IST-2000-25153

Deliverable D7

Description of Implementations of the Clinical Testbeds

Contractual Date of Delivery to the European Commission:	**December 2001**
Actual Date of Delivery to the European Commission:	**January 2002**
Editor(s):	**Dr Dipak Kalra, UCL**
Participant(s):	**UCL**: D Kalra, T Austin, A O'Connor, D Lloyd, D. Ingram, D Patterson **UKT:** M Rall **RUS:** P Christ, Y Scheerer, Y Liang **UMM:** K Zielinski, A Koprowski, D Radziszowski, P Rzepa
Workpackage:	**5**
Title of Deliverable:	**Description of Implementations of the Clinical Testbeds**
Security:	**IST**
Nature:	**R**
Version:	**1.0**
Number of pages:	**83**

Abstract: This deliverable describes the technical infrastructure and the clinical applications intended for the three clinical testbed demonstrator sites of the 6WINIT Project. These sites provide a means of validating the technical 6WINIT solutions and of the potential benefits of using wireless IPv6 services. In this deliverable each site has documented the proposed technical infrastructure in terms of the partner components to be deployed. Each site has also provided a description of the clinical applications to be demonstrated.

Keywords: Health informatics, Computerised medical records, Distributed systems, IPv6/IPv4 Transition, IP Security, Mobile IPv6

Executive Summary

The 6WINIT project aims to validate the introduction of the new mobile wireless internet in Europe.

Three clinical sites have been chosen to represent the early marketing targets within the healthcare domain as demonstrator sites:

- John Paul II Hospital, Krakow, Poland
- Eberhard-Karls University, Tübingen, Germany
- Whittington Hospital, London, UK

These sites were chosen partly because they have a longstanding relationship with three of the technical partners in the project (UCL, RUS and UMM respectively), and partly because the applications they proposed were useful tests of the type of services which could be provided well in the mobile environment.

This deliverable presents the technical architecture envisaged at each site, including the 6WINIT partner components that will be demonstrated and an overview of the clinical applications that will exploit the overall 6WINIT IPv6 solutions.

The deliverable consists of three similarly-structured sections, one describing each site. Each site description in turn comprises:

1. The clinical scenarios to be demonstrated, including (where known) the locations, devices and kinds of information services to be accessed.
2. A brief summary of the overall technical architecture, fuller descriptions of which were provided in Deliverable 3.
3. A structured analysis of the functional requirements and proposed technical solutions for each site, presented as a set of small tables, one per functional requirement.
4. A description of the clinical applications being developed, with an indication of the progress and expected completion of this work.

A slight exception to this is the report of the Tübingen site. A considerable effort has recently gone into this site in preparation for the IST Demonstration in Düsseldorf (December 2001). This site report describes the clinical applications and scenarios in terms of that demonstration, which was a realistic exemplar of the intended real demonstration at that site.

This deliverable is expected to pave the way for the detailed specification, configuration and deployment of partner components at each site in the coming months, to establish the 6WINIT technical solution for final validation and demonstration.

Table of Contents

1 INTRODUCTION

This Deliverable describes separately the three clinical demonstrators that are being developed in London, Krakow and Tübingen. In fact the demonstrators are not that separate; there is detailed interaction between them. Moreover, they all use different components from the technical workpackages. Thus, for example, the London and Krakow demonstrators both use the 6WIND routers from WP6 and D8, and are collaborating (with their technical support at UCL and UMM) in the testing and evaluation of the routers. Several of them will be using the same IPAC terminals for some of their work; again they are all collaborating with the IPAC implementations being carried out in WP7 and D10.

Similarly the clinical demonstrators are very sensitive to the need for transitioning between IPv4 and IPv6 regimes. For this reason, there has been considerable interaction between the trajectory proposed by the clinical demonstrators, and the transition techniques described in D9.

While this Deliverable is written entirely from the viewpoint of clinical demonstrators, it will be clear from the technical components in each case that they are making heavy use of the developments in the technical workpackages. For example all the security infrastructure, Mobile IP, and network support comes from these workpackages. It would, however have been tedious to have put cross-references at all times between the developments in WP4, WP6, WP7 and WP8 and these demonstrators.

So far we are describing only three demonstrators; the Project Work Plan also made mention of a demonstrator at the University Hospital of Basel (UHB). The work at UHB has been carried out under another project (Möbius). There have been discussions with them, and a proposal for UHB will be discussed at the Annual Review. Up to the time covered by this Deliverable, the talks are not yet conclusive. For this reason no mention of a UHB Demonstrator is made in the remainder of this report.

