Health Certificates
Certification Practice Statement (CPS)
for the
New Zealand
Certificate Authority (CA)

Document Number:	CAS01 Certificate Practice Statement v7.0.doc
Version Number and Status:	7.0
Publication Date:	11 January 2007
Authors:	HealthLink Limited

Table of Contents

HealthLink CPS Revision Record

Identification

'HealthSecure', 'SecureCert' and 'HealthGoldCert' Certificates Certification Practice Statement – NZHealth CA.

Distribution List

All Health Certificates subscribers via HealthLink's web site and internally, as a controlled document.

Version Release History

Change control applies to this document.

Revision date	No. of revision	Section revised	Subject of revision	Reviewed by
13/12/02	1.0	First publication	New document	G Stretch
13/1/03	1.1	All		
27/2/03	1.2	Various		S Hunter
20/01/04	1.3	Various	Updates	E Cooper
21/01/04	1.4	Various	Updates	E Cooper
15/03/04	1.5	Various	Updates	E Cooper
14/04/04	1.6	Various	Updates	G Stretch, C Christie and Edwina Cooper
14/04/04	2.0		Copy for publication	Edwina Cooper
20/04/04	3.0		Copy for publication	Edwina Cooper
19/05/04	4.0	Renewals Various	Change in process Updates	Edwina Cooper
16/12/04	4.1	2.4 Fees	Fees Updated	Andrew Lamont
25/10/2005	5.0	Various	Added HealthGoldCert Info	Jo Hansen and Edwina Cooper
4/11/2005	5.1	3.1.2	Description for HealthGoldCert DC access clarified	Edwina Cooper
8/1/2007	6.0	2.4	Clarified prices	Edwina Cooper
11/1/2007	7.0			

1. INTRODUCTION

This section introduces HealthLink Limited's (hereafter referred to as HealthLink) Certification Practice Statement ('CPS') framework for it's role as a Health Certificate Authority. This CPS assumes that the reader is generally familiar with digital certificates, digital signatures and public key infrastructure (PKI) concepts.

The Ministry of Health has appointed HealthLink as a Certificate Authority to provide digital certificates to the New Zealand Health Sector as a consequence of Baycorp exiting the digital certificate business.

1.1 Overview

This CPS describes the practices that HealthLink adopts in its approach to Certification Authority (CA) operations. These include the issuing, revoking and renewal of a digital certificate under an X.509 certificate-based PKI.

It also forms the contract between HealthLink, Accident Compensation Corporation (ACC), Ministry of Health (MOH) subscriber, and third parties that rely on Health Certificates ('relying parties'). The contract between HealthLink and a subscriber, or between HealthLink and a relying party, consists of assent to this CPS.

All references to legislation and 'Acts' in this document are references to New Zealand legislation.

1.2 Identification

This document shall be cited as the 'Health Certificates CPS' or 'Health Certificates Certification Practice Statement'. When hyperlinked or cross-referenced, then the citation should be underlined.

This document is available in electronic form within HealthLink's repository located at:

www.healthlink.net and http://ca.healthlink.net/cp/

1.3 Applicability

This CPS is only applicable to the Digital Certificates Governing Board (DCGB), HealthLink, *subscribers* of HealthSecure digital certificates, *subscribers* of HealthGoldCert and *those who are relying on* HealthSecure digital certificates.

1.3.1 Certification Authorities (CA)

HealthLink is a Certification Authority for New Zealand, a trusted third party that issues and manages digital certificates, as permitted by this CPS.

1.3.2 Registration Authorities (RA)

A Registration Authority acts exclusively under the authority of ACC and the MOH (DCGB), and can validate and approve/reject certificate applications and request the revocation of certificates. All RA actions must conform to this CPS. There may be more than one RA approved.

1.3.3 Certificate Subscribers

Subscribers of HealthLink's certificates must be a holder of identification documents as specified in the appropriate registration process provided by the RA. For details of this process, please refer to the document located at the Ministry of Health – Health Intranet website:

http://www.hin.moh.govt.nz/docs/HealthSecure%20DC%20Information%20Sheet.pdf

1.4 Miscellaneous

1.4.1 Binding Effect

Except as otherwise provided, this CPS shall be binding on the successors, executors, heirs, representatives, administrators, and assignees of HealthLink. Neither this CPS nor the subscriber's certificate shall be assignable by the subscriber. Any such attempted assignment or delegation shall be null, void and of no effect.

