Security Management Framework. The ISO17799 Information Security Management Standard provides a suitable framework.

A private key can be protected using a hardware token, where the private key is stored on a token which can perform cryptographic calculations and is accessed by the relying party through use of a password or passphrase. This is a more secure method of protecting the private key as there is no electrical connection to the computer, it can not be accessed through a network and sophisticated authentication algorithms can be placed on the token.

It is also possible to use a USB key or similar hardware token, which just stores the private key, with the cryptographic logic stored on a host computer.

A private key can also be stored on a floppy disk. This is less secure. The private key can also be stored on the hard disk of a computer workstation. This is the least secure method as it may be possible to access the private key through a network the computer workstation is attached to.

To access the private key stored on one of these devices, the relying party, or another device or application, is required to be authenticated, most commonly by password or passphrase, or by displaying some otherwise unique characteristic such as a retinal pattern. There are different types of authentication mostly based upon characteristics such as where you are, what you know, are, or have. eg requiring the use of a password (something you know with use of a physical device such as a token (something you have). Using more than one

type of authentication, known as two factor authentication, greatly increases the security of the private key.

This technical specification identifies a need for multiple levels of security and states that higher levels of security will require a hardware token for private key protection. Managing the private key is covered in detail in Part 3, Sections 6.2 and 6.3.

Moving personal health information between jurisdictions, across national boundaries using an insecure medium such as the Internet, where sender and recipient may have had no previous contact and no personal contact means there needs to be methods to authenticate the involved parties, to ensure the information transmitted and stored remains confidential, to ensure the information is not altered in transmission and that none of the parties can later deny having sent or received the communication. This is the business requirement in the health industry for security services that a public key infrastructure can address.

8 Public key infrastructure

8.1 The components of a Public Key Infrastructure (PKI)

Public Key Infrastructure (referred to as PKI in this document) is an infrastructure with the components below used in the relation between a key holder and a relying party including a Certification Authority (CA) that allows a relying party to use a certificate relating to the key holder for at least one application using a public key dependent security service.

A PKI will consist of:

8.1.1 A Certificate Policy

This is a named set of rules that indicates the applicability of a certificate to a particular health care community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of a request by a Renal Specialist for a pathology test. Certificates based on a certificate policy, which is specifically designed to meet the needs of health care information, support services such as authorisation, access control and information integrity. The particular needs of the health care system as described in Section 6, mean that digital certificates need to be specified especially for health care.

8.1.2 Certification Practice Statement (CPS)

This is a statement of the practices which a certification authority employs in issuing certificates to implement the Certificate Policy. For example, it will indicate the actions it will take when it receives a request from a health authority to issue a health professional a certificate.

8.1.3 Certification Authority (CA)

A Certification Authority (CA) is a trusted entity that verifies the identity of a relying party, allocates a Distinguished Name to that relying party, and verifies the correctness of information concerning that relying party by signing the data and in doing so verifying the binding between names or identities and public keys, which constitutes the digital signature for that relying party. (It is conceivable that some of the CA functions may be devolved to the RA e.g. allocation of a distinguish name, which is best performed at a local level.

The private key can then be stored on the subject's computer, on a floppy disk or other media such as a smart card. The key is generally accessed by the relying party entering a pass phrase.

This Technical Specification recognises that health authorities may obtain certification services in different ways. Some may run their own, others may outsource the activi ty to accredited private organisations. There may also be multiple certifications depending on the purpose for which the certificates are issued. Certificate holders may also have multiple certificates.

Depending on how countries organise their own health care public key infrastructure, there may be up to several levels of CAs who may provide certificates for relying parties within an organisation, for the health care industry as a whole, or for anyone in that country.

The Certification Authority should be a recognised organisation with suitable controls and procedures in place to provide the required degree of trust. The controls and procedures need to conform to ISO17799.

8.1.4 Registration Authority (RA)

A registration authority is an entity which establishes the identities of relying parties and registers their certification requirements with a Certification Authority. *[ISOTC215/WG4 Glossary of Security Terms].* A registration authority may also verify a relying party's role, rank or employment status for information that may be stored on an attribute certificate. In this situation it is possible the registration authority that verifies an attribute like employment status eg a government hospital authority, may be a different registration authority to an organisation that verifies a health professional's qualification to practice eg a health professional registration board.

The identification of the Health Care Professional role may be performed by such bodies as:

- National/ State or Provincial Health Authorities (covering associated hospitals and health facilities)
- Medical or Health Professional Registration Boards
- Medical or Health Care Professional Bodies for example Colleges of Surgeons, Psychiatrists, Nurses.
- Public or Private Health Insurance Organisations

A health care PKI may rely on one or more of these bodies for the validation of health professional's credentials. Procedures for registration are described in Part 3, Section 3.1.8 to 3.2.3.