2 LONDON CLINICAL DEMONSTRATOR

2.1 User Scenarios

The following access scenarios describe the various technical settings in which healthcare staff or patients may need to access electronic health record information via 6WINIT networks. (A fuller description of the London clinical scenario was published in 6WINIT Deliverable 3.)

2.1.1 Roadside emergency access to patient's medical summary

Clinical information requirement The doctor, nurse or ambulance worker needs to review (but not change) the basic medical summary of an accident victim or other emergency care patient, held on the CHIME record server, from any public location including the street. A web-based (WAP) application is being developed for this.

Device and location They will need to view the data on a hand-held device, and may be some kilometres from their own place of work but will not need to roam while connected.

Security The user will need to be authenticated and verified (e.g. via token and PKI), and their connection needs to be secured (i.e. encrypted).

Telecommunications pathway The hand-held will need connection to a GPRS service, and onward routing to the server at CHIME via UCL Computer Science.

QoS The need here is primarily for reliability of connection. The data are character based and performance or bandwidth are not of concern.

Intended demonstration It is intended to demonstrate this GPRS access from test-bed locations in Ipswich and London (provided by BT) and later from Berlin (provided by DTAG), using 6WINIT CHIME clinical staff in lieu of real users. A more forward-looking demonstration is also intended using UMTS facilities at the Ericsson "Kista Ring": CHIME and Ericsson staff (mimicking real emergency clinicians) will access medical summary information using a PDA or mobile phone from within the Kista shopping centre.

2.1.2 Hospital outpatient access to patient's medical summary

Clinical information requirement The cardiologist or nurse specialist needs to add, review or update the basic medical summary of a patient attending a cardiac outpatient clinic, accessing the record server based at CHIME. A web-based (html) application is being developed for this.

Device and location They will need to use the existing networked PC workstations situated in the Whittington hospital. There is no mobility requirement.

Security The user will already be authenticated (by the hospital), and a trustworthy mechanism needs to be established for their user profile to be forwarded with their data request. The connection needs to be secured (i.e. encrypted).

Telecommunications pathway The workstations, connected to a legacy IPv4 network inside the wider NHSnet, will need to access the CHIME IPv6 server via an NHSnet managed gateway to the public Internet.

QoS The need here is primarily for reliability of connection. The data are character based and performance or bandwidth are not of concern.

Intended demonstration It is intended to demonstrate this legacy access actually from the Whittington Hospital, by clinical staff users of equivalent real applications.

2.1.3 Patient access to their medical summary and personal health diary

Clinical information requirement Patients may wish to review their basic medical summary as it is held by their GP or hospital. They may wish to add information about their present symptoms or to record the results of period home monitoring tests. The records will need to be accessed from the CHIME record server, potentially from any public location including the home or place of work. A web-based (WAP) application is being developed for this.

Device and location For simplicity and in view of the likely availability of such devices, it is proposed that they should view or edit their record using a hand-held device. For the present, it has been agreed that they will not be able to roam while connected but in the longer term such roaming access may be desirable to some classes of citizen.

Security The user will need to be authenticated and verified (e.g. via token and PKI), and their connection needs to be secured (i.e. encrypted).

Telecommunications pathway The hand-held will need connection to a GPRS service, and onward routing to the server at CHIME via UCL Computer Science.

QoS The need here is primarily for reliability of connection. The data are character based and performance or bandwidth are not of concern.

Intended demonstration It is intended to demonstrate this GPRS access from test-bed locations in Ipswich and London (provided by BT) and Berlin (provided by DTAG), using 6WINIT CHIME clinical staff in lieu of real patients.

2.1.4 Hospital outpatient access to cardiovascular applications

Clinical information requirement The cardiologist or nurse specialist needs to add, review or update the medical record of a patient attending a cardiac outpatient clinic, accessing the record server based at CHIME. A web-based (html) application is being developed for this.

Device and location They will need to use the existing networked PC workstations situated in the Whittington hospital. There is no mobility requirement.

Security The user will already be authenticated (by the hospital), and a trustworthy mechanism needs to be established for their user profile to be forwarded with their data request. The connection needs to be secured (i.e. encrypted).

Telecommunications pathway The workstations, connected to a legacy IPv4 network inside the wider ***NHSnet***, will need to access the CHIME IPv6 server via an **NHSnet** managed gateway to the public Internet.

QoS The need here is primarily for reliability of connection. The data are character based and performance or bandwidth are not of concern.

