



Connected Health

UNI Specifications

Prepared by:	Peter Shephard
Date:	12/08/2008
Version:	V1.4
Status:	Final

Table of Contents

1	INTRODUCTION	3
2	INTERFACE SPECIFICATIONS.....	4
2.1	UNI-0	5
2.2	UNI-1	6
2.3	UNI-2	6
2.4	UNI-3	7
2.5	UNI-4	9
2.6	UNI-5	9

1 Introduction

This document details the technical specifications for the User-to-Network (UNI) class 0 to 5 interfaces described in the Connected Health Architectural Framework V0.4.

The specifications define a set of minimum and preferred characteristics for each of the interface classes outlined in the framework.

These specifications will form the baseline requirements for the definition of a set of standardised Connected Health certified access products. These are intended to be used by the Connected Health Industry forum to finalise the product standards to be used by Telecommunications providers for developing their own specific certified Connected Health product sets.

The document has been amended after the first Connected Health Standards Working Group meeting on 28th May 2008 and is now available for review and input from all participants as version 1.2 FINAL.

The document has been amended after the second Connected Health Standards Working Group meeting on 10th July 2008 and is now available for review and input from all participants as version 1.3 FINAL.

The document has been amended after the third Connected Health Standards Working Group meeting on 12th August 2008 and is now available for review and input from all participants as version 1.4 FINAL.

2 Interface Specifications

As per the reference architecture, the following is a table of the User-to-network (UNI) classes defined. The technical specifications for each of these UNI's are defined in sections 2.1 to 2.6.

Class	Description	Minimum Requirements
UNI-0	Public UNI – Basic Public Internet access	Internet access using single fixed public IP address. Network Address Translation (NAT) may be used to hide any RFC1918 private IP addresses behind the UNI. Connection to NNI-2 is via authenticated VPN tunnels (eg. GRE, L2TP, SSL, TSL, etc).
UNI-1	Public UNI – Public Internet	Internet access using multiple public IP address. NAT may be used to hide any RFC1918 private IP addresses behind the UNI. Connection to NNI-2 is via authenticated VPN tunnels (eg. GRE, L2TP, SSL, TSL, etc).
UNI-2	Public UNI – Mobile Internet Access	Mobile access to Connected Health using a public internet service over a Mobile telephone connection. For mobile Connected Health users (UNI-2), end points must have a fixed network identifier to ensure the end-point can always be validated as an authorised connection for inbound access to the Connected Health network. Connection to NNI-2 is via authenticated VPN tunnels (eg. GRE, L2TP, SSL, TSL, etc).
UNI-3	Public/Private UNI – Public Internet with fixed VLAN to Connected Health Private IP	Interface providing access to both the Internet and Connected Health private IP network using 802.1Q VLAN's
UNI-4	Private UNI– Private IP	Access to Connected Health using single fixed private IP addresses. NAT may be used to hide any RFC1918 private IP addresses behind the UNI. This interface is required to provide an IPv4 to IPv6 boundary point if a Connected Health member's SI cannot support native IPv6 connectivity to the connection point. The UNI will be required to tunnel IPv4 traffic over the Connected Health core IPv6 network.
UNI-5	Private UNI 2 – Private IP	Access to Connected Health using multiple fixed private IP addresses. NAT may be used to hide any RFC1918 private IP addresses behind the UNI. This interface is required to provide an IPv4 to IPv6 boundary point if a Connected Health member's SI cannot support native IPv6 connectivity to the connection point. The UNI will be required to tunnel IPv4 traffic over the Connected Health core IPv6 network.

2.1 UNI-0

The User-to-Network-Interface (UNI-0) is the basic public Internet access specification for connection to Connected Health. Connections to Connected Health will be via authenticated VPN's terminating at a Connected Health NNI-2.