8.1.5 Certificate Distribution (and Revocation) Systems

The CA has the important role of distributing certificates to subjects, maintaining a directory of certificates (together with their public keys). revoking any certificates that may become invalid and ensuring all relevant relying parties are promptly informed of any revocation of certificates. It needs to set up systems in order to do this. These systems and their applicability to supporting the transfer of information across national boundaries are described in Parts 2 and 3.

8.2 Establishing Identity using Qualified Certificates

Qualified Certificates are a type of certificate whose primary purpose is to identify a person with high level of assurance in digital signature services. Qualified Certificates are particularly relevant in relation to the legal recognition of electronic signatures. This specification makes provision for the use of Qualified Certificates in response to increasing numbers of countries legislating requirements to be met by health and other service providers supporting electronic signatures and requirements for signers and verifiers so that an electronic signature can be legally recognised.

The need for qualified certificates has been recognised by the IETF which has produced *RFC 3039-Internet X.509 Public Key Infrastructure Qualified Certificates Profile*. This RFC forms a certificate profile for Qualified Certificates and aims to define a general syntax independent of local legal requirements. The Qualified Certificate profile is used by the IETF to describe the format for a certificate whose primary purpose is to reliably identify an individual person. The IETF Qualified Certificates Profile is used by this specification as the framework to support qualified certificates. A Qualified Certificates profile is specified in Part 2.

Within the health care context a qualified certificate could be used to reliably identify an individual health care provider or consumer to a level of confidence necessary to validate that person's electronic signature. This technical specification recommends the use of qualified certificates for regulated health professionals and non-regulated health care employees.

8.3 Establishing Specialty and Roles using Digital Certificates

This specification recognises that not all doctors are the same in the eyes of a patient/consumer. Patients/consumers may use different physicians for different health issues. HIV/AIDS, communicable diseases, mental health, are just some of the health issues where people manage separate relationships. As a result a decision to grant a health professional access to particular parts of an patient/consumer's health record is usually

based on that health professional's specialty eg Surgeon and role eg Duty Surgeon at Midtown General Hospital Emergency Department.

It is critical to note that authorisation information does not have the same lifetime as the binding an entity identity to a public key. For example someone may be a qualified Physician for 40 years but may only be contracted to work as a Consultant Psychiatrist at a particular hospital for several months. When authorisation information is placed in a Public Key Certificate (PKC) extension, the general result is the shortening of the PKC's useful lifetime. Secondly, the PKC issuer is not usually authoritative for the authorisation information. In this case the PKC issuer may be able to verify the person concerned is a particular Medical Doctor but is less likely to be able to verify that person's role as the consulting psychiatrist in a particular hospital. This results in additional steps for the PKC issuer to obtain authorisation information from the authoritative source. It may also result in a shortening of the life span of a PKC because some of the information it contains is no longer valid, causing an increase in administrative effort to revoke that PKC and issue a replacement. For these reasons, it is often better to separate this authorisation information from the PKC. *[INTERNET-DRAFT October 1999 4.1 X.509 Attribute Certificate]*

While the IETF Attribute Certificate Specification describes how the public key is used to validate digital signatures or cryptographic key management operations, it states that not all request and disclosure decisions are identity-based. Such access control decisions can also be rule-based, role- based, and rank-based decisions and therefore require additional information. For example, information about a health professional being a particular type of specialist may be more important in deciding access than their identity. In these situations authorisation information to support such decisions may be placed in a PKC extension or placed in a separate attribute certificate (AC). [INTERNET-DRAFT October 1999 4.1 X.509 Attribute Certificate]

This Technical Specification recommends that the PKC should have proving identity as it main purpose. Information provided on X.509 Certificates about a relying party's identity and authorisations can be used as the basis for making decisions on whether to disclose information in response to a request made on a server for a certain purpose (Identification /Authentication, Encipherment/ Deciphement). X.509 public key certificates (PKCs) [X.509],[RFC2459] bind a client identity and a public key. The identity may be used to support identity-based decisions which manage requests and disclosure of information after the relying party proves that they have the private key that corresponds to the public key contained in the *PKC [INTERNET-DRAFT October 1999 4.1 X.509 Attribute Certificate]*

Once identity is proved, attribute certificates can then be used to more appropriately manage information in situations where some of the information bound to a PKC is more volatile or ephemeral than other information. For this reason provision is made in this Technical Specification for attribute certificates.

However there are difficulties with this approach. The detailed specification for Attribute Certificates is still evolving and the specification still needs to be more widely implemented in the software industry. Also information about the a health professional's specialisation eg. Psychiatry, Paediatrics, Urology does have some longevity. Also there needs to be some capacity to record information about a patient/ consumer role. For these reasons, this Technical Specification makes provision for this by specifying an extension called HCRole to the PKC Identity Certificate Types. This extension is specified in Part 2, Section 4.1.

8.4.1 Using Attribute Certificate for Authorisation and Access Control

The IETF Attribute Certificate Specification concludes that the placement of authorisation information in the Public Key Certificate (PKC) is not desirable. This technical specification recognises the desirability of multi-useability and need to minimise the information to be kept on identity certificates. It recommends that secondary roles, group membership, security clearance be placed on accompanying attribute certificates.