1.4.2 Force Majeure

Neither party will be liable for any act, omission, or failure to fulfil its obligations under this CPS to the extent that such act, omission of failure arises from a cause reasonably beyond its control including acts of God, strikes, lockouts, riots, acts of war, epidemics, governmental action after the date of this CPS, fire, communication line failures, earthquakes or other disasters (called 'Force Majeure').

1.4.3 Severability

If any provision of this CPS, or its application, shall for any reason and to any extent, be invalid or unenforceable, the remainder of this CPS shall apply. It is expressly understood and agreed that each and every provision of this CPS that provides for any limitation, disclaimer, or exclusion of liability, warranties, or damages is intended by the parties to be severable and independent of any other provision and to be enforced as such.

1.4.4 Survival of Clauses

This agreement terminates on expiry or revocation of a digital certificate. This shall not affect the validity and enforceability of this clause 1.4 and the following:

Clause 2.2	Liability
Clause 2.3	Interpretation and Enforcement (including dispute resolution)
Clause 2.7	Privacy

1.4.5 Entire Agreement

This CPS and a formal service level agreement constitutes the entire agreement of the parties with respect to the issuance and use of digital certificates, and supersedes all previous oral and written agreements or understandings between the parties.

1.5 Contact Details

Comments, feedback and requests for further help and information are welcome. HealthLink makes every effort to respond promptly to enquiries, and in any case not later than seven working days after the day on which the request was received. Please address your correspondence to:

The Manager
Certificate Services
HealthLink Limited
PO Box 8273
Auckland
New Zealand

phone +64 (9) 638 6650
fax +64 (9) 638 6059
email casupport@heathlink.co.nz

2. GENERAL PROVISIONS

This section identifies obligations and issues that relate to HealthLink, its subscribers, and to relying parties.

2.1 Obligations

2.1.1 Certification Authority (CA) Obligations

HealthLink shall conform to this Certification Practice Statement (CPS) and use only systems and procedures that comply with this CPS when executing HealthLink's CA duties.

1. Publication of certificates may occur before subscribers receive them.

2. HealthLink is not responsible for the use of subscribers' private key and their use of certificates.

3. HealthLink is bound by its Privacy Policy located at http://www.healthink.net

4. Specific responsibilities of the CA when issuing digital certificates are described in more detail in the Service Level Agreement (SLA) between HealthLink and other associated parties.

2.1.2 Registration Authority (RA) Obligations

A Registration Authority acts exclusively under the authority of the DCGB, and is bound by all obligations applicable to the DCGB, unless otherwise specified in this CPS.

1. RA's can approve/reject certificate applications and revocations.

2. The DCGB has the right to request changes to the CPS.

3. The DCGB will arrange for the RA to be audited.

4. Specific responsibilities of the RA when issuing digital certificates are described in more detail in the Service Level Agreement (SLA) between HealthLink and other associated parties.

2.1.3 Subscriber Obligations

This CPS, as an agreement between a subscriber and HealthLink, will become effective on the date the subscriber submits a certificate application to the RA. By submitting a certificate application the subscriber is requesting that HealthLink issue them a digital certificate and is expressing their agreement to the terms and conditions of this CPS. The subscriber agrees to be bound, in advance, by any changes HealthLink makes to this CPS or any related policies.

The Duly Authorised Officer (DOA) is the individual who makes the application for a certificate on behalf of an organisation who subscribes for the certificate. The DOA remains the subscriber's single point of contact for HealthLink.

The subscriber is also bound by the NZ Health Information Privacy Code 1994 (available at http://www.privacy.org.nz/shealthf.html), which is an integral part of this CPS.

In this CPS the term 'subscriber' is defined, in Appendix II, as the organisation or organisation server named as the subject of the certificate. Where the subject is a server, the server will be controlled by an individual or by a designated person in an organisation. A server is considered to be a host computer, network device or message responder.

Before Health Certificates that include the name of an organisation can be issued, they must register with the RA, completing the appropriate RA registration forms (e.g. the registration

forms may differ depending on the RA, in accordance with registration procedures set out in section 3.

Industry Groups, organisations and organisation units, if registered, are also considered 'subscribers', even though they are not the subject of any certificate.

The subscriber confirms to HealthLink, and any parties relying on the certificate issued for the subscriber by HealthLink, that the subscriber holds the private key corresponding to the certificate's public key. The subscriber agrees that they will not, voluntarily or otherwise, allow a third party or similar body to hold the subscriber's private key. The subscriber will not pass ownership or control of their private key to a trustee or beneficiary in any case. If the subscriber becomes disabled or dies the subscriber's trustee or beneficiary must revoke the certificate.