Intended demonstration It is intended to demonstrate this legacy access actually from the Whittington Hospital, by clinical users of equivalent real applications.

2.1.5 Ward (bedside) access to cardiovascular applications

This scenario is identical to 2.1.4 above, except that the clinical staff need to use a tablet-style device to access the same cardiovascular applications at the patient's bedside, connected via WLAN.

Intended demonstration As there is no WLAN provision in the hospital as yet, this access will be simulated using a conventional laptop connected to the WLAN at the UCL Computer Science Department. This will be an IPv6 connection, thereby demonstrating a future rather than legacy technical scenario for this kind of access.

2.1.6 Access to cardiovascular applications from a patient's home

This scenario is identical to 2.1.4 above, except that the clinical staff need to use a tablet-style device to access the same cardiovascular applications at the patient's bedside, connected via WLAN.

Intended demonstration A secure dial-up connection to the Whittington Hospital communications server will permit the laptop to be logically part of the Hospital Intranet

2.1.7 Hospital outpatient access to cardiovascular investigation results

This scenario is still being considered, and would involve extending the scope of the cardiovascular applications to include multimedia investigation results such as ECG and Doppler ultrasound studies. This scenario is more complex because the original data will reside inside the hospital, and is not presently available in the form of anonymised records that could be used in a demonstration. The main benefit of this scenario would be to challenge the technical architecture from the bandwidth perspective. This challenge is at the heart of another 6WINIT demonstrator site in Tübingen.