It is noted that authorisation information is distinct from information on health-care roles or licences, which may be appropriately included in a PKC. Role or licence implies an authorisation level, but they are not necessarily authorisation information in themselves. This specification makes provision for the use of Attribute Certificates to support the transmission of role based information regarding health care providers.

While an identity certificate issued by a PKC may imply a role, it does not contain sufficient information in many situations to make the access control decision. For example while a PKC issued on behalf of a physician on behalf of a Registration Authority like the College of Surgeons, does imply that physician is a surgeon, it is usually not sufficient information to authorise that physician while employed as a locum in a particular hospital emergency department to admit a patient to the hospital.

Such detailed authorisation information is more appropriately supplied by using an attribute certificate that is bound to the health professional's public key. A health professional may have many attribute certificates which reflect multiple roles. Such attribute certificates are typically more short lived than an identity certificate.

The IETF Attribute Certificate Internet Draft also states that authorisation information needs to be protected in a fashion similar to a PKC and an attribute certificate (AC) provides this protection. It is simply a digitally signed (or certified) set of attributes. An AC is a structure similar to a PKC; the main difference being that it contains no public key. An AC may contain attributes that specify group membership, role, security clearance, and other access control information associated with the AC owner.

A specification of the data elements in an Attribute Certificate in accordance with *INTERNET-DRAFT October 1999 4.1 X.509 Attribute Certificate* is provided in Part 2. As the specification for attribute certificates is still evolving, health care attribute certificate types will be specified in more detail in later versions of this Technical Specification.
Need to include a short paragraph on the need for Attribute Certificate Authorities to make this section complete.

9 Interoperability requirements or models?

9.1 Overview

This technical specification seeks to adopt and add to the Internet Engineering Task Force (IETF) and other existing security standards to support the secure electronic transfer of health care information across national boundaries. The Internet is becoming increasingly used as the vehicle of choice to support this transfer.

The purpose of this technical specification is to define the essential elements of a health care public key infrastructure to support the secure transmission of health care information across national boundaries. The specification must be Internet based if it is to work across national boundaries. For this reason it uses the *IETF PKIX RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* as a basis for the specification and references other relevant IETF RFCs as required.

The secure transfer of health information across national boundaries could be achieved by participating countries mutually recognising the mechanisms each country puts in place to review the policies , practices and procedures to accredit Certification Authorities.

The governance of health care PKIs needs further development and is outside the scope of this Technical Specification. This specification suggests that interoperability across national boundaries be achieved by a series of bilateral and multilateral agreements between countries, based upon minimum requirements as specified in Part 3 of this Technical Specification Ultimately the relying party needs Certification Authorities to establish procedures as needed, to enable them to use the infrastructure with the level of assurance required.

9.2 Options for Setting up a Health Care PKI across jurisdictions

The main issue to address for any PKI that aims to span jurisdictions, including national boundaries, is trust. Trust is the practice of many parties relying on the policies and practices and, by extension, the validity of digital certificates issued to a relying party by some established authority. The options for deploying a health care PKI architecture may be summarised as follows:

Option 1: Single PKI Hierarchy

This is from a technical viewpoint, the easiest option. It is not feasible however to establish a world spanning health care PKI with one centralized registration and certification authority. Registration could be devolved I this scenario. However, if this were the case, the management arrangements might be unworkable.

Option 2: Relying party management of trust

In this option it is the responsibility of the relying party to decide whether to trust the issuing Certification Authority concerned. This option has inherent difficulties as it requires the trust decision to fall on the relying party, in some situations this may place inappropriate responsibility upon the relying party who may not be in a position to make an informed decision.

Option 3 – Cross Recognition

This term refers to an interoperability arrangement in which a relying party in one PKI domain can use authority information in another PKI domain to authenticate a subject in the other PKI domain, and vice-versa. Typically such authority information either results from a formal licensing or accreditation process in the jurisdiction of the other PKI domain, or else results from a formal audit process performed by or on behalf of a representative CA of the relying party' s PKI domain. Technically, the information can be stored as the value of a certificate field accessible by the relying party.

Compared to cross-certification, the onus of whether to trust a foreign PKI domain lies with the relying party or the owner of the application or service, rather than a CA that the relying party directly trusts. It does not necessarily involve a contract or an agreement between two PKI domains.

In a cross-recognition arrangement, detailed mapping of Certificate Policies and Certification Practice Statements is not necessary. Instead, the relying party (via the application at hand) decides whether to accept a foreign certificate for the purpose depending on whether the certificate has been issued by a trustworthy foreign CA.

The CA is regarded as trustworthy if it has been licensed/accredited by a formal licensing/accreditation body or has been audited by a trusted independent party. Also, the relying party must be able to unilaterally make an informed judgement based on the policies stipulated in the Certificate Policy or Certification Practice Statement in the foreign PKI domain. Hence, the process is comparatively less complicated than cross-certification, especially policy and legal harmonisation. The process is also inherently scalable.