The subscriber confirms that they will take all precautions to prevent their private key being compromised, lost, or disclosed. The subscriber agrees to notify HealthLink immediately if they believe this to be the case. The subscriber acknowledges that it is their responsibility, and not HealthLink's, to protect their private key.

The subscriber, where generating their own keys, agrees to protect their private key with a pass phrase as a minimum. The subscriber agrees that the pass phrase will not be a valid word or series of valid words. Loss, compromise or disclosure of the pass phrase is considered equivalent to loss, compromise or disclosure of the private key.

A subscriber agrees to be bound by all terms and conditions specified within this CPS.

In addition, registered organisations have the following obligations:

1. A subscriber may have a digital certificate issued with the approval of a registered organisation, and any organisation unit, of which they are a member. The issued certificate will identify the organisation, and organisation unit (if applicable). In addition, organisations can revoke the certificates of such subscribers.
2. The organisation and subscriber acknowledge that the use of the private key by the subscriber is authorised by the organisation.
3. Should a transfer of control of an organisation server's private key be required, HealthLink must be notified.
4. Organisations and organisation units are to provide and maintain with HealthLink lists of signatories authorised to approve certificate registration requests, and to suspend and revoke certificates in specified circumstances. Should updates be required to the list of authorised signatories then these updates must be registered in writing with HealthLink.
5. An organisation or organisation unit indemnifies HealthLink for any errors, omissions, or false statements in the member and server information provided to HealthLink. Organisations or organisation units will ensure that HealthLink is advised immediately of any changes to the information held by HealthLink.

Subscribers may also be a relying party (see 2.1.4).

2.1.4 Relying Party Obligations

A relying party accepts the following constraints and obligations in using Health Certificates.

This CPS becomes effective for a relying party when it:

1. checks a digital signature created with a private key corresponding to a public key contained within a current HealthLink-issued certificate, or
2. uses a current HealthLink-issued certificate for encrypted communication with the Subject named in the certificate, or
3. uses a current HealthLink-issued Certificate Revocation List, or

4. submits a search to HealthLink's Certificate Directory for a HealthLink-issued certificate or Certificate Revocation List.

A certificate is to be used solely for lawful purposes. By use of a HealthLink issued certificate the user accepts that HealthLink's assertions are limited to the following:

1. the subscriber holds the private key corresponding to the public key included in the certificate at the time of their application;
2. the subscriber's public and private key constitute a functioning key pair;
3. the subscriber has met and passed all specified criteria, including the validation process;
4. all information contained in the certificate has been validated, unless HealthLink incorporates a reference in the certificate stating otherwise.

A relying party is responsible for deciding whether to trust a digital certificate, including checking as to whether it had been suspended or revoked, at the time its matching private key had been used in any digital signature.

Users of HealthLink certificates should ensure that their use of the certificate is consistent with the certificate's Key Usage (found as part of the certificate itself – refer 4.4.2).

Relying parties, whether New Zealand residents or not, agree to be bound by the New Zealand Privacy Act 1993 in relation to the information obtained from HealthLink certificates and directory, whether or not the information pertains to New Zealand residents and whether or not they are organisations.

Relying parties acknowledge the limitations of HealthLink's liability as specified in clause 2.2.

2.1.5 Obligations regarding the Directory and Repository

HealthLink will promptly publish certificates, certificate revocations (CRLs), CPS amendments/updates and other information consistent with procedures in this CPS.

The Health Certificates repository, containing all authenticated HealthLink documents is located at http://www.healthlink.net

2.1.6 Binding Agreement

The agreement between the subscriber and HealthLink, i.e. this CPS, becomes effective when the subscriber submits a completed and signed Health Certificates registration form to the RA. The subscriber and HealthLink will then be bound by the terms and conditions of this CPS.

2.2 Liability

HealthLink disclaims liability for any implied warranties, including warranties of merchantability or fitness for purpose and for negligence or lack of reasonable care. HealthLink disclaims all liability for indirect consequential and punitive damages.

HealthLink carries out authentication procedures as described in this CPS and makes no assurances of the accuracy, authenticity, integrity or reliability of information contained in the certificates. Furthermore, no oral or written information or advice given by HealthLink or its employees or representatives shall create a warranty or in any way increase the scope of HealthLink's obligations under this CPS.

