

Connected Health User to Network Interface Specifications

HISO 10037.3:2015

To be used in conjunction with:

HISO 10037.1 Connected Health Architectural Framework

HISO 10037.2 Connected Health Network to Network Interface Specifications

### Copyright

This work is licensed under the Creative Commons Attribution 4.0 International licence. In essence, you are free to: share ie, copy and redistribute the material in any medium or format; adapt ie, remix, transform and build upon the material. You must give appropriate credit, provide a link to the licence and indicate if changes were made.

### Keeping standards up-to-date

HISO standards are regularly updated to reflect advances in health information science and technology. Always be sure to use the latest edition of these living documents. We welcome your ideas for improving this standard and will correct any errors you report. Contact us at standards@health.govt.nz or write to Health Information Standards, Ministry of Health, PO Box 5013, Wellington 6145. See the HISO website for information about our standards development processes.

First published September 2010

Updated March 2015
by the Ministry of Health

PO Box 5013, Wellington, New Zealand

978-0-478-44497-1 (online)

This document is available on the HISO website:

<http://ithealthboard.health.nz/standards>

Updates

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Pagenumber | Sectionnumber | Changes |
| September 2010 |  |  | Published |
| October 2011 | 3 | 2 | ‘User’ removed from the minimum requirements for UNI-0 and UNI-3 |
| October 2011 | 3 | 2 | ‘High Speed’ deleted from UNI-4 |
| October 2011 | 7 | 2.2 | ‘User’ removed from 2nd sentence |
| October 2011 | 7 | 2.2 | Note 10 added |
| October 2011 | 9 | 2.4 | ‘User’ removed from 2nd sentence |
| October 2011 | 9 | 2.4 | Note 8 added |
| October 2011 | 12 | 2.6 | ‘High Speed’ removed from 1st sentence |
| October 2011 | 12 | 2.6 | Minimum Speed Range attributes changed to: >512Kbits/s download >512Kbit/s upload |
| October 2011 |  |  | Preferred Speed Range attributes changed to: >5Mbits/s download >5Mbit/s upload |
| December 2011 |  |  | Change status from ‘Interim’ Standard to ‘Full’ Standard  |
| April 2014 | Document Contributors |  | Removal of historic organisation to support legal requirement |
| September 2014 |  | 2, 2.6 | Changes to reflect the UFB Bitstream 2 service |
| July 2016 |  |  | Move to Creative Commons Attribution 4.0 International licence |

Table of Contents

[Copyright i](#_Toc412215044)

[Keeping standards up-to-date i](#_Toc412215045)

[1 Introduction 1](#_Toc412215046)

[1.1 Background 1](#_Toc412215047)

[1.2 Document purpose 1](#_Toc412215048)

[1.3 Target Audience 1](#_Toc412215049)

[2 User to Network Interface Specifications 3](#_Toc412215050)

[2.1 Interface Considerations 5](#_Toc412215051)

[2.2 UNI-0 8](#_Toc412215052)

[2.3 UNI-1 9](#_Toc412215053)

[2.4 UNI-2 10](#_Toc412215054)

[2.5 UNI-3 11](#_Toc412215055)

[2.6 UNI-4 13](#_Toc412215056)

[2.7 UNI-4a 15](#_Toc412215057)

[2.8 UNI-5 16](#_Toc412215058)

[Appendix 1: Use Cases 18](#_Toc412215059)

[Appendix 2: Service Performance Targets 24](#_Toc412215060)

[Appendix 3: Glossary of Terms 27](#_Toc412215061)

Table of Figures

[Figure 1: Typical CH network of networks topology 5](#_Toc412215062)

[Figure 2: The CH User to Network Interface and end to end performance 7](#_Toc412215063)

[Figure 3: Single user accessing web based services 19](#_Toc412215064)

[Figure 4: Single mobile user accessing web based services 20](#_Toc412215065)

[Figure 5: Multiple user site accessing CH services 21](#_Toc412215066)

[Figure 6: Large multiple user site accessing CH services 22](#_Toc412215067)

[Figure 7: DHB using MAN 23](#_Toc412215068)

Table of Tables

[Table 1: UNI Definitions 3](#_Toc412215069)

[Table 2: UNI-0 Specifications 8](#_Toc412215070)

[Table 3: UNI-1 Specifications 9](#_Toc412215071)

[Table 4: UNI-2 Specifications 10](#_Toc412215072)

[Table 5: UNI-3 Specifications 11](#_Toc412215073)

[Table 6: UNI-4 Specifications 13](#_Toc412215074)

[Table 7: UNI-4a Specifications 15](#_Toc412215075)

[Table 8: UNI-5 Specifications 16](#_Toc412215076)

[Table 9: Possible Use Cases 18](#_Toc412215077)

[Table 10: Service Performance Targets 24](#_Toc412215078)

Document Contributors

The following contributed to the drafting of this document:

|  |  |
| --- | --- |
| Name | Organisation |
| Mikel Huth | Ministry of Health |
| Murray Milner | Milner Consulting Ltd |
| Steve Martin | Ministry of Health |
| Steve Miller | Formerly Gen-i |
| Health IT Cluster Standards Working Group | A group from the NZ health service provider community, including Datacraft, Smartlinx3, Kordia, Gen-i, Telecom, FX Networks, Microsoft, HealthLink, VividSolutions. |
| Grant Ardern | Healthshare Ltd |

The terms ‘normative’ and ‘informative’ are used in Standards to define the application of an appendix. A ‘normative’ appendix is an integral part of a Standard, whereas an ‘informative’ appendix is only for information and guidance and does not form part of the mandatory requirements of the Standard.

Related Documents

**HISO Standards**

10029 Health Information Security Framework

10037.1 Connected Health Architectural Framework

10037.2 Connected Health Network to Network Interface Specification

**New Zealand Legislation**

The following Act of Parliament has specific relevance to this standard. Readers should be aware of the need to consider other Acts and Regulations as may be appropriate to their own implementation or use of this standard.