However it is procedurally less rigorous than cross-certification and places a potential burden on the relying party, who may not be aware of the full consequences of accepting a certificate. [APEC Achieving PKI Interoperability]

In cross-recognition, the decision of whether to trust a foreign certificate lies with the relying party and not his or her CA.

Option 4: Cross Certification

This option moves trust decisions to protocols operating within the PKI infrastructure. This model is more difficult to achieve than Options 1 or 2 or 3, but is more user friendly and easier to support from the end user's perspective. It also means the end user may not need to assume the responsibility for making the trust decision, as it can be left to the Certification Authority for that end-users Certification Authority domain.

Cross-certification results in a bilateral approach with two PKI domains (in whole or in part) being merged into one larger domain through an elaborate process carried out by two representative Certification Authorities. For hierarchical PKIs, the representative Certification Authority is usually the root CA. However, cross-certification can also be implemented between any two Certification Authorities. In the latter case, each PKI domain constitutes only one Certification Authority and its subscribers. For cross-certification to be possible, there must be compatibility at the application level, the policy level and the technical level. When this occurs, for the relying party in the

Certification Authority domains covered by cross certification, the movement of information is transparent and the Certification Authorities are responsible for decisions about trust.

The process of cross-certification requires detailed mapping of the respective policies of each CA and the effort in doing this will increase geometrically with each CA domain that is to be included in the PKI domain. This raises issues of scalability. There is also a risk that a third CA may cross certify with the second CA, but find the first CA's policy inappropriate. In a situation like that CA-3 cannot exclude CA-1. As a result, cross-certification is more relevant for *relatively closed health care models* and at best, *open but bounded systems.* It is most suitable if the two PKI domains belong to two work contexts that share a close working relationship with each other. For example, both work domains may share the set of applications and services e.g. email and financial applications. [APEC Achieving PKI Interoperability]

In cross-certification, the decision of whether to trust a foreign certificate lies with the Certification Authority and not the relying party.

Option 5: Bridge CA

The Bridge Certification Authority model depends upon all of the Certification Authorities within the potential community of CA domains agreeing to a common set of minimum standards. These minimum standards are then incorporated into their own Certificate Policy and Certification Practice Statements. The difference from the Cross Certification model is that individual Certification Authorities may have their own local requirements in addition to the shared minimum standards. These local requirements are not required for Bridge Certificates from relying parties who are not in that local CA domain. This model works best where Certification Authorities have a considerable common interest and are prepared to allow some local variations. Usage examples could be where State or Provincial health authorities within a particular country.

In this model, organisations can build their own CAs, then decide later whether to join a Bridge CA or not.

In the Bridge Certification Authority model, the decision of whether to trust a foreign certificate lies with the Certification Authority and not the relying party.

9.2.1 Option Usage

This specification recognises that differences in administrative arrangements and policies exist between jurisdictions. As a result any option may be acceptable. What ever option is chosen will benefit from adopting this Technical Specification

In order to allow maximum flexibility, Part 2 Certificate Profiles, defines profiles for bridge certificates and defines fields on CA Certificates fields for the CA's Audit Status and Auditor's accreditation which will support cross recognition.

Annex A. (informative) Bibliography

APEC Telecommunications Working Group , Business Facilitation Steering Group Electronic Authentication Task Group PKI Interoperability Expert Group, Achieving PKI Interoperability., September, 1999.

ASTM Draft Standard: Standard Guide for Model Certification Practice Statement for Health care**.** January 2000

Canadian Institute for Health Information: Digital Signature and Confidentiality Certificate Policies for Health PKI, 2000

Drummond Group, The Healthkey Program **,** PKI IN HEALTH CARE: RECOMMENDATIONS AND GUIDELINES FOR COMMUNITY-BASED TESTING, MAY 2000.

EESSI European Electronic Signature Standardisation Initiative (EESSI), Final Report of the EESSI Expert Team 20th July 1999

Feghhi Jalal, Feghhi Jalil, Williams Peter, Digital Certificates – Applied Internet Security, Addison-Wesley 1998.

Government of Canada, Criteria for Cross Certification, 2000

Klein, Gunnar, Lindstrom Valter, Norr Anders, Ribbegard Goran, Torlof, Per Technical Aspects of PKI, January 2000

Klein, Gunnar, Lindstrom Valter, Norr Anders, Ribbegard Goran, Sonnergren Elizabeth, Torlof, Per, Infrastructure for Trust in Health Informatics, January 2000

Strategies for the Implementation of a Public Key Authentication Framework (PKAF) in Australia SAA MP75, Standards Australia

Wilson, Stephen, Audit Based Public Key Infrastructure, Price Waterhouse Coopers White Paper, November 2000.