The specifications for this UNI are as follows:

Attributes	Minimum				Preferred			
Speed Range	>0.5Mbit/s Download > 150Kbit/s Upload				>5Mbit/s Download > 0.5Mbit/s Upload			
Service Quality	Availability	Packet loss	Jitter	Latency	Availability	Packet loss	Jitter	Latency
	Best effort	Best effort	Best effort	Best effort	Best effort	Best effort	Best effort	750ms
IP Version	IPv4				IPv6			
No of Public IP Addresses	1 (Fixed)				1 (Fixed)			
Firewall / Type	SPI and filtering, External IPsec/Mutual SSL capable				SPI and filtering, Integrated Internal			
Interconnection	Standard Internet				Nearest available Internet interconnection point			
Authentication Type (VPN Access)	Radius + IP Address				Radius + IP Address			
Encryption scope	Device ¹	Network	Application		Device ¹	Network	Application	
	Optional	✓	Optional		Optional	✓	Optional	
Service definition (Grade of Service)	Best effort				Negotiated SLA			

Remark: Firewall attributes are highlighted in gray in the UNI-specification which means that they need further discussions in the Standards working group. The working group will comment on the Authentication and Security Framework proposal from EAC to align with the security requirements on firewalls.

¹ This is the encryption device / Firewall

2.2 UNI-1

UNI-1 is also a basic public internet access specification but allows for a provider to allocate multiple public Internet addresses to the Connected Health access point. Connections to Connected Health will be via authenticated VPN's terminating at a Connected Health NNI-2.

The specifications for this UNI are as follows:

Attributes	Minimum				Preferred			
Speed Range	>0.5Mbit/s Download > 160Kbit/s Upload				>5Mbit/s Download > 0.5Mbit/s Upload			
Service Quality	Availability	Packet loss	Jitter	Latency	Availability	Packet loss	Jitter	Latency
	Best effort	Best effort	Best effort	Best effort	Best effort	Best effort	Best effort	750ms
IP Version	IPv4				IPv6			
No of Public IP Addresses	> 1 (Fixed)				> 1 (Fixed)			
Firewall / Type	SPI and filtering, External IPSec/Mutual SSL capable				SPI and filtering, Integrated Internal			
Interconnection	Standard Internet				Nearest available Internet interconnection point			
Authentication Type (VPN Access)	Radius + IP Address				Radius + IP Address			
Encryption scope	Device ²	Network	Application		Device ²	Network	Application	
	Optional	✓	Optional		Optional	✓	Optional	
Service definition (Grade of Service)	Best effort				Negotiated SLA			

Remark: Firewall attributes are highlighted in gray in the UNI-specification which means that they need further discussions in the Standards working group. The working group will comment on the Authentication and Security Framework proposal from EAC to align with the security requirements on firewalls.

² This is the encryption device / Firewall

2.3 UNI-2

UNI-2 is for Mobile access to Connected Health using a public Internet service over a mobile telephone connection. For mobile Connected Health users (UNI-2), end points **must** have a fixed network identifier (e.g. MAC address) to ensure the end-point can always be validated as an authorised connection for inbound access to the Connected Health network. Connections to Connected Health will be via authenticated VPN's terminating at a Connected Health NNI-2.

The specifications for this UNI are as follows:

Attributes	Minimum	Preferred												
Speed Range	>60KBit/s Download > 40KBit/s Upload	>60KBit/s Download > 40KBit/s Upload												
Service Quality	None	None												
Authentication to Connected Health Network Access Control	Radius +MAC Address or equivalent	Radius +MAC Address or equivalent												
IP Version	IPv4	IPv6												
No of IP Public Addresses	1	1												
Firewall / Type	SPI and filtering, External IPSec/Mutual SSL capable	SPI and filtering, Software – Integrated												
Interconnection	Standard Internet	Nearest available Internet interconnection point												
Encryption scope	<table border="1"> <tr> <td>Device</td> <td>Network</td> <td>Application</td> </tr> <tr> <td>Device certificate</td> <td>Optional ³</td> <td>Optional ³</td> </tr> </table>	Device	Network	Application	Device certificate	Optional ³	Optional ³	<table border="1"> <tr> <td>Device</td> <td>Network</td> <td>Application</td> </tr> <tr> <td>Device certificate</td> <td>Optional ³</td> <td>Optional ³</td> </tr> </table>	Device	Network	Application	Device certificate	Optional ³	Optional ³
Device	Network	Application												
Device certificate	Optional ³	Optional ³												
Device	Network	Application												
Device certificate	Optional ³	Optional ³												
Service definition (Grade of Service)														

Remark: Firewall attributes are highlighted in gray in the UNI-specification which means that they need further discussions in the Standards working group. The working group will comment on the Authentication and Security Framework proposal from EAC to align with the security requirements on firewalls.