Telecommunications Act 2006

**New Zealand Standards**

SNZ HB 8169:2002 Health Network Code of Practice

**Other Standards**

Health Level Seven Inc., HL7 Standard version 2.4 - An Application Protocol For Electronic Data Exchange in Healthcare Environments

**Other Connected Health Documents**

Connected Health: An Overview

Connected Health Principles

Connected Health Operational Policy for Telecommunications Service Providers

Service Management Guide

**Other Publications/Websites**

Commerce Commission 13 December 2007 (incorporates clarifications up to 8 July 2010). *Standard Terms Determination for Telecom’s Unbundled Bitstream Access Service* URL: <http://www.comcom.govt.nz/assets/Telecommunications/STD/UBA/UBA-STD-as-at-8-July-2010/UBA-STD-General-Terms-8-July-2010.pdf> Accessed 17 August 2010.

International Telecommunication Union – Telecommunication Standardisation Sector 2006. Recommendation Y.1541 *Network performance objectives for IP-based services* URL: <http://www.itu.int/rec/T-REC-Y.1541-200602-I> Accessed 17 August 2010.

InternetNZ, NZ Marketing Association, Telecommunications Carriers’ Forum 2007. *Internet Service Provider Spam Code of Practice* URL: <http://www.tcf.org.nz/library/45a3afab-3e1d-4d43-b8d4-b6d73cfbd201.cmr> Accessed 17 August 2010.

IT Health Board 2010. *National Health IT Plan* URL: <http://www.ithealthboard.health.nz/our-plan> Accessed 17 August 2010.

MIT Communications Futures Program 2006. *Interprovider Quality of Service whitepaper* version 1.1URL: <http://cfp.mit.edu/docs/interprovider-qos-nov2006.pdf> Accessed 17 August 2010.

Telecom Wholesale 2010. *Product Profile: High Speed Network Service* URL: [http://www.telecomwholesale.co.nz/f73,1460/1460\_25751\_HSNS\_3-0.pdf](http://www.telecomwholesale.co.nz/f73%2C1460/1460_25751_HSNS_3-0.pdf) Accessed 17 August 2010.

Telecom Wholesale 2008. *Product Profile: Unbundled Network Service* URL: [http://www.telecomwholesale.co.nz/f77,5705/5705\_22570\_UNS\_A3\_2-0.pdf](http://www.telecomwholesale.co.nz/f77%2C5705/5705_22570_UNS_A3_2-0.pdf) Accessed 17 August 2010.

Telecommunication Carriers’ Forum 2009. *Guidelines for Undertaking Community Engagement for Wireless Telecommunications Facilities* URL: <http://www.tcf.org.nz/library/2f5239c7-446e-4171-8ff3-387d01b1f85a.cmr> Accessed 17 August 2010.

Telecommunication Carriers’ Forum 2007. *Co-siting Code* URL: <http://www.tcf.org.nz/library/c4efc274-8252-4482-9e2c-0c679dc8f899.cmr> Accessed 17 August 2010.

Telecommunication Carriers’ Forum 2008. *Customer Complaints Code* URL: <http://www.tcf.org.nz/library/b6808eed-f840-4d29-bb52-9693e610eaff.cmr> Accessed 17 August 2010.

Telecommunication Carriers’ Forum 2006. *Code for the Transfer of Non Regulated Telecommunications Services* URL: <http://www.tcf.org.nz/library/c96a3a73-ebb3-4ec3-a48b-68afe0d17eb7.cmr>

Telecommunication Carriers’ Forum 2006. *Code for the Transfer of Telecommunications Services* URL: <http://www.tcf.org.nz/library/d72c3ecf-8f4e-4871-9deb-f1b9e566ac3f.cmr> Accessed 17 August 2010.

Telecommunication Carriers’ Forum 2008. *Disconnection Code* URL: <http://www.tcf.org.nz/library/2c5f7197-fca9-4763-a7dc-e4464755f978.cmr> Accessed 17 August 2010.

Telecommunication Carriers’ Forum 2009. *Emergency Calling Code* URL: <http://www.tcf.org.nz/library/a4a3ad46-2e90-42f3-8733-a66f7bd1065c.cmr> Accessed 17 August 2010.

Telecommunication Carriers’ Forum 2009. *Guidelines for Interception Capability* URL: <http://www.tcf.org.nz/library/cc58568d-2100-46a8-9cfc-982c3d0679d8.cmr> Accessed 17 August 2010.

Telecommunication Carriers’ Forum 2008. *Code of Practice for Provision of Content via Mobile Phones* URL: <http://www.tcf.org.nz/library/90423ff2-0e52-4eeb-985e-0b00e9d2a854.cmr> Accessed 17 August 2010.

Telecommunication Carriers’ Forum 2008. *Mobile Premium Messaging Services Code* URL: <http://www.tcf.org.nz/library/163a6fd5-abd8-4774-9497-391afa6c1c9c.cmr> Accessed 17 August 2010.

Telecommunication Carriers’ Forum 2010. *Code for Residential and SOHO Premises Wiring* URL: <http://www.tcf.org.nz/library/e72d1374-8040-4022-ba79-428d56eb4a9b.cmr> Accessed 17 August 2010.

Telecommunication Carriers’ Forum 2008. *Code for the Control of Unauthorised Use of Mobile Phones in Prisons* URL: <http://www.tcf.org.nz/library/e7b0100d-e056-4ef7-9d12-c18e5b4fb103.cmr> Accessed 17 August 2010.

# Introduction

## Background

Currently health information is accessed from and transferred over many different types of computers, telecommunications networks and information systems in the New Zealand health sector. Often these have been implemented in isolation of one another making it difficult and costly to share information between providers and systems in a secure way.

In a person-centred health system the ability to connect services, applications and systems is essential for allowing patients to be cared for by the right clinician, at the right time and place, providing access to their records electronically with the confidence that information is kept secure at all stages.

The Connected Health (CH) programme is a key step in achieving this aim. Its purpose is to establish the secure environment needed for the safe sharing of health information between all the participating health providers. To achieve this, the programme is delivering the following foundation components:

* a common connectivity framework
* connectivity standards
* core network components
	+ three managed points of interconnection
	+ a uniform addressing scheme
* an accreditation and certification process for telecommunication service providers
* governance and management oversight.

To date, the connectivity standards delivered include:

* HISO 10037.1 Connected Health Architectural Framework
* HISO 10037.2 Network to Network Interface Specifications
* HISO 10037.3:2015 User to Network Interface Specifications (this document)

Further specifications and standards will be developed over time.