Annex B. (informative) Scenarios for PKI Use in Health Care

B1. Introduction

This annex presents a series of high-level business cases or "scenarios" representing core business and technical requirements for PKI solutions that will support a broad cross-section of the health care industry.

General requirements are presented first, speaking to basic privacy and security principles and fundamental needs of the health care industry. The document then details each scenario as follows:

1. A description of the scenario, or health care situation requiring secure, private electronic communications

2. Business and technical requirements that a PKI solution must provide

B2. Scenario Explanation

The care scenarios described in section B3 show how PKI can be used in health care. Each scenario is intended to be:

1. Policy Driven:

   The scenarios are intended to show how PKI can implement the requirements of the health care industry to implement international, national and local requirements to ensure that information used to provide health care to individuals and communities is used for the purposes for which it is intended.

2. Applicable across Health Care

   With the dispersed nature of health care across the world, together with the range of different persons and organisations that will need to actively co-operate to provide seamless health care, it is essential that any PKI be able to operate across different health care settings, including hospital and community based care, public and private sectors.

3. Technology Neutral:

   One of the essential purposes of developing a PKI Technical Specification for the health care industry is to ensure that information can be securely passed between providers, consumers, insurers and other relevant parties without regard to the vendor, hardware, operating system or applications they are running.

4. Satisfying Current and Emerging Privacy Requirements:

   If electronic health applications are to become widely used, they need to be trusted by providers and patients. Privacy and security concerns need to be addressed to develop this trust.

5. User Friendly:

   The security services provided by a PKI should not interfere with the authorised function of the health care organisation or professional. If the daily operation of a security system becomes too onerous, clinicians will try to by-pass it, or will not adhere adequately enough to the management procedures. If this occurs there will be significant risk of a security breach.

B.3 Services Exemplified in Health Care Scenarios

Service	Scenario Number														
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	15
Authentication	X		X	X	X	X	X	X	X	X	X	X	X	X	X
Confidentiality	X		X			X	X	X	X	X	X		X		
Integrity		X		X	X		X	X						X	
Digital Signature		X		X	X			X			X	X	X	X	X

Scenarios

1. ER Access to Records
2. Temporary Services (Emergency Aid)
3. Enrol new member
4. Tele Imaging
5. Automated Results Reporting
6. Results Reporting/ Practitioner Messaging
7. Patient Physician Treatment Discussion
8. Patient Care Registry Summary
9. Patient Pharmacist Question
10. Patient – Pharmacist Messaging
11. Remote access to Clinical Info System
12. Emergency Access
13. Remote Transcription
14. Electronic Transcription
15. Authenticate Physician Order

B.4 Scenario Descriptions

B.4.1. Emergency Department access to records

Scenario Description

A patient, visiting from another country is brought into an Emergency Department (ED). The patient is unable to answer questions coherently, and a medical history cannot be reliably obtained. His health plan membership card is in his wallet, and positive identification is provided by his passport

Without PKI:

From the information on the health plan card, the attending ED physician attempts an international call to the health plan. Because of time zone differences, the physician is asked to call back when the administrative office is open. The physician treats the patient's symptoms. The cause of the patient's incoherence is unknown.

With PKI:

From the information on the health plan card, the attending ED physician accesses the patient's health plan site over the Internet, and presents her digital certificate identifying herself in her current role as an ED physician. The health plan web services validates the electronic credential by verifying the digital signature, checking that the certificate is not expired or revoked. Because this credential is validated and follows existing standards, it is accepted by the health plan's web services and access to the patient's chart is granted. An audit record documenting access is created with date, time, attending physician's full name and medical license number, and identification of the ED facility. The physician learns from the medical history, allergies, and current medications that the patient has had a recent change in one of his prescriptions and may have had an adverse reaction. After treating the patient, the ED physician sends a digitally signed and enciphered copy of the Emergency Department visit to the health plan, which places it in the patient's electronic patient record, indicating the presenting symptoms, diagnosis, treatment, and disposition.

B4.2. Temporary Services (Emergency Aid)

Scenario Description

A major earthquake causes extensive damage in a large metropolitan area. Local hospitals and clinics are themselves damaged, and there are catastrophic numbers of deaths and injuries. National health resources are unable to deal with the conditions, and international offers of aid are accepted.

Without PKI:

It is not possible to immediately verify the qualifications, practice licenses of the health professionals offering help. It is also not possible to ensure that early offers of help are not later denied.

With PKI

The offers of help from health professionals are immediately validated by reading their attached digital certificates. The messages of help are not able to be repudiated because they have been digitally signed by the private key of those offering help.

B.4.3. Enrol Member

Scenario Description

In preparation for a six to twelve month stay in another country, a head of the household arranges for health plan coverage.