HealthLink shall not be in breach of its obligations as a result of any delay in or failure of performance on its part that arises out of any equipment failure or telecommunications breakdown beyond the reasonable control of HealthLink.

2.3 Interpretation and Enforcement

2.3.1 Governing Law

New Zealand law shall govern the interpretation, enforceability and validity of this CPS, irrespective of contract or other jurisdictions of law provisions. This choice of law is made to ensure uniform procedures and interpretation for all subscribers no matter where they reside or use their certificates. Each party irrevocably submits to the non-exclusive jurisdiction of the New Zealand courts.

The export of certain software, to certain sectors or states, may require the approval of government authorities. Subscribers shall conform to applicable export laws and regulations.

2.3.2 Dispute Resolution Procedures

Parties will, as soon as reasonably practicable, give the other notice of any dispute arising between them under this Agreement. If there is a dispute, then parties are to try to resolve the dispute within a maximum of three working days.

2.3.3 Referral to Mediator

If the parties do not resolve the dispute, after three working days, then the parties are to try to settle their dispute by mediation. Either party may initiate mediation by giving written notice to the other party. The mediation process shall not (unless otherwise agreed between the parties) extend beyond a period of 10 working days following the appointment of the mediator. The President of the New Zealand LEADR organisation (Lawyers Engaged in Alternative Dispute Resolutions), or its successors, will select a mediator if the parties cannot agree on a mediator within a maximum of three working days of the notice.

2.3.4 Continuity

If a dispute arises during the term of this Agreement the parties will continue to perform their obligations in this Agreement, which are not directly at issue in the dispute.

2.3.5 Arbitration (will take place in New Zealand)

New Zealand Arbitration Act 1996: Any dispute or difference arising between the parties under this Agreement which cannot be resolved pursuant to clause 2.3.2 within the periods referred to in clause 2.3.2 is to be referred to arbitration in accordance with this clause 2.3.3 and the New Zealand Arbitration Act 1996.

Arbitration: Arbitration will take place using either a single or three arbitrators. On a referral to arbitration the parties will appoint a single arbitrator if they can agree on one. If they cannot agree, the parties shall appoint one arbitrator each. These two arbitrators will then appoint a third arbitrator.

Sole Arbitrator: If either party fails to appoint an arbitrator within three working days after the other, having appointed its arbitrator, has served the defaulting party with a notice to make the appointment, the party who appointed an arbitrator shall be entitled to appoint the arbitrator as sole arbitrator in the dispute.

Qualifications

Any arbitrator:

a. shall be suitably qualified to act as an arbitrator in matters relevant to the dispute;
b. shall be as independent from either party as reasonably possible;
c. shall not be an ex-employee of either party; and
d. shall not have entered into significant contracts or arrangements with either party.

Decision: Any arbitration will be by majority decision of the arbitrators.

Binding: The award (including the right to determine damages) will be final and binding on both parties.

Continuity: Pending resolution of any dispute by arbitration, the parties will continue to perform their obligations in this Agreement that are not directly at issue in the dispute.

2.4 Fees

2.4.1 Certificate Issuance Fees

The subscriber on issuance or renewal of certificates pays the fees, except where another such as the MOH or ACC agrees to pay. HealthLink reserves the right charge for additional services not covered by the base fee. The following table states the fees charged to subscribers. These fees may vary for volume purchases.

These fees are valid from the 1st November 2005

Certificate type	Initial Fee NZ$ (excl GST)	Validity Period	Renewal Fee NZ$ (excl GST)
Client	100.00	12 months	80.00
Server (first)	400.00	12 months	350.00
Server (second and further)	200.00	12 months	180.00
USB Dongle and Software only*	110.00	(refer to standard certificate validity period)	No charge
Load New Certificate on USB Dongle	No Cost	(refer to standard certificate validity period)	25.00
Load Existing Certificate on USB Dongle	25.00	(refer to standard certificate validity period)	25.00

* Excludes cost of certificate

Additional Services

Urgent certificate issue $250 (same day between 9:00am and 3:00pm)

Certificate renewals are annual.

For organisations, invoices are mailed on the last working day of each month. Payment is required within 14 days of receipt of the invoice or the certificate/s may be revoked.

2.4.2 Goods and Services Tax

New Zealand Goods and Services Tax, where applicable, is payable at the prevailing rate on all subscriptions and renewals.

2.4.3 Fees for Other Services

HealthLink reserves the right to charge for services not otherwise specified in this CPS. Such charges will be advised to the customer prior to the actions requested of HealthLink being undertaken.