Further background information about CH, product certification and supplier accreditation can be found in Connected Health: An Overview.

## Document purpose

The CH Architectural Framework describes the role of and the need for

User to Network Interfaces (UNIs).

This document details the technical specifications for the UNI class 0 to 5 interfaces and defines a set of minimum and preferred characteristics for each. It forms the baseline requirements for the definition of a set of standardised CH certified access products.

## Target Audience

This technical specification is mainly intended for organisations looking to provide certified telecommunications services in the CH environment It is also intended for CH management to inform policy and procedure development around accreditation of Telecommunication Service Provider (TSP) organisations, and certification of products and solutions.

# User to Network Interface Specifications

As outlined in the HISO 10037.1 Connected Health Architectural Framework, the UNI classes are defined below. The technical specifications for each UNI are defined in sections 2.2 to 2.8 of this document.

Table : UNI Definitions

|  |  |  |
| --- | --- | --- |
| Class | Description | Minimum Requirements |
| UNI-0 | Public UNI–Basic Public Internet access | A basic public Internet access specification where connection will be established via authenticated Virtual Private Networks (VPNs) terminating at a CH NNI-2. A single Personal Computer (PC) (not on a Local Area Network (LAN)) connecting to: * a browser based application e.g. a form based service or;
* a non-browser based CH application e.g. Health Level 7 (HL7) messaging and legacy applications.
 |
| UNI-1 | Public UNI–Public Internet | A basic public Internet access specification where connection will be established via authenticated VPNs terminating at a CH NNI-2. A single PC user or a small LAN connecting to:* a browser based application e.g. a form based service or a web based email or;
* a non-browser based CH application e.g. HL7 messaging and legacy applications.
 |
| UNI-2 | Public UNI–Mobile Internet Access | For mobile access to CH using a public Internet service over a mobile telephone connection specification where connection will be established via authenticated VPNs terminating at a CH NNI-2 A single mobile device connecting to a browser based application e.g. a form based service or a web based email. |
| UNI-3 | Public/Private UNI– Public Internet with fixed VPN to CH private Internet Protocol (IP) | A high speed symmetrical public Internet access specification where connection will be established via authenticated VPNs terminating at a CH NNI-2.A small to medium sized LAN connecting to:* a browser based application e.g. a form based service or a web based email or;
* a non-browser based CH application e.g. HL7 messaging and legacy applications.
 |
| UNI-4 | Private UNI–private IP | A private network access with a single end-point Internet Protocol (IP) address specification directly connecting to the CH private IP network via a fixed authenticated Virtual Local Area Network (VLAN) to an NNI.A large LAN environment (with possible sub-networks) with multiple users accessing both browser based and non-browser based applications and services e.g.: * a form based service or web based email; or
* non-browser based CH applications, e.g. HL7 messaging and legacy applications.
 |
| UNI-4a | Private UNI–private IP | A private network access method based on the UFB Bitstream 2 service with a single end-point IP address directly connecting to the CH private IP network via a fixed authenticated VLAN to an NNI.A small LAN environment (with possible sub-networks) with multiple users accessing both browser based and non-browser based applications and services, such as the examples listed for UNI-4. |
| UNI-5 | Private UNI–private IP | A high speed private network access multiple end-point IP address specification directly connecting to the CH private IP network via a fixed authenticated VLAN to an NNI. A large LAN environment (with possible sub-networks) with multiple users accessing both browser based and non-browser based applications and services e.g.:* a form based service or web based email; or
* non-browser based CH applications e.g. HL7 messaging and legacy applications.
 |

## Interface Considerations

A number of considerations should be understood as part of the implementation of these specifications:

* the use of Government Logon Service (GLS) as a requirement for authentication needs to be evaluated to determine feasibility and practicality. This will be facilitated through the CH management function.
* during the transition process, authentication at a network layer may not seamlessly integrate with authentication at an application layer. Therefore a user may be required to provide credentials twice to authenticate within the same application.
* split-Domain Name System (DNS) functionality is preferred in every UNI device but Telecommunications Service Provider (TSP) recursive DNS functionality will also be accepted.

Figure 1 shows the typical CH network of networks topology, with UNI to UNI service achieved via multiple IP networks interconnected by multiple NNI-1 links.

Figure : Typical CH network of networks topology



Figure 1 illustrates four separate networks:

* The Internet
* CH as a ‘network of networks’
* TSP-1’s CH IP Network
* TSP-2’s CH IP Network.

Each network has a number of certified CH UNIs connected to it. The Internet supports UNIs 0-3. TSP-1 is supporting UNIs 4 and 5 and TSP-2 is supporting UNIs 4 and 5. The UNIs can be physically located anywhere within New Zealand. One or more interconnection links provide connectivity between each network domain. The interconnection links are defined as NNI-1 and NNI-2 (refer to HISO 10037.2 Connected Health Network to Network Interface Specifications).

UNIs consist of a standard Service Provider UNI plus a piece of Customer Located Network Equipment (CLNE) or terminal as illustrated in Figure 2. The CLNE or terminal includes specific functions related to the certification of the health certified access service. The additional functionality relates to one or more of the following:

* security functions, including authentication and encryption
* health specific network addressing
* quality of service functionality.

All CH certified NNI Service Level Agreements (SLAs) are measured between the CH UNI and he Service Provider NNI-1.

Figure : The CH User to Network Interface and end to end performance



Appendix 1 lists the various Use Cases that may apply to each UNI.

## UNI-0

A basic public Internet access specification whereby connection will be established via authenticated VPNs terminating at a CH NNI-2. This is a single PC (not on a LAN) connecting to:

* a browser based application e.g. a form based service
* a non-browser based CH application e.g. HL7 messaging and legacy applications.

Network authentication is the responsibility of the TSP.