A prospective member wishes to enrol in a health plan. He accesses the insurance company's home page which contains membership enrolment forms. He completes the form and sends it to the enrolment department's mailbox. The form is validated and forwarded to Medical Review. Medical Review makes an appointment for a physical exam for the prospective member and notifies him by letter. The prospective member keeps the appointment and the physician determines that he is acceptable for membership. The physician notifies Medical Review and this information is forwarded back to Membership Enrolment. Membership Enrolment sends Mr. Charles a contract under which he agrees to have his monthly dues deducted from a checking account. Membership Enrolment accepts the new member, and sends instructions for obtaining his photo ID health plan card. As part of the membership process, the prospective member has to show a driver's license or other recognised Photo-ID. When he receives his new health plan Photo-ID card, he also receives instructions for downloading a digital certificate from the health plan.

Without PKI:

It will not be possible for the new member to reliably identify himself to the physician, nor for the physician to identify himself to the patient. Although there are other means to encipher the messages between the two. The combination of authenticity and confidentiality is not possible.

With PKI

Using the newly issued digital certificate, he is able to access member services over the web, including some of his personal health data, and exchange secure e-mails with his physician

B.4.4. Tele-Imaging

Scenario Description

A physician tele-imaging specialist interprets an angiogram series by viewing them on a PC and creating a text version of the analysis. The specialist has a heavy workload (10-15 cases per day) and prefers to do some of it at home. At home, the physician accesses the imaging server over the Internet, using her digital certificate to authenticate herself, and downloads the images. While viewing the images on her workstation the physician also accesses the health care institution's clinical information system over the Internet to review other medical information on the patient. The physician is confident the image is correct because the application includes an integrity checking function, through use of a hashing algorithm which verifies the integrity of the message. The physician enters the findings she sees on the images into an imaging report and has the option of electronically signing her reports remotely.

Without PKI:

The physician is not able to authenticate herself to the hospital to the same level of confidence as with a digital certificate, which means the acceptance of some risk by the hospital that they may be downloading images to an impostor. Her electronically transmitted opinions and findings are also open to the same risk. The physician can also not be sure the downloaded image has not suffered some transmission error or intentional alteration.

With PKI

The physician can authenticate herself to the hospital to a level of confidence that will be acceptable to a court of law. The physician can be confident that the image downloaded to her is correct and she will not make her findings on an inaccurate image. The hospital can also rely on her digital signature to verify she did send the report.

B.4.5. Automated Results Reporting to the Physician

Scenario Description

On Tuesday, a patient goes to the lab and has some blood drawn.. When the result is ready, the system automatically generates a message to the physician, telling him his results are ready. On Thursday, the physician logs onto the health care delivery organisation's web site with his Health Worker ID and PIN. He sees that there is a message waiting for him and goes into his in-basket. There he finds a message with the subject "Cholesterol Test." The message tells him his patient's cholesterol level is 220 and this puts the patient in the moderate risk category. The physician discusses the result with the patient and suggests the patient contact the lipid management team to learn how to reduce his cholesterol through diet and exercise. The physician also recommends a follow-up repeat cholesterol test and office visit in 6 months. The patient requests the physician to add the result to the patient's internet based electronic medical record. The patient's web site contains several links for additional information. One link leads to information about the cholesterol test itself. A second link connects him to the lipid management team appointment scheduling function, and another link leads to personal diet recommendations based on current clinical protocols, which have been drawn from a variety of data about the patient (e.g., age). The diet recommendations contain further links to a behaviour-change support application that helps him create and track his diet over the next 6 months.

Without PKI:

The laboratory cannot be sure that physician ha received the message. There is no guarantee the message will not have been read or altered.

With PKI

PKI will ensure proof that the physician has received the message and the physician can be sure the message has indeed come from the laboratory and the links given to the patient for managing the cholesterol issue are valid.

B.4.6. Results Reporting with Practitioner Messaging

Scenario Description

During a routine doctor's office visit a physician orders a CBC (cell blood count) for his patient. After asking the patient about her preference, the physician checks a box on the order screen, indicating that the results should be sent to the patient via the Internet after the physician has viewed them and had a chance to comment.

The results come back mostly normal, with one result slightly high. The physician knows that this is of no concern for the patient, so he types a quick note to that effect and attaches it to the result record.

Later that day, the patient gets a generic notice in her email box that a message from her doctor is waiting for her on the secure web site. She clicks the embedded URL, enters her Medical Record Number and password, and reads both the lab result and the message from her physician. The web site has automatically determined that this is a CBC result and displays a link to the health encyclopaedia section that contains a lay person's description of the CBC and its results.

Without PKI:

Without the ability to confidently authenticate the e-mail from the laboratory or the physician, or to ensure it is transmitted in an enciphered secure form, the patient receives the result by post, notices the slightly high reading for one result and telephones the physician for further information. The physician is with another patient and cannot be disturbed, while the patient with the blood test has an important meeting to attend. They finally connect but not without a few days of anxiety on behalf of the patient and a number of unsuccessful telephone calls by the physician.

With PKI

The results are rapidly conveyed to the patient in a verified, secure manner, the patient is able to read the physician's explanatory e-mail and access the web sites for more information and her anxiety is quickly eased, without requiring the telephone conversation.