2.2 Technical Architecture

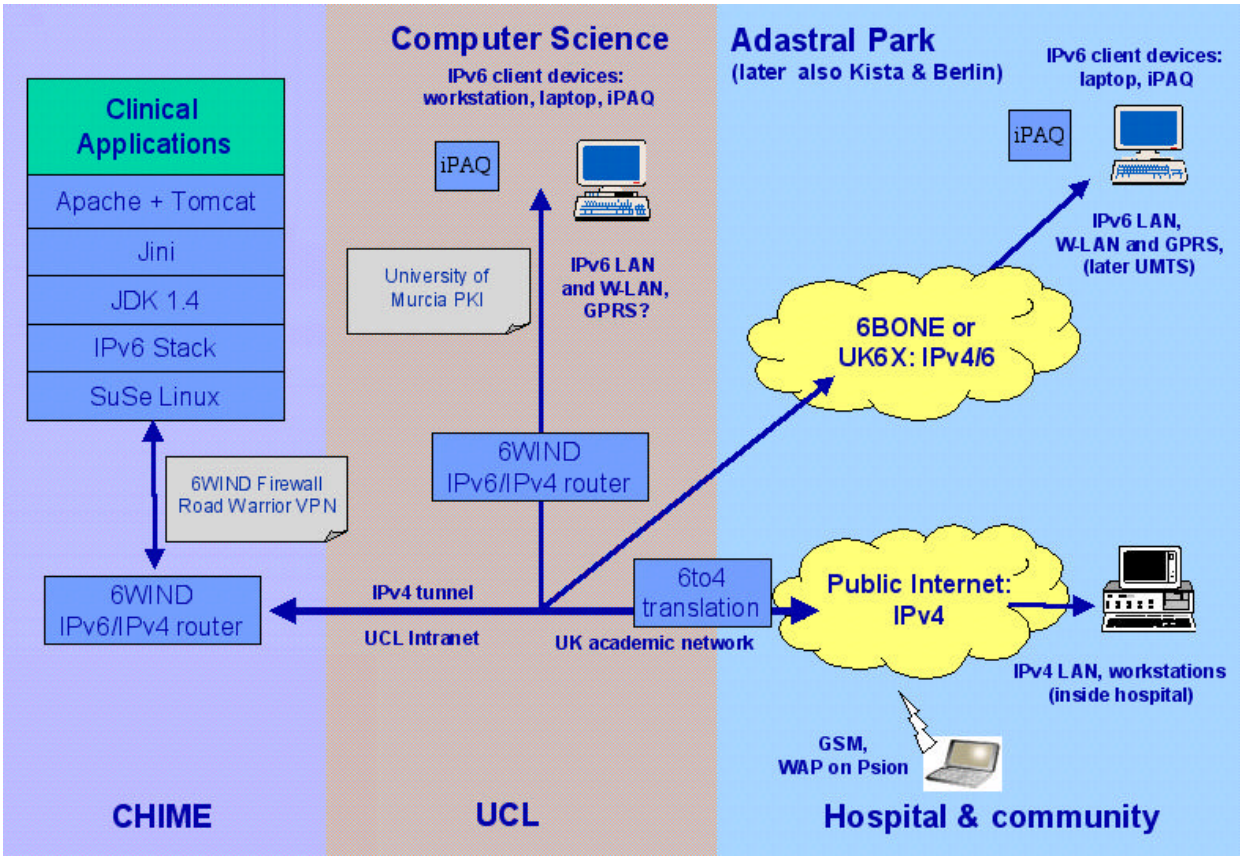


Figure 1: Network architecture of the London demonstrator site

Figure 1 above shows the principal clinical application (health record) services, located at CHIME, being delivered via an IPv6 stack infrastructure, communicated to UCL Computer Science and routed forward to the public Internet and to 6BONE or UK6X.

The communications pathway involves the use of some IPv4 networks, such as the UCL Intranet connecting CHIME in north London to Computer Science in central London, and the public Internet. IPv6 networks exist within UCL Computer Science, including WLAN, and at nominated wireless demonstrator locations in London (GPRS, provided by BT), Adastral Park (Ipswich), Berlin (GPRS, provided by DTAG) and Kista (UMTS, provided by Ericsson).

IPv6 transition mechanisms are an important component of this demonstrator, since each scenario described above will need at minimum to utilise one IPv6/IPv4 tunnel for the UCL Intranet. Hospital staff (scenarios 2.1.2, 2.1.4 and 2.1.5) will require translation to enable IPv4 “legacy” access from existing devices and networks.

Security requirements include end-`user authentication, certificate handling, and encrypted data flows. In practice, it has been agreed that the demonstration will only use pseudonymised data to permit the gradual introduction of security measures independently of other aspects of the 6WINIT network architecture. As the number of demonstration users will be limited, a full PKI is not required; instead a simpler manual certification mechanism will be utilised. Weak authentication (using only user passwords) might also be accepted as an interim measure. For encryption and firewall protection IPSec tunnels have been proposed to create a VPN; this will ideally be demonstrated both for fixed IP and Mobile IP scenarios.

2.3 Technical Component Descriptions

Note: this section draws on previously published material in 6WINIT Deliverables 1 and 2, and new Deliverables 8, 9 and 10. References are given to additional technical descriptions in these deliverables, using the notation style [D1 Section x.y.z].

2.3.1 IPv6 Transition Mechanisms

2.3.1.1 **Tunnelling**

Functional Requirement

Native IPv6 services from the main application server will need to be tunnelled via IPv4 from CHIME (north London) to Computer Science (central London) using UCL's main University Intranet. Additional tunnel(s) may be required for remote connectivity to other IPv6 islands via 6BONE.

Proposed Technical Solution: 6WIND IP Edge Device

The 6WIND IP Edge Device implements the v4-v6 migration mechanisms over a dual stack entirely developed by 6WIND. Several types of tunnels are available, especially 6in4, 4in6 and 6to4. This dual stack also integrates IPv6 features such as DiffServ and IPSec. [D1 Section 6.5.2.3, D2 Section 2.2.1, D9 Section 2.2.2]

One Edge device will be configured and installed at CHIME, and another at UCL Computer Science. It is not yet clear if 6WIND will be the Edge Device provider at other 6WINIT site locations.

Outstanding Issues - none

Industrial Benefit

This installation provides proof of concept validation of the IPv6/4 tunnelling mechanisms within the Edge Device.

2.3.1.2 **Translation**

Functional Requirement

a) IPv6 to 4 translation may be required to permit hand-held (PDA) access to the native IPv6 services via GPRS.

b) Some scenarios involve users having access to the native IPv6 services using IPv4 clients from within IPv4 networks (e.g. from inside a hospital Intranet, accessed via an NHSnet managed gateway to the public Internet).

Proposed Technical Solution: a) BT Ultima b) 6WIND IP Edge Device

a) Ultima is a BTexact Technologies IP product that provides interworking between IPv4 and IPv6. NAT-PT (Network Address Translator - Protocol Translator) provides a translation facility between IPv4 and IPv6. Translation is bi-directional (i.e. can be initiated at either IPv6 or IPv4 host) without any modifications to either the IPv4 or the IPv6 host protocol stacks, and the operation of the translator is totally transparent to the end user. Translation is initiated via the initial DNS exchange; this requires the addition of a special DNS translator (DNS ALG) to the standard NAT-PT packet translation process. [D2 Section 2.5, D9 Section 2.6]

b) The dual stack in the Edge Device should soon include a translation mechanism that allocates a temporary IPv4 address to a dual stack host in the IPv6 network when it is required for IPv4 communication. IPv4 user devices will access clinical applications via this temporary IPv4

address rather than the IPv6 address of the main clinical server. [D2 Section 2.1.1]
Outstanding Issues Interoperation between 6WIND and BT Ultima devices
Industrial Benefit This installation provides proof of concept validation of the translation mechanisms within the 6WIND Edge Device and BT Ultima.