Table : UNI-0 Specifications

|  |  |  |
| --- | --- | --- |
| **Attributes** | Minimum | Preferred |
| **Speed Range** | >0.5Mbit/s download >180Kbit/s upload | >5Mbit/s download>0.5Mbit/s upload |
| **Class of Service – Best Effort** |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| Best effort |

  |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| 99.7% | Best effort | <400ms |

  |
| **Individual Authentication** |

|  |  |
| --- | --- |
| Service Type | Encryption (128 bit minimum) |
| Device | Network | Application |
| Browser based services | Not Applicable | Optional(IPsec, SSL, TLS client, etc) | Mandatory(SSL, TLS, client, etc) |
| Non-browser based services | Not Applicable | Mandatory(IPsec, SSL, TLS client, etc) | Optional |

  |
| **IP Version** | IPv4 | IPv6 |
| **No of Public IP Addresses** | Single IP address allocated by TSP |
| **Interconnection to other TSP UNIs** | Nearest available NNI-2 |
| **Service Performance Targets** | As per Appendix 2 |

Notes:

1. Performance between customer premises and the TSPs will be measured in the manner prescribed by existing customer SLAs.
2. Speed / throughput - 99.9% probability of providing from any test source to any provisioned end user a minimum downlink average throughput of 32Kbit/s during any 15 minute period on demand.
3. Network based authentication of IP address is not required.
4. Digital certificates, allocated by the CH certification authority, will be for authentication to applications and services rather than at network level.
5. One encryption method is mandatory for traffic transported across the public IP network.
6. SLAs to be measured on the UNI local access only.
7. UNI-0 references the Commerce Commission’s Standard Terms Determination for Telecom’s Unbundled Bitstream Access Service and the International Telecommunication Union – Telecommunication Standardisation Sector recommendation (ITU-T) Y1541 standard.
8. Figure 3 of Appendix 1 identifies the Use Case applicable to this UNI.
9. Number of public IP addresses – Dual stack Internet Protocol version 4 (IPv4) / Internet Protocol version 6 (IPv6) addresses will be allocated by CH.
10. A single PC refers to a single user, health dedicated computing device

## UNI-1

A basic public Internet access specification where connection will be established via authenticated VPNs terminating at a CH NNI-2. It is a single PC user or a small LAN connecting to:

* a browser based application e.g. a form based service or web based email.
* a non-browser based CH application e.g. HL7 messaging and legacy applications.

UNI-1 uses multiple addresses due to possible internal network subnet/s.

Table : UNI-1 Specifications

|  |  |  |
| --- | --- | --- |
| Attributes | Minimum | Preferred |
| **Speed Range** | >0.5Mbit/s download >180Kbit/s upload | >5Mbit/s download>0.5Mbit/s upload |
| **Class of Service – Best Effort** |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| Best effort |

  |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| 99.7% | Best effort | <400ms |

 |
| **Individual Authentication** |

|  |  |
| --- | --- |
| Service Type | Encryption (128 bit minimum) |
| Device | Network | Application |
| Browser based services | Not Applicable | Optional(IPsec, SSL, TLS client, etc) | Mandatory(SSL, TLS, client, etc) |
| Non-browser based services | Not Applicable | Mandatory(IPsec, SSL, TLS client, etc) | Optional |

  |
| **Site Authentication** **(Digital Certificate per site)** |

|  |  |
| --- | --- |
| Service Type | Encryption (128 bit minimum) |
| Device | Network | Application |
| Browser based services | Mandatory | Mandatory (IPsec, SSL, TLS client, etc) | Optional |
| Non-browser based services | Mandatory | Mandatory(IPsec, SSL, TLS client, etc) | Optional |

  |
| **IP Version** | IPv4 | IPv6 |
| **No of Public IP Addresses** | Multiple IP addresses, 1 allocated by TSP, others allocated by CH | Multiple static IP addresses, 1 allocated by TSP, others allocated by CH |
| **Interconnection to other TSP UNIs** | Nearest available NNI-2 |
| **Service Performance Targets** | As per Appendix 2 |

Notes:

1. Performance between customer premises and the TSPs will be measured in the manner prescribed by existing customer SLAs.
2. Speed / throughput - 99.9% probability of providing from any test source to any provisioned end user a minimum downlink average throughput of 32Kbit/s during any 15 minute period on demand.
3. Network based authentication of IP address is not required.
4. Digital certificates, allocated by the CH certification authority, will be for authentication to applications and services rather than at network level.
5. One encryption method is mandatory for traffic transported across the public IP network.
6. SLAs to be measured on the UNI local access only.
7. UNI-1 references the ITU-T Y1541 standard.
8. Figure 5 of Appendix 1 identifies the Use Cases applicable to this UNI.

## UNI-2

UNI-2 is for accessing CH using a public Internet service over a mobile telephone connection specification where connection will be established via authenticated VPNs terminating at a CH NNI-2.

This is a single mobile device connecting to a browser based application e.g a form based service or web based email.

Table : UNI-2 Specifications

|  |  |  |
| --- | --- | --- |
| Attributes | Minimum | Preferred |
| **Speed Range** | >60Kbit/s download >40Kbit/s upload | >1.4Mbps download>0.5Mbps upload |
| **Class of Service –Realtime** |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| Best effort |

  |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| 99.7% | < 0.1% | < 5ms | < 20ms |

  |
| **Class of Service –Interactive** |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| Best effort |

  |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| 99.7% | < 0.5% | < 50ms | < 100ms |

  |
| **Class of Service – Best Effort** |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| Best effort |

  |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| 99.7% | Best effort | 400ms |

  |
| **Individual Authentication** |

|  |  |
| --- | --- |
| Service Type | Encryption (128 bit minimum) |
| Device | Network | Application |
| Browser based services | Not Applicable | Optional(IPsec, SSL, TLS client, etc) | Mandatory(SSL, TLS, client, etc) |
| Non-browser based services | Not Applicable | Mandatory(IPsec, SSL, TLS client, etc) | Optional |

  |
| **IP Version** | IPv4 | IPv6 |
| **No of Public IP Addresses** | One IP address allocated by TSP |
| **Interconnection to other TSP UNIs** | Nearest available NNI-2 |
| **Service Performance Targets** | As per Appendix 2 |

Notes:

1. Performance between customer premises and the TSPs will be measured in the manner prescribed by existing customer SLAs.
2. Speed / throughput - 99.9% probability of providing from any test source to any provisioned end user a minimum downlink average throughput of 32Kbit/s during any 15 minute period on demand.
3. Network based authentication of IP address is not required.
4. Digital certificates, allocated by the CH certification authority, will be for authentication to applications and services rather than at network level.
5. One encryption method is mandatory for traffic transported across the public IP network.
6. UNI-2 references the ITU-T Y1541 standard.
7. Figure 4 of Appendix 1 identifies the Use Case applicable to this UNI.
8. A single mobile device refers to a single user, health dedicated mobile device

## UNI-3

A high speed symmetrical public Internet access specification where connection will be established via authenticated VPNs terminating at a CH NNI-2. It is a small to medium sized LAN connecting to:

* access browser based applications e.g. a form based serviced or web based email; or
* access non-browser based CH applications e.g HL7 messaging and legacy applications
* expose a low bandwidth service or email server to the CH community.