B.4.7. Patient-Physician Treatment Discussion

Scenario Description

A member covered by a health insurance plan, has a question about her treatment plan. She logs onto her physician's web site, using a trusted digital certificate for authentication, fills out a message form, and clicks "Send" to initiate the conversation:

> *Hi, Dr. C.*
>
> *Yesterday you told me to change the dressing on my wound. But I can't remember how often you want me to change the dressing. You said something about not changing it as often as normal, but I don't remember if you said to change it once a week or what. Also, I forgot to ask you—how much of a scar do you think it will leave?*

Within a couple of hours, an advice nurse at the Call Centre reviews the patient's message and determines that it is non-urgent and that it should be responded to by a member of her Primary Care Team. Shortly thereafter, the message appears on the computer screen of the patient's primary care physician, who types in a response, and digitally signs the message. The next morning, the patient logs onto her physician's web site again, and reads the message:

> *Hi, [Patient Name].*
>
> *For the next couple of weeks, only change the dressing every 4 or 5 days, unless it becomes wet, in which case you should change it right away. After that, you'll be seeing me again and we can decide where to go from there. In terms of a scar, I think you'll always have a bit of a scar there, but it won't be very strong—just a little bit of a line.*

Without PKI:

The absence of a reliable authentication technique means the health care organisation the physician works for is unable to verify that [Patient Name] is the person e-mailing them, and it may be someone else seeking free advice. The patient can also not be certain that the reply from the physician did in fact come from him. Neither can be certain the exchange has not been intercepted and read by a third party.

With PKI

The health insurance organisation and the physician can be confident they are securely communicating with a known and valid member of one of their health plans. The patient can be confident her physician did address her inquiry and it is in fact him who is replying to her.

B.4.8. Patient Care Registry Summary

Scenario Description

The Diabetes Risk Registry gathers clinical data from a variety of clinical information systems in the health care delivery organisation about a patient with diabetes. Clinical guidelines built into the Registry enable the generation of a personal report summarising the patient's condition, history, risks, and next steps. This summary report, after review by the physician is presented to the patient via the organisation's web site. The patient authenticates to the web site using a digital certificate issued by the health care delivery organisation's CA. When the patient views the summary, hypertext links embedded in the report enable him easily to view relevant educational information (e.g., class schedules, descriptions of tests, patient education), request a non-urgent appointment, or send a message to a clinician. The system provides assurance that the patient has accessed the report.

Without PKI:

Without PKI there can not be sufficient level of confidence for the patient that the web site is really the web site of the Diabetes Risk Registry and that the communication with the registry is confidential. It is also not possible for the registry to be certain that the patient has accessed the site and received the information.

With PKI

PKI enables the patient and Registry to authenticate each other, to conduct confidential communication and to the Registry can be certain the patient has accessed the site and received the information.

B.4.9. Patient Pharmacist Question

Scenario Description

A health plan member's 7 year-old daughter has asthma. The paediatrician recently prescribed cromolyn for her, but the member can't tell when the inhaler is empty and when it's full. He goes to his health care organisation's web site looking for information about this, but he's still confused, so he sends a question to the Online Pharmacist asking how to tell when an inhaler is empty.

The Online Pharmacist uses e-mail with access to a health care PKI directory, where the member's digital certificate and public are stored, and sends an enciphered message, using a template designed for this question, and adding a few personal lines and a phone number to call if there are still questions.

Without PKI:

It would not be possible for the pharmacist to authenticate to the required level of confidence, the health plan member. It would be possible still to send a secure message but it would not be able to be authenticated.

With PKI

With PKI it would be possible to authenticate the member and send them an enciphered message. The member could be confident that it came from the pharmacist.

B.4.10. Patient-Physician Messaging, unstructured to specific clinician

Scenario Description

A patient has a rash and sees a dermatologist, who prescribes a cream. The dermatologist tells the patient that if the rash hasn't cleared up in 3 weeks, he should let her know so that she can prescribe a different medication.

Three weeks later, the rash still looks pretty much the same, so the patient logs onto the group practice web site, using his health care digital certificate to authenticate himself. He sends a secure, unstructured message to the physician:

> I've been using that cream for 3 weeks now, and it hasn't gotten any better. What should I do now?

The physician writes a new prescription and tells the patient he can pick up the new cream either by coming in to the pharmacy or by ordering it online.

When the patient reads the message from the dermatologist on the secure web site, he simply clicks to the online pharmacy section and orders the cream to be shipped to his home.

Without PKI:

The physician is not able to authenticate the patient to a high enough level of confidence to give e-mail advice on treating the condition.

With PKI:

The physician and patient can authenticate themselves to each other and the pharmacist. Confidential messages can be exchanged and a new type of cream can be ordered with the pharmacist. All parties are confident the others did send the messages they claimed to have sent.