2.3.2 Security Mechanisms

2.3.2.1 VPNs using IP Routers

Functional Requirement

To provide an encrypted channel of communication between the clinical applications server and the end-user (possibly including the use of wireless devices). Certificate-based key management needs to be implemented e.g. via PKI. [D10 Section 4.1]

Proposed Technical Solution: 6WIND IP Edge Device

6WIND routers are able to create IPsec tunnels over IPv6 connections, including also the possibility of being certified by a PKI. [D8 Section 3.1.1, D10 Section 4.2]

The 6WIND IP Edge Device supports IPSec and IKE functionality compliant with the corresponding RFCs. Different configurations can be accommodated: IPSec with static keys; IPSec with IKE pre-shared keys; IPSec with IKE certificates. All the security features proposed in the IP Edge Device are available for the both IPv4 and IPv6 versions with similar management interfaces. [D2 Section 3.2.1]

Because IPSec VPNs are complex to configure, 6WIND provides a management tool called Network Management System (NMS). [D1 Section 6.1.1, D2 Section 3.2.1.2]

6WIND provides a tool to produce and manage certificates. This tool could be sufficient for small or medium configurations. [D2 Section 3.2.1.3]

UCL-CS also has experience of using the Public Key Infrastructure of the University of Murcia, based on the design and implementation of a complete and robust group of IPv6-enabled certification services. The interoperation of this PKI with the 6WIND Edge Device will also be explored. [D10 Section 4.1.3]

The key management methodology for the demonstrator will be decided later, balancing the practical needs to provide a small and stable number of certificates with the wish to demonstrate a realistic and scalable scenario. A VPN will be established between CHIME and UCL Computer Science, to users connected via fixed LAN and WLAN. Ideally the VPN will extend to remote users connected via the Internet both using a fixed address and using GPRS.

Outstanding Issues

How to establish a VPN through to fixed and mobile users using native IPv4 devices connected via the public Internet (and possibly GPRS).

Industrial Benefit

Proof of concept verification of the Edge Device IPSec functionality and demonstration of a secure infrastructure for future adoption by regional health care networks.

2.3.2.2 Road Warrior

Functional Requirement

To provide an authenticated and encrypted channel of communication between the clinical applications server and the end-user specifically supporting the use of mobile devices connected via GPRS or UMTS. Although PKI certificate-based security will be needed in real deployment situations, authentication using a pre-exchanged (public) RSA key would be the preferred method for a demonstration.

Proposed Technical Solution: IABG in partnership with 6WIND

IABG and 6WIND will collaborate to validate a mechanism to support the authentication and certificate/key management approach for mobile users whose IP address is allocated only at the time of connection. [D8 Section 3.2]

Outstanding Issues - none

Industrial Benefit

The collaboration will verify a technical approach that could inform IETF on potential modifications to IPSec to support Mobile IP. Component interoperability between IABG and 6WIND might lead to other future collaborations.

2.3.2.3 **Firewall**

Functional Requirement

The CHIME-hosted clinical applications server (running SuSe Linux 7.2) needs to be protected from hostile attack including unauthorised access and denial of service attack.

Proposed Technical Solution: 6WIND IP Edge Device

The 6WIND IPSec VPN will limit access to authorised users and from known IP addresses (the Mobile IP scenario is a specific exception, to be protected separately). This will provide firewall protection by way of packet filtering.

The 6WIND Edge Device provides IPv4 and IPv6 Packet Filtering mechanisms that have been recently implemented and that are available in version 4.1. This Firewall functionality is used to protect local networks when they are interconnected with non-secure networks, like Internet. [D10 Section 4.3.1]

Outstanding Issues

Mobile IP security measures will need to be managed separately

Industrial Benefit

This feature is an important “by-product” of the VPN, as a demonstrated security solution for regional health networks.