This UNI uses multiple addresses due to possible internal network subnet/s.

Table : UNI-3 Specifications

|  |  |  |
| --- | --- | --- |
| Attributes | Minimum | Preferred |
| **Speed Range** | >5Mbit/s download >5Mbit/s upload | >10Mbit/s download>10Mbit/s upload |
| **Class of Service – Realtime** |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| Best effort |

  |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| 99.7% | < 0.1% | < 5ms | < 20ms |

  |
| **Class of Service – Interactive** |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| Best effort |

  |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| 99.7% | < 0.5% | < 50ms | < 100ms |

  |
| **Class of Service – Best Effort** |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| Best effort |

  |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| 99.7% | Best effort | 400ms |

  |
| **Individual Authentication** |

|  |  |
| --- | --- |
| Service Type | Encryption (128 bit minimum) |
| Device | Network | Application |
| Browser based services | Not Applicable | Optional(IPsec, SSL, TLS client, etc) | Mandatory(SSL, TLS, client, etc) |
| Non-browser based services | Not Applicable | Mandatory(IPsec, SSL, TLS client, etc) | Optional |

  |
| **Site Authentication** **(Digital Certificate per site)** |

|  |  |
| --- | --- |
| Service Type | Encryption (128 bit minimum) |
| Device | Network | Application |
| Browser based services | Mandatory | Mandatory(IPsec, SSL, TLS client, etc) | Optional |
| Non-browser based services | Mandatory | Mandatory(SSL, TLS, etc) | Optional |

  |
| **IP Version** | IPv4 | IPv6 |
| **No of Public IP Addresses** | Multiple IP addresses One allocated by TSP, others assigned by CH |
| **Interconnection to other TSP UNIs** | Nearest available NNI-2 |
| **Service Performance Targets** | As per Appendix 2 |

Notes:

1. Performance between customer premises and the TSPs will be measured in the manner prescribed by existing customer SLAs.
2. Speed / throughput - 99.9% probability of providing from any test source to any provisioned end user a minimum downlink average throughput of 32Kbit/s during any 15 minute period on demand.
3. This is a symmetrical service offering
4. Network based authentication of IP address is not required
5. Digital certificates, issued by the CH certification authority, will be for authentication to applications and services rather than at a network level
6. One encryption method is mandatory for traffic transported across the public IP network
7. SLA to be measured on the UNI local access only
8. UNI-3 references the ITU-T Y1541 standard.
9. Figure 5 of Appendix 1 identifies the Use Case applicable to this UNI
10. Access to applications may require authentication.

## UNI-4

This is a private network access with a single end-point IP address specification directly connecting to the CH private IP network via a fixed authenticated VLAN to an NNI.

This is a large LAN environment (with possible sub-networks) with multiple users accessing both browser based (e.g. a form based service or web based email) and non-browser based applications and services (e.g. CH applications such as HL7 messaging and legacy applications).

This UNI will also support access to applications, services or websites they choose to host.

Table : UNI-4 Specifications

|  |  |  |
| --- | --- | --- |
| Attributes | Minimum | Preferred |
| Speed Range | >512Kbits/s download >512Kbit/s upload | >5Mbit/s download>5Mbit/s upload |
| Class of Service - Customisable | Customisable with multiple Class of Service (CoS) options with selection of predefined customer CoS profiles. |
| **Class of Service – Realtime** |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| 99.7% | Best Effort |  | < 400ms |

  |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| 99.9% | < 0.1% | < 5ms | 20ms |

  |
| **Class of Service – Interactive** |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| 99.7% | Best Effort |  | < 400ms |

  |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| 99.9% | < 0.5% | < 25ms | 50ms |

  |
| **Class of Service – Best Effort** |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| 99.7% | Best Effort |  | < 400ms |

  |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| 99.9% | < 1.0% | < 50ms | 100ms |

  |
| **Site Authentication** **(Digital Certificate per site)** |

|  |  |
| --- | --- |
| Service Type | Encryption (128 bit minimum) |
| Device | Network | Application |
| Browser based services | Optional | Optional | Optional |
| Non-browser based services | Optional | Optional | Optional |

 |
| IP Version | IPv4 | IPv6 |
| No of Public IP Addresses | Multiple IP addresses supportedOne allocated by TSP, others assigned by CH as standard, others available by application |
| Interconnection to other TSP UNIs | Nearest available NNI-1 |
| Service Performance Targets | As per Appendix 2 |

Notes:

1. Performance between customer premises and the TSPs will be measured in the manner prescribed by existing customer SLAs.
2. Speed/throughput are defined by the TSP service.
3. Network based authentication of IP address is not required.
4. Digital certificates, issued by the CH certification authority, will be for authentication to applications and services rather than at a network level.
5. Encryption is mandatory on at least one of the device, transport or application layers.
6. Private VLANs and edge firewalls are mandatory.
7. SLA to be measured on the UNI local access only.
8. UNI-4 references the ITU-T Y1541
9. Figure 6 of Appendix 1 identifies the Use Case applicable to this UNI.

## UNI-4a

This is a private network access method based on the UFB Bitstream 2 service. This will be delivered with a single endpoint IP address directly connecting to the Connected Health private IP network via a fixed authenticated VLAN to an NNI.

This is a small LAN environment (with possible sub-networks) with multiple users accessing both browser based (for example, a form based service or web based email) and non-browser based applications and services (for example, Connected Health applications such as HL7 messaging and legacy applications).