B.4.11. Remote Access to a Clinical Information System

Scenario Description

A physician dials in to his organisation's Clinical Information System Results Management Functions. He uses the system functionality to

- review test results,
- notify patients of their results by auto-generation of letters, or email including personal comments from the physician,
- orders more tests,
- orders a new medication,
- changes a medication dose.

The patients are notified by phone, letter or email of a new inbox item for them in the organisations secure web site.

The system marks the reviewed tests as:

- signed-off (reviewed),
- patients notified,
- how notified, and
- acted on.

Without PKI

Not being able to authenticate the physician's identity to an acceptable level of confidence, would prevent the above exchange occurring.

With PKI

Nonrepudiation of origin, and receipt, integrity, and confidentiality of these actions and messages are provided under the Clinical Information system and web site, using the organisation's PKI.

B.4.12. Emergency Access

Scenario Description

An Emergency Department Physician is treating a patient brought into the emergency department in a semiconscious condition. The patient is incoherent, and is unable to explain what has happened. While the potential causes of the condition are many, they could be caused by interactions or complications of abused substances, or by medication used to treat psychiatric disorders. The patient is in a life-threatening situation, and it is important to know medical history (including possible recreational drugs used) as well as all medications prescribed. A methadone prescription, for example, would likely be hidden from general access because it is part of a State law protected substance abuse program. The physician initiates the "break the glass" routine, granting him access to information on all of the patient's prescriptions and medications, including those that are restricted information. The system uses PKI authentication and the contents of the physician's digital certificate to create a record of the emergency access of restricted data.

The ED physician sees that the patient has a history of cocaine and methamphetamine use, and has been prescribed lithium. He follows the recommended protocols, ensuring that a diagnosis and treatment are rendered in the most expeditious fashion. A full report of the emergency access log will be generated for follow-up by the IT Security Department and/or the security committee.

Without PKI

Depending on the level of security placed on the patient's file, it may not be possible for a normally non treating physician to access the data. This situation could be life threatening. If he could access the record, without the digital certificate it would not be possible to link with any degree of confidence the accessing of the record with the identity of the accessing physician.

With PKI

The physician could authenticate himself to the system using his digital certificate and obtain the required information about the patient. However an audit trail would be left that could be investigated later for any unauthorised patient access.

B.4.13. Remote Transcription

Scenario Description

A physician dictates a consultation note on one of his patients, via telephone connection to the ABC Transcription Service in Virginia, USA, which contracts Toronto Memorial Hospital in Canada, where the patient is currently hospitalised. The dictation is accessed and transcribed by a subcontracting medical transcriptionist in India, who posts it to ABC Transcription Service's secure Web site. After it is accessed, reviewed, and approved by the service's QA reviewer, the document is again posted to the company's secure Web site and the transcription supervisor at Swanson Memorial Hospital is alerted by e-mail that it is available. She posts it on the hospital's secure Web site and in turn notifies the physician that it is available for review. After access, review, and authentication by the physician, the document is added to the patient's electronic medical record.

Without PKI

It would not be possible for the transcriptionist, the QA reviewer, nor the physician to authenticate themselves to the required level of confidence to enable the interaction to take place.

With PKI

PKI would enable authentication of all authorised parties, ensure the confidentiality of the record and would ensure that none were able to later deny the communications existed.

B.4.14. Electronic Prescription

After conclusion of an appointment, a physician writes an electronic prescription for the patient. The ePrescription system verifies that the drugs prescribed are in the formulary, that the patient has no known allergies to the medications, checks for interactions with other medications the patient may be receiving, and verifies that the amounts prescribed are within best practices guidelines. The physician digitally signs the prescription, and transmits it to the pharmacy. The pharmacy receives the prescription, verifies the physician's medical credentials and digital signature, fills and files the ePrescription. By the time the patient reaches the pharmacy, the prescription is ready and waiting.

Without PKI

It would not be possible to authenticate the physician and also the physician could later deny having sent the ePrescription.

With PKI

It will be possible for the pharmacy to verify the physician's identity and credentials and the fact he has ordered the prescription. The physician would not be able to later deny that he had ordered the ePrescription.

.

B.4.15. Authentication of Physician Orders

Patient presents to the physician's office with a complaint of epigastric pain for some months. The patient reports that the pain is relieved by food and antacids, but is chronic and recurrent. After and initial examination, the physician suspecting peptic ulcer disease decides to schedule the patient for an outpatient upper gastrointestinal endoscopy. From his office computer he is able to access the ambulatory clinic's central scheduling application. He is able to determine that an appropriate time is available for the procedure in the morning. He is then able to complete and digitally sign an admission order scheduling the patient for the endoscopic procedure.

Without PKI

The clinic would not be able to authenticate the physician to a high enough level of confidence, as a result the physician would need to telephone the clinic and make the appointment manually, taking considerably more time.

With PKI

The physician would be able to authenticate himself to the clinic, make the booking and the clinic could be confident it was the physician who make the booking and he would not be able to claim at a later time that he did not make the booking.