³ One encryption method is mandatory, choice of network encryption or application encryption.

2.4 UNI-3

UNI-3 is for Ethernet (fibre or copper or wireless) based access to a public Internet service. Connections to Connected Health will be via authenticated VPN's terminating at a Connected Health NNI-2.

The specifications for this UNI are as follows:

Attributes	Minimum				Preferred			
Speed Range	>5MBit/s Download > 5MBit/s Upload				>10MBit/s Download > 10MBit/s Upload			
Service Quality	Availability	Packet loss	Jitter	Latency	Availability	Packet loss	Jitter	Latency
	Best effort	Best effort	Best effort	Best effort	Best effort	Best effort	Best effort	750ms
IP Version	IPv4				IPv6			
No of Public IP Addresses	1 (Fixed)				> 1 (Fixed)			
Firewall / Type	SPI and filtering, External IPSec/Mutual SSL capable				SPI and filtering, Integrated Internal			
Interconnection	Standard Internet				Nearest available Internet interconnection point			
Authentication Type (VPN Access)	Radius + IP Address				Radius + IP Address			
Encryption scope	Device ⁴	Network	Application		Device ⁴	Network	Application	
	Optional	✓	Optional		Optional	✓	Optional	
Service definition (Grade of Service)	Best effort				Negotiated SLA			

Remark: Firewall attributes are highlighted in gray in the UNI-specification which means that they need further discussions in the Standards working group. The working group will comment on the Authentication and Security Framework proposal from EAC to align with the security requirements on firewalls.

⁴ This is the encryption device / Firewall

2.5 UNI-4

UNI-4 is for Ethernet (fibre or copper) based access directly connected to Connected Health private IP network using a single end-point IP address, via direct link or a fixed authenticated VLAN to connected Health.

The specifications for this UNI are as follows:

Attributes	Minimum	Preferred	
Speed Range	>5MBit/s Download > 5MBit/s Upload	>10MBit/s Download > 10MBit/s Upload	
Service Quality	3 differentiated Levels of QoS		
	Real Time	interactive	Best effort
	✓	✓	✓
Authentication to Connected Health Network Access Control	Radius + IP Address		
	Radius + IP Address		
	Radius + IP Address		
IP Version	IPv4	IPv6	
No of IP Addresses	1 (Fixed)	1 (Fixed)	
Firewall / Type	SPI and filtering, External IPSec/Mutual SSL capable	SPI and filtering, Integrated Internal	
Interconnection	To at least one Connected Health NNI	To more than one Connected Health NNI	
Encryption scope	Device ⁵	Network	Application
	Optional	✓	Optional
	Optional	✓	Optional
Service definition (Grade of Service)	SLA	SLA	

Remark: Firewall attributes are highlighted in gray in the UNI-specification which means that they need further discussions in the Standards working group. The working group will comment on the Authentication and Security Framework proposal from EAC to align with the security requirements on firewalls.

⁵ This is the encryption device / Firewall

2.6 UNI-5

UNI-5 is for Ethernet (fibre or copper) based access directly connected to Connected Health private IP network using multiple end-point IP addresses, via direct link or a fixed authenticated VLAN to connected Health.

The specifications for this UNI are as follows:

Attributes	Minimum	Preferred	
Speed Range	>5MBit/s Download > 5MBit/s Upload	>10MBit/s Download > 10MBit/s Upload	
Service Quality	3 differentiated Levels of QoS		
	Real Time	interactive	Best effort
	✓	✓	✓
Authentication to Connected Health Network Access Control	Radius + IP Address		
	Real Time	interactive	Best effort
	✓	✓	✓
IP Version	IPv4	IPv6	
No of IP Addresses	>1 (Fixed)	>1 (Fixed)	
Firewall / Type	SPI and filtering, External IPSec/Mutual SSL capable	SPI and filtering, Integrated Internal	
Interconnection	To at least one Connected Health NNI	To more than one Connected Health NNI	
Encryption scope	Device ⁶	Network	Application
	Optional	✓	Optional
	Optional	✓	Optional
Service definition (Grade of Service)	SLA	SLA	

Remark: Firewall attributes are highlighted in gray in the UNI-specification which means that they need further discussions in the Standards working group. The working group will comment on the Authentication and Security Framework proposal from EAC to align with the security requirements on firewalls.

⁶ This is the encryption device / Firewall