Table : UNI-4a Specifications

| **Attributes** | **Minimum** | **Preferred** |
| --- | --- | --- |
| **Speed Range** | 30Mbits/s download (5Mbps CIR) 10Mbits/s upload (5Mbps CIR) | 100Mbits/s download (10Mbps CIR) 50Mbits/s upload (2.5Mbps CIR) |
| **Class of Service** | Fixed Class of Service (CoS) with customer selectable amount of high priority bandwidth. |
| Class of Service – - High (CIR) |

| **Service Quality** |
| --- |
| **Availability** | Packet loss | Jitter | Latency |
| **99.7%** | Best Effort | ≤5 ms | ≤ 100ms |

  |

| **Service Quality** |
| --- |
| **Availability** | Packet loss | Jitter | Latency |
| **99.9%** | Best Effort | ≤ 5ms | ≤ 20ms |

  |
| Class of Service – Best Effort |

| **Service Quality** |
| --- |
| **Availability** | Packet loss | Jitter | Latency |
| **99.7%** | Best Effort |

  |

| **Service Quality** |
| --- |
| **Availability** | Packet loss | Jitter | Latency |
| **99.9%** | **Best Effort** |

  |
| **IP Version** | IPv4 | IPv4 + IPv6 |
| ***No of Public IP Addresses*** | *Multiple IP addresses supported**One allocated by TSP, others assigned by CH as standard, others available by application* |
| **Interconnection to other TSP UNIs** | Nearest available NNI-1 |

Notes:

1. Performance between customer premises and the TSPs will be measured in the manner prescribed by existing customer SLAs.
2. Speed/throughput are defined by the TSP service.
3. Network based authentication of IP address is not required.
4. Digital certificates, issued by the CH certification authority, will be for authentication to applications and services rather than at a network level.
5. Encryption is mandatory on at least one of the device, transport or application layers.
6. Private VLANs and edge firewalls are mandatory.
7. SLA to be measured on the UNI local access only.
8. The fixed Class of Service supports the mapping of DSCP ‘EF’ and PCP ‘5’ into the ‘High Priority’ class. All other traffic is in the ‘Best Effort’ class.

## UNI-5

This is a high speed private network access multiple end-point IP address specification directly connecting to the CH private IP network via a fixed authenticated VLAN to an NNI.

This is a large LAN environment (with possible sub-networks) with multiple users accessing both browser based (e.g. a form based service or web based email) and non-browser based applications and services (e.g. CH applications such as HL7 messaging and legacy applications).

This UNI will also support access to applications services or websites they choose to host.

The specifications for this UNI are set out below.

Table : UNI-5 Specifications

|  |  |  |
| --- | --- | --- |
| Attributes | Minimum | Preferred |
| Speed Range | >5Mbit/s download >5Mbit/s upload | >10Mbit/s download>10Mbit/s upload |
| Class of Service – Realtime |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| 99.7% | < 0.1% | ≤ 5ms | 10ms |

  | Customisable with multiple CoS options with selection of predefined customer CoS profiles. Availability will be greater than 99.95% |
| Class of Service – Interactive |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| 99.7% | < 0.5% | ≤ 10ms | < 25 ms |

  |
| Class of Service – Best Effort |

|  |
| --- |
| Service Quality |
| Availability | Packet loss | Jitter | Latency |
| 99.7% | < 1.0% | < 50ms | < 100ms |

  |
| Site Authentication (Digital Certificate per site) |

|  |  |
| --- | --- |
| Service Type | Encryption (128 bit minimum) |
| Device | Network | Application |
| Browser based services | Optional | Optional | Optional |
| Non-browser based services | Optional | Optional | Optional |

 |
| IP Version | IPv4 | IPv6 |
| No of Public IP Addresses | Multiple IP addresses supportedOne IP address assigned by CH as standard, others available by application |
| Interconnection to other TSP UNIs | Nearest available NNI-1 |
| Service Performance Targets | As per Appendix 2 |

Notes:

1. Performance between customer premises and the TSPs network will be measured in the manner prescribed by existing customer SLAs.
2. Speed/throughput are defined by the TSP service.
3. Measurement of availability to be the average by CH UNI per TSP over a 12 month period.
4. Network based authentication of IP address is not required.
5. Digital certificates, issued by the CH certification authority, will be for authentication to applications and services rather than at a network level.
6. Encryption is mandatory on at least one of the device, transport or application layers.
7. Multiple VLAN/CoS profiles to be supported.
8. Jitter description needs definition to ensure commonality of measurement by vendors.
9. SLAs to be measured on the UNI local access only.
10. UNI-5 references the ITUY1541.
11. Figure 6 of Appendix 1 identifies the Use Case applicable to this UNI.

Appendix : Use Cases

(Informative)

Overview

Some possible Use Cases are summarised below.

Table : Possible Use Cases

|  |  |  |
| --- | --- | --- |
| UNI | Network Authentication | Use Case |
| UNI-0 | Individual | 1 |
| UNI-2 | Individual | 2 |
| UNI-1/3 | Site Certificate | 3 |
| UNI-4 | Not applicable | 4 |
| UNI-5 | Not applicable | 5 |

Use Case 1: Single user accessing services

A single user using a UNI–0 connection accesses a service.

* The user authenticates to the network at the VPN termination point (NNI-2).
* The CH DNS resolves the domain name and the user connects to the requested health service where any application based authentication is carried out.
* When authenticated the user is able to access the health services, using HTTPS or another suitable client.

Figure : Single user accessing web based services



Note that the CH Meta Directory and CH Authentication systems are included in the diagram as signals of future direction.

Use Case 2: Single mobile user accessing web based services

A single mobile device user using a UNI-2 connection accesses a web based service.

* The user authenticates to the network at the VPN termination point (NNI-2).
* The CH DNS resolves the domain name and the user connects to the requested health service where any application based authentication is carried out.
* When authenticated the user is able to access the health services, using HTTPS or another suitable client.

Figure : Single mobile user accessing web based services



Note that the CH Meta Directory and CH Authentication systems are included in the diagram as signals of future direction.

Use Case 3: Small multi user site accessing services

Multiple users connected to a LAN are authenticated by their site connectivity device to the CH network.