2.4.4 Refund Policy

There are no refunds following revocations of certificates, nor for failure to utilise the service once it has been subscribed, unless HealthLink ceases to act as a CA.

2.5 Publication and Repository

2.5.1 Publication of CA Information

HealthLink shall maintain records, either computer or paper based, relating to each certificate issuance or revocation. These records shall contain relevant information relating to the certificate subscriber's identity, the identity of the person requesting the revocation of a certificate and other information represented in the certificate.

2.5.2 Frequency of Publication

HealthLink will publish all certificates on their issuance.

Certificate Revocation Lists ('CRLs') will be updated daily on the actioning of a certificate suspension or revocation request.

2.5.3 Access Controls

If HealthLink determines that there is misuse of available information in contravention with this CPS, including HealthLink's Privacy Policy and the NZ Health Information Privacy Code 1994, then HealthLink will take appropriate action.

2.6 Privacy

HealthLink takes the privacy of its subscribers very seriously. We ensure the confidentiality and security of the information provided to HealthLink. HealthLink's Privacy Policy and the NZ Health Information Privacy Code 1994 are an integral part of this CPS and can be located at http://www.healthlink.net

The Privacy Policy covers issues such as:

- what information is gathered
- how this information is used and stored
- who the information will be shared with
- opt-out policy
- change/modify/update information

3. CERTIFICATE MANAGEMENT

This section details the procedures for certificate application, issuance, renewal, revocation and expiration.

3.1 Certificate Types

This CPS anticipates three methods of issue for certificates:

- HealthSecure Certificates - Web-issue, Floppy or CD delivery
- HealthGoldCert Cerificates – Dongle Delivery only
- SecureCert Certificates – Web-issue, Floppy or CD delivery

HealthSecure Certificates and SecureCerts Certificates are issued under different registration authorities.

All Health Certificates are used for the transfer of clinical information and electronic claims.

3.1.1 HealthSecure Certificates

HealthSecure Certificates are for the New Zealand Health & Disability Sector and are issued by the CA under the instruction from RA's accredited by the DCGB. HealthSecure certificates are used to access online Health Sector applications.

3.1.2 HealthGoldCert Certificates

HealthGoldCert Certificates are for the New Zealand Health & Disability Sector and are issued by the CA under the instruction from RA's accredited by the DCGB. HealthGoldCert certificates are used to access online Health Sector applications. In addition, HealthGoldCert certificates are also used to submit Special Authority Forms to HealthPac using a browser.

3.1.3 SecureCert Certificates

Some New Zealand non-health organisations will be issued with SecureCerts.

3.1.4 Client and Server Certificates for HealthSecure and SecureCert Only

HealthSecure and SecureCert digital certificates can be issued in a client or a server version. A server certificate is used where a private key is in use on one host computer, network device, message responder or software publisher. The computer is identified by an Internet Address i.e. server name - including a registered domain name or IP address (the applicant or their organisation must be the owner of the registered domain name). The person who owns or is currently responsible for the private key must be identified to HealthLink.

3.2 Key Pair Generation

Subscribers can either securely generate their own private-public key pair or use HealthLink's securely generated key pair.

3.2.1 Subscriber Key Generation

This service is only available to subscribers who subscribe for HealthLink's services or where the RA has specified the need on an application form eg for a selected server certificates.

3.2.2 HealthLink Key Generation

Subscribers who do not meet the requirements of 3.2.1 are offered digital certificates with key pairs generated by HealthLink unless subscriber key generation is specifically requested e.g. for selected HealthSecure server certificates (refer section 3.2.1).

3.3 Certificate Issuance

When the RA is satisfied that all application and validation procedures have been completed successfully, it shall approve, and advise HealthLink to issue a certificate. The issuance of a Health Certificate digital certificate indicates a complete and final approval of the certificate application by HealthLink.

The RA reserves the right to decline any application and the RA accepts no liability for declining the application.

HealthLink shall have no continuing duty to monitor the correctness of the information in a certificate. Subscribers are responsible for advising the RA of any changes to the information contained in the certificate.

3.4 Certificate Validity Period

Health Certificates remain valid for 12 months from date and time of issue, unless revoked. The operational period is contained in the certificate.

3.5 Names on Certificates

HealthLink uses an X.500-based 'Distinguished Name' to identify the name of a subscriber (which might be a host computer, network device or message responder).