* The user authenticates to the network at the VPN termination point (NNI-2).
* The CH DNS resolves the domain name and the user connects to the requested health service where any application based authentication is carried out.
* When authenticated by CH the user is able to access the health services using encrypted VPN tunnel Digital certificates which will be issued by the CH certification authority.

Figure : Multiple user site accessing CH services



Note that the CH Meta Directory and CH Authentication systems are included in the diagram as signals of future direction.

Use Case 4: Large multiple user site accessing web based services

Multiple users connected to a LAN are authenticated by their site connectivity device to the CH network.

1. The CH DNS resolves the domain name
2. The user connects to the requested health service where any application based authentication is carried out.

Figure : Large multiple user site accessing CH services



Note that the CH Meta Directory and CH Authentication systems are included in the diagram as signals of future direction.

Use Case 5: District Health Board (DHB) using Metropolitan Area Network (MAN).

The DHB is using a MAN to provide a network to health practitioners within a region. The DHB networks then interface with other TSP networks and the Internet by the corresponding NNI connections. This allows users to access both web based and non web based health services.

Figure : DHB using MAN



Appendix : Service Performance Targets

(Informative)

Classes of Service (CoS):

* **Multiple CoS -** CoS are to be available in a number of pre-configured profiles and selected custom profiles that set the proportion of each UNI allocated to each CoS. Customers will be able to choose which of the available CoS profiles will be used for each UNI.
* **Real-time –** Optimised for applications involving real-time human interaction, multimedia interactions such as interactive video or IP voice e.g. Mobile Surgery Services.
* **Interactive –** Optimised for applications involving interactive input and response, such as human-to-PC conversations, for example thin client (Citrix/Sun Ray, SNA, Telnet, H.323 signalling), streaming video and audio, web browsing, instant messaging.
* **Best Effort –** For applications such as Personal Computer-to-Personal Computer transmission of files and objects, form based interactions or structured and unstructured messaging that need fairly prompt delivery, e.g. database access, HL7 Messaging (pathology results, eReferrals), Accident Compensation Corporation (ACC) and HealthPac Claiming, email, FTP downloads.

Table : Service Performance Targets

|  |  |  |
| --- | --- | --- |
| Service Attribute | Attribute Definition | Service Target |
| 1. Agreed service hours
 | The hours during which, if a customer call or monitoring alarm indicates a fault, the TSP will commence restoration work.  | 0700 to 1900 business days, or longer where relevant Service Level Options are offered. |
| 1.a Optional extended service hours | Extended hours during which, when a customer call or monitoring alarm indicates a fault, the TSP will commence restoration work. | **Option a:** 0700 to 1900 x 7 days. **Option b:** 24 hours x 7 days. |
| 1. Call reception
 | The hours during which incoming telephone calls from customers to the TSP Help Desk are accepted and logged, and the call answering times. | Calls accepted 24 hours x 7 days and answered within 20 seconds. |
| 1. Monitoring hours
 | The hours during which infrastructure monitoring systems are operational. | 24 hours x 7 days. |
| 1. Proactive Alarm Notification
 | The elapsed time between a service-impacting alarm or a major core network event occurring and the customer being notified that it has occurred and is being investigated. | Customer notified within 45 minutes (Manual) or 30 minutes (Automated) of alarm occurrence during agreed service hours, or as otherwise agreed. |
| 1. Response time
 | The elapsed time during agreed service hours between Call Reception or alarm occurrence and the TSP commencing restoration work. | Within 60 minutes of Call Reception or alarm occurrence during agreed service hours. An estimated restore time is provided if known. |
| 1. Initial restoration update
 | The elapsed time during agreed service hours between Call Reception or alarm occurrence and the customer being notified that initial diagnosis is completed. | Within 60 minutes of Call Reception or alarm occurrence during agreed service hours. An estimated restore time is provided if known. |
| 1. Progress updates
 | Updates during agreed service hours on the status of service restoration activity. | Hourly or as agreed. |
| 1. Remote service restoration
 | The elapsed time during agreed service hours between Call Reception or alarm occurrence and the customer being notified that service is restored to the defined levels without a site visit. | Within 4 hours, and 80% within 2 hours. |
| 1. On-site service restoration
 | The elapsed time during agreed service hours between Call Reception or alarm occurrence and the customer being notified that service is restored to the defined levels as a result of a site visit. | **NZ metro areas:** Within 6 hours**NZ rural areas:** Within 8 hours |
| 1. Billing enquiry resolution
 | The elapsed time during agreed service hours between reception of a billing enquiry and confirmation to the customer of its resolution. | Within 2 business days. |
| 1. Planned outage notification
 | Prior notice of planned maintenance that could cause a service outage. | 5 business days. |
| 1. Provisioning / Change Request acceptance
 | The elapsed time between a customer logging a Provisioning/Change Request and the confirmed acceptance of that request. | Receipt acknowledged within 2 business hours. Committed Ready for Service Date advised within 2 business days. |
| 1. Provisioning / Change Request completion
 | The elapsed time between the confirmed acceptance of a Provisioning/Change Request and the completion of that request. |  |
| 1. Remote Simple
 | Within 2 business hours. |
| 1. Standard (with local access, no contract variation required)
 | Within 3 business days. |
| 1. Standard (with local access, contract variation required)
 | Within 5 business days. |
| 1. Standard (with no local access, contract variation required)
 | Within 21 business days (or on a defined date and time). |
| 1. Complex
 | As agreed. |