The Distinguished Name attributes on Health Certificates that are used to identify the subscriber are:

Country	the Subscriber's two character ISO Country Code. In the case of a server this must be the country location where the server is hosted
Location	the Subscriber's City (or town/rural region if required to ensure a unique Distinguished Name). If the certificate includes the name of the

	Subscriber's Organisation, then the *Country, State* and *Location* components would describe the Subscriber's place of work
Common Name	**Organisation** The subscriber's HealthLink user name. Industry Groups registered will appear in the organisation field with the letters [IG] after them. Any members of that IG will appear in the first Org Unit field under the IG name. **Individual** The name of the individual subscriber as stipulated on their registration form - email address, this should in the case of an individual be the email address confirmed in their registration, and in the case of a server, it is the address that the holder stipulates on the registration form. **Server** The Common Name is the server's currently valid Internet Address, but for a Message Responder will also include the words 'Message Responder' and for software publishing must include the [name] followed by the phrase software publishing. A domain name or IP address must be registered in the name of the applicant or applicant's organisation. The person who owns or is currently responsible for the private key must be identified to HealthLink
Email Address	The principal email address used by the individual DOA.
Organisation	The Subscriber's Organisation (which will identify any limitations of liability such as Ltd, Plc, Pty, etc if applicable).

Example 1:

Country: NZ
State: -
Location: Wellington
Common Name: Bob Smith
Email Address: bob.smith@wfd.co.nz
Organisation: Bob Smith

3.6 Key Escrow

HealthLink does not provide a key escrow service currently.

3.7 Certificate Revocation

3.7.1 Circumstances for Revocation

A certificate must be revoked if there has been a loss, theft, unauthorised disclosure or compromise of the subscriber's private key. The subscriber shall notify the RA immediately if they believe this to be the case. The RA is the primary authoriser of any revocation request.

A certificate may also be revoked if HealthLink believes:

- a subscriber has breached an obligation under this CPS;
- another subscriber's information is either threatened or compromised;
- should the common name in a server certificate not correctly describe the host computer, network device or message responder that the certificate and/or matching private key is being used upon;
- a material fact represented in the subscriber's certificate is believed to be false;
- a certificate was not issued in accordance with the procedures in this CPS;

- where an organisation invoice has not been paid;
- that, in an official assignee or liquidators opinion, an organisation subscriber is no longer solvent;
- HealthLink's private key, or trustworthy system, was compromised in a manner materially affecting the certificate's trustworthiness.

When a subscriber's certificate is revoked, the agreement between the subscriber and HealthLink (i.e. this CPS) ends. HealthLink accepts no liability for acting on a revocation request.

3.7.2 Who can Request Revocation

HealthLink will revoke a certificate upon the subscriber's or RA's request once it has confirmed that the person requesting the revocation is in fact the subscriber or the RA.

As well as the person named in the certificate being able to revoke their certificate, an authorised signatory of an organisation or organisation unit may also revoke such certificates.

3.7.3 Procedure for Revocation Request

A request from the subscriber or an organisation or organisation unit authorised signatory in the form of a digitally signed email, signed letter or fax, letter or voice message is pre-requisite to HealthLink revoking a certificate. The authentication will be by means of the subscriber confirming certain details that were supplied on the initial registration form.

HealthLink will make every effort to notify the subscriber, in the form of email, letter, fax, post or voice message, confirming the certificate has been revoked.

3.7.4 Private Keys corresponding to Revoked Certificates

Where the subscriber still controls the private key corresponding to a revoked certificate, they shall continue to safeguard the private key until the expiry date specified in the revoked certificate.

3.7.5 Checking HealthLink Certificate Revocation List (CRL)

All parties who use and rely on HealthLink certificates must determine whether they can be trusted for their own purposes. To assist relying parties in deciding whether to trust certificates, they may retrieve HealthLink's CRLs from at http://ca.healthlink.net/crl/

3.7.6 CRL Issuance Frequency

When a certificate has been revoked HealthLink must publish the certificate's serial number and the date and time of processing of the request by HealthLink in its directory in the form of a Certificate Revocation List (CRL).

Certificate Revocation Lists (CRLs) will be published on the actioning of a certificate revocation request or daily (which ever is the sooner).

3.8 Certificate Renewal

3.8.1 Subscriber Using HealthLink.net

Subscribers using HealthLink.net software will be automatically renewed.