Appendix : Glossary of Terms

(Informative)

|  |  |
| --- | --- |
| Term | Description |
| 3rd Generation Partnership Project (3GPP) | A collaboration between groups of telecommunications associations to create a globally applicable third generation (3G) mobile phone system specification. This activity is within the scope of the International Telecommunication Union’s project known as the International Mobile Telecommunications-2000. 3GPP specifications are based on evolved Global System for Mobile Communications (GSM) specifications. 3GPP standardisation encompasses radio, core network and service architecture. |
| Accident Compensation Corporation (ACC) | An organization which provides comprehensive, no-fault personal injury cover for all New Zealand residents and visitors to New Zealand. |
| Availability | A measure of what proportion of total available time a service is actually available, normally expressed as a percentage. Total available time normally excludes planned service outages or a force majeure event. |
| Basic Unbundled Bitstream Access (BUBA) | A Telecom wholesale service which allows service providers to offer own-branded Internet-grade broadband services to home and small enterprise end-users, delivered over Digital Subscriber Line (DSL) access lines. |
| Class of Service (CoS) | A method of grouping network traffic into classes for the purpose of prioritisation. Commonly used in relation to Quality of Service (QoS) services. |
| Client Software | Software that resides in a user’s desktop or laptop computer, PDA or cellphone. |
| Committed Information Rate (CIR) | Committed information rate is the average bandwidth for a virtual circuit guaranteed by an ISP to work under normal conditions. |
| Communication Lag, Latency or Transfer Delay | The time taken for a packet of data to be sent by an application, travel and be received by another application.The absolute time (in milliseconds) from the time the first bit of an IP packet enters the customer side of the ingress (source) terminating equipment to the time the first bit of the same packet exits from the customer side of the egress (destination) terminating equipment. |
| Connected Health (CH) / Connected Health Team | The Ministry of Health programme or business entity that implements and supports improved network inter-connectivity for the health sector, facilitating the delivery of improved network resources to health providers. |
| Customer Located Network Equipment (CLNE) | Equipment from a TSP that supports connection to a customer’s network, and is placed on a customer’s site. |
| Demilitarized zone (DMZ) | A physical or logical sub network that contains and exposes an organisation’s external services to a larger un-trusted network, usually the Internet. |
| Domain Name Service (DNS) | A service that matches IP addresses to Domain Names and vice versa. |
| Government Logon Service (GLS) | Also known as igovt logon service, a service that collects and validates credentials for a person accessing a variety of secure online government services. This service is operated and maintained by the State Services Commission. |
| Health Network Code of Practice (HNCOP) | Developed by Standards New Zealand in 2002 as the code of practice for all Health Network members, including telecommunication providers. |
| HISO 10029.1 Health Information Security Framework (HISF) | The HISF is based on AS/NZS ISO/IEC 27002:2006. It specifies minimum policy standards and technical requirements to support organisations and practitioners holding personally identifiable health information to improve the security of that information, so it can be produced, stored, disposed of and shared in a way that ensures confidentiality, integrity and availability.  |
| Hypertext transfer protocol (HTTP) | An application layer network protocol for distributed information systems, providing a standard for Web browsers and servers to communicate. |
| Internet Protocol (IP) | A widely adopted and standardised computer communications protocol used to enable computers to be networked and to communicate by transferring information between them. |
| Internet Protocol Security (IPsec) | A protocol suite for securing IP communications by authenticating and encrypting each IP packet. |
| IPv4 address | The fourth revision in the development of the IP and the first version of the protocol to be widely deployed. Together with IPv6, it is at the core of standards-based Internetworking methods of the Internet. IPv4 has a smaller address space than Ipv6. IPv4 uses a 32-bit address compared to 128 bits for IPv6. |
| IPv6 address | The next-generation IP version designated as the successor to IPv4. It is an Internet layer protocol for packet-switched networks. IPv6 has a vastly larger address space using a 128-bit address, compared to 32 bits for IPv4. |
| Jitter | An unwanted variation of one or more characteristics of a periodic signal in telecommunications, also known as Delay Variation.The difference (in milliseconds) between the minimum and maximum Latency. This is calculated one-way over a one minute interval for 99% of equal-sized IP packets in a stream with randomly varying arrival times. |
| Layer 2 | Layer 2 is the ‘data’ level in Open Systems Interconnection (OSI) 7-layer model. In very basic terms, Layer 1 is the physical cable connection; Layer 2 adds transmission error detection, while Layer 3 adds packet routing/error correction/congestion control. Layer 2 is a non-managed service. |
| Layer 3 | Layer 3 is the network layer is the third layer of the OSI model. Layer 3 is responsible for end-to-end (source to destination) packet delivery, whereas Layer 2 is responsible for node to node delivery. Layer 3 is typically associated with routing. Layer 3 services are often referred to as ‘managed services’. |
| Local Area Network (LAN) | A group of computers and associated devices that share a common communications line or wireless, link within a single physical location. |
| Metropolitan Area Network (MAN) | A network that interconnects users with computer resources in a geographic area or region larger than that covered by a Local Area Network but smaller than the area covered by a Wide Area Network. Typically a city. |
| Network to Network Interface (NNI) | An interconnection point between IP carrier networks. NNI1 is an interconnection between private networks and NNI2 is an interconnection between private and public networks. |
| Openness | Openness is an architectural principle referring to equal availability of products and services to participating suppliers and organisations. |
| Packet Loss | Occurs when one or more packets of data travelling across a computer network fail to reach their destination. |
| Personal Computer (PC) | A desktop, tablet, notebook, laptop, or portable computer. |
| Secure Sockets Layer (SSL) | A cryptographic protocol that provides security for communications over networks such as the Internet and is the predecessor to Transport Layer Security (TLS). |
| Service Level Agreement (SLA) | A formal agreement between two parties where one party agrees to deliver a defined and measurable level of service to the other party. |
| Telecommunications Service Provider (TSP) | A provider of telecommunications services (telephone, network, internet services etc.) to the New Zealand public, private, commercial and government sectors, and which has a network licence as defined under the Telecommunications Act 2006. |
| Throughput | The maximum average data rate for a given packet size that a network connection can sustain while conforming to the specified functional performance targets. Also known as Sustained Data Rate. |
| Transit TSP | A TSP that carries network data between POI. |
| Transport Layer Security (TLS) | A cryptographic protocol that provides security for communications over networks such as the Internet and is the successor to Secure Socket Layer (SSL). |
| Unbundled Network Service (UNS) | A business grade, Layer 2 data access tail product that delivers a range of symmetrical access bandwidth options to an end-user site over a Digital Subscriber Line copper line. The end-user is presented with an ethernet interface. |
| User to Network Interface (UNI) | The connectivity product/service that connects a subscriber to the Connected Health network. This is the physical and logical IP connectivity to the network from one of the end points, such as a single PC or large private network. |
| Virtual Local Area Network (VLAN or vLAN) | A method of creating independent logical networks within a physical network. Several VLANs can co-exist within a single physical network. |
| Virtual Private Network (VPN) | A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organisation's network. |