3.8.2 Subscribers Using HealthLink Generated Key Pair

The Registration Authority will contact subscribers of an impending expiry of their certificate within two months of the expiry whenever possible. This allows the subscriber the opportunity to renew their certificate. Contact will be by phone call, email or by letter depending on the subscriber's ability to receive email. The Registration Authority will endeavour to follow up where no response has been received, but it is also the responsibility of the subscriber to be

aware of a certificate expiry date. The Registration Authority cannot be held responsible if subscribers don't proactively monitor their certificate expiry date and respond to the Registration Authority in a timely manner, and, as a result, a certificate expires. If a certificate expires, subscribers will have to apply for a new certificate as per the initial application process (see 3.2).

Subscribers confirming renewal are required to:

1. Confirm they wish to renew their certificate when they are contacted by the Registration Authority.
2. Advise of any changes to the details on their current certificate, or other details held by the RA.

The Certification Authority will be notified by the Registration Authority of those certificates requiring renewal and renewed certificates will be issued directly to the existing certificate holder before the date of expiry.

3.9 CA Termination

Should HealthLink cease to act as a Certification Authority it must:

1. Provide to the subscriber of each unrevoked or unexpired certificate 6 months notice of their intention to cease acting as a CA.
2. The RA may request that all certificates be revoked
3. Make a reasonable effort to ensure that discontinuing its certification services will cause minimal disruption to its subscribers and to anticipated relying parties;
4. Make reasonable arrangements for preserving its records;
5. Continue providing support until the date of cessation.

4. CERTIFICATE AND CRL PROFILES

This section describes the contents, profiles and policies of Health Certificates digital certificates.

Profiles define the structure of certificates and Certificate Revocation Lists (CRLs). Within the HealthLink documentation, certificate profiles are commonly referred to as policies.

4.1 Issuing Certificate Authorities

The Health Certificates Certificate Authority is a self signed Certificate Authority. The Health Certificates Certificate Authority issues CRLs.

4.2 Certificate Type

A digital certificate contains a subscriber's public key, information describing the subscriber, and the digital signature of a Certificate Authority. Certificates issued by HealthLink comply with the ISO X.509v3 standard. This standard also allows appropriately formatted extensions to be included in certificates.

4.3 Certificate Renewal

Delivery Mechanism for New, Renewed and Updated Certificates:

Subscriber key pair generated	Certificates are automatically renewed by HealthLink's communication software, HealthLink.net.
HealthLink key generated	Certificates either web-issued to the subscriber or couriered, with or without key pairs, depending on the initial requirements specified when the certificate was first generated (refer section 3.2).
Certificate Lifetime	370 days

4.4 Other Standard Information

4.4.1 Algorithms

Health Certificates are issued only for RSA public keys with:

- a key strength of 1024 bits or greater.
- the SHA-1 hashing algorithm.

4.4.2 Key Pair Usage

All Health Certificates are issued either for signing and/or encryption. All Health Certificates are also enabled for software signing. (The specified usages for the key pair may be extended in the future).

key usage extension	will have the following capabilities set: digital signature key encipherment

4.4.3 Further Detail

For more detail on the contents of HealthSecure, SecureCert or HealthLink certificates, please either contact HealthLink and/or retrieve the HealthLink NZHealthCA root and HealthSecure/SecureCert sub CA certificates from the HealthLink directory: http://ca.healthlink.net/ and analyse it using commercial or freeware utility software.

4.4.4 Certificate Revocation Lists Profile

The CRLs are signed by the issuing Certificate Authority, and list the serial number and HealthLink revocation processing date and time for each currently revoked certificate.

These revoked certificates are found in HealthLink's directory located at the following distribution point:

http://ca.healthlink.net/crl/

5. ADMINISTRATION OF CPS CHANGES

5.1 Specification Change Procedures

HealthLink reserves the right to update and publish this CPS and any associated policies, as long as the end result doesn't reduce service levels, security levels or increase customer risk in any way. HealthLink will identify and publish the changes in the HealthLink repository at:

http://www.healthlink.net and the certificate policies URL http://ca.healthlink.net/cp/

5.2 CPS Approval Procedures

HealthLink will follow a change control procedure when amending this CPS.

6. APPENDIX II - GLOSSARY

Term	Definition
Applicant	Person who submits an application to HealthLink requesting a digital certificate or other HealthLink service.
Archive	To keep records and any associated material to meet security, backup, auditing or procedural requirements.
Authentication	Verifies the sender/receiver.
Authorised signatory	The initial signatory of an industry group/organisation/organisation unit registration form delegates to a list of authorised signatories the ability to approve certificate requests and suspend/revoke certificates, in accordance with the rights and obligations of that entity.
Certification Authority	A trusted third party that issue digital certificates.
Certificate	An electronic document formatted in compliance with the ISO X.509 version 3 standard, that identifies HealthLink, names or identifies its subscriber, contains the subscriber's public key, identifies its operational period, and is digitally signed by HealthLink.
Certification Practice Statement	A declaration by HealthLink of the practices that HealthLink employs in support and issuance of a certificate. It also forms part of the contract between HealthLink and the subscriber.
Certificate Revocation List (CRL)	Contains a list of certificates that have been suspended or revoked.
Confidentiality	Ensures the information exchanged between the sender/receiver stays private.
Cryptography	Cryptography is the science of disguising information through encryption (scrambling) and restoring it to its original form through decryption.
Digital certificates	Refer to certificate definition above.
Digital signature	Technically a digital signature is a hash total of a document. The hash total is then encrypted by a public key algorithm in conjunction with the signer's private key.
Duly Authorised Officer	Individual authorised by the organisation to apply for and assume the responsibilities of complying with the CPC
Encryption	Encryption is a way of scrambling information so that the information cannot be understood by anyone other than the intended recipient.
Hash algorithm	An algorithm that creates a digital representation or fingerprint in the form of a hash result.
Hash result or message digest	The output produced by a hash algorithm upon processing a message.
HealthSecure Certificate	Health Certificate digital certificate approved by a registration authority under the authorisation of the DCGB. Certificates will typically be issued within New Zealand health sector organisations only.
SecureCert	Health Certificate digital certificate used by approved by non-government registration authorities. Certificates will typically be issued to Australian health sector organisations.
HealthGoldCert Certificates	Health Certificate digital certificate approved by a registration authority under the approval of the DCGB. Certificates will typically be used within the New Zealand health sector organisations only.
Industry Group	Any organisation group within the health sector such as an Independent Practitioner Associations (IPA),
ICANZ	Institute of Chartered Accountants of New Zealand

Integrity	Confirms that information sent is intact and was not altered in transit.
Key Escrow	Authorised persons can retain a subscriber's key pair for later reuse. This always includes the subscriber and may include authorised signatories of their organisation. Either HealthLink or an independent lawyer in public practice depending on which option is requested by the subscriber encrypts escrowed keys and identifying information. All encrypted files are securely archived by HealthLink.
Key Pair Generation	Generation of private-public key pair. The subscriber can elect to generate the keys or have HealthLink generate the key pair.
Message	A digital representation of information.
Non-repudiation	Provides proof that a transaction took place.
Operational period	The operational period of a certificate begins on the date and time it is issued by HealthLink and ends on the date and time it expires, unless earlier revoked or suspended.
Promptly	HealthLink must act with appropriate dispatch.
Public/private keys	In a public key cryptography system two keys, a public and a private key, are required to exchange information securely.
Digital Certificates Governing Board (DCGB)	Digital Certificates Governing Board (DCGB) accredits Registration Authorities to approve and revoke digital certificates for the CA.
Relying Party	A relying party is responsible for deciding whether to trust and rely on a digital certificate.
Repository	A trustworthy system for HealthLink operational information.
Revocation	To permanently end the operational period of a certificate.
Subscriber	The person or server named as the subject of the certificate. Where the subject is a server, the server will be controlled by an individual or by a designated person in an organisation. A server is considered to be a host computer, network device, message responder or software publisher. Industry Groups, organisations and organisation units, if registered, are also considered subscribers.
Suspension	To temporarily suspend the operational period of a certificate.
Token	A portable device with a built-in microprocessor and memory used for identification and/or holding private-public key pairs and digital certificates. A token holding private-public key pairs is usually referred to as a cryptographic token. When inserted into a reader, a cryptographic token encrypts and decrypts information passed to it. The most common form of token is an ISO 7816 compliant smartcard.
Time-stamp	A notation that gives the date and time of an action and the identity of the person/server that verified the notation.
Unlisted service	As a subscriber of a HealthLink digital certificate you may elect to have your certificate 'unlisted' i.e. not listed in HealthLink's public directory. This has to be requested at time of registration.
Working day	New Zealand working days are the weekdays, Monday to Friday, but excluding: the first two weekdays of January February 6th Good Friday and Easter Monday April 25th 1st Monday in June 4th Monday in October the first two weekdays after December 24th