2.3.3 Mobile IPv6

2.3.3.1 MIPv6 Home Agent

Functional Requirement

Users need to be able to reliably connect to the clinical applications server from a mobile (non-roaming) device whose Care of (IP) Address is dynamically provided by an ISP or other foreign network. [D8 Section 2, D10 Section 2.2.1]

Proposed Technical Solution: 6WIND IP Edge Device

A native IPv6 mobility is included in a prototype of the IP Edge Device, though this function is not currently included in commercial version of the IP Edge Device. The "Home Agent" functionality is implemented according to the IETF draft [Joh01]. Like the implementation of other providers, all the aspects have not yet been taken into account mainly because they are not well defined at the moment. [D2 Section 4.1.1, D2 Section 4.2.1, D1 Section 7.3, D8 Section 2.2.3, D10 Section 2.3.4].

The practical demonstration of this will be considered later in the project.

UCL-CS is also prototyping Helsinki University's mobile IPv6 stack implementation (www.mipl.mediapoli.com) on the mobile hosts, since this is widely believed to be amongst the most progressive work on mobile IPv6 stacks. [D8 Section 2.2.1]

Outstanding Issues

This function is work in progress.

Industrial Benefit

6WIND will study how to add security over the mobility and will see if the privileged location at the boundary of the network can be exploited by the Edge Device to solve the problem of security and mobility. [D2 Section 4.2.2.1]

2.3.3.2 802.11b Access

Functional Requirement

Users need to be able to reliably connect to the clinical applications server from a wireless LAN, using a laptop, hand-held or tablet device.

Proposed Technical Solution: 6WIND IP Edge Device

The 6WIND IP Edge Device can be used at the border between wired and wireless networks. WLAN technology like 802.11b has been tested and proved to be compatible with IPV6 networks…. The Aironet kit from Cisco has been used in the preliminary experiments. [D2 Section 4.2.1.2]

The deployment of the Edge Device to enable WLAN users to access the CHIME clinical applications will build on early work carried out at UCL in the ANDROID project.

Outstanding Issues

This function is work in progress.

Industrial Benefit

To verify that the 6WIND IP Edge Device is suitable to act as a wireless gateway (D2 Section 4.2.2.2]. 6WIND also wish to verify their 802.11b solution with Lucent WLAN.

2.3.3.3 **GPRS**

Functional Requirement

Users need to be able to reliably connect to the clinical applications server from a mobile (non-roaming) hand-held device. This will include the need for wireless access via GPRS.

Proposed Technical Solution: 6WIND IP Edge Device

This is very new (emerging) functionality within the 6WIND Device, and its demonstration will be confirmed later in the project. [D1 Section 4.1.2.2, D2 Section 4.2.1.2] It will ideally be verified eventually at the 6WINIT partner GPRS test-beds in Ipswich and London and Berlin.

Outstanding Issues

This development work is in progress. Router compatibility (e.g. 6WIND/Ericsson-Telebit) will need to be verified in order to confirm that these demonstrations are feasible.

Industrial Benefit

One of the main objectives for 6WIND in the scope of the 6WINIT project is to integrate in the IP Edge Device new wireless interfaces like GPRS and UMTS for the WAN side… [D2 Section 4.2.2.2]

2.3.4 QoS

2.3.4.1 TAG

Not required at this site

2.3.4.2 JMF

Not required at this site

2.3.4.3 DiffServ

Functional Requirement

The proposed London user scenarios place only a limited demand for QoS functionality, primarily for reliability. However, future planned clinical applications will include the use of multimedia data requiring high bandwidth and high performance capability, so an opportunity to test this could be engineered.

Proposed Technical Solution: 6WIND IP Edge Device

The 6WIND IP Edge Device implements the standard mechanisms and is compliant with the "RFC 2475 Architecture for Differentiated Services". It implements flow classification, queues management and scheduling mechanisms. All the QoS mechanisms of the Edge Device can be applied on the two versions of IP, IPv6 and IPv4. [D1 Section 2.2.1, D2 Section 5.2, D10 Section 5.1, D10 Section 5.1.2]

The 6WIND Edge Device implementation of DiffServ allows interoperability with IPSEC/IKE functions and Migration mechanisms (tunnels) also provided by this equipment. [D10 Section 5.1.2.3]

Plans for exploiting this in the demonstrator will be considered later.

Outstanding Issues – none

Industrial Benefit

To be confirmed

2.3.5 Signalling Gateways – SIP

2.3.5.1 SIP

Not required at this site

2.3.6 Multimedia Conferencing Gateways

Not required at this site

2.3.7 WAP Gateways

Functional Requirement There is considerable attraction to making a patient's medical summary available to them using a WAP phone or a PDA using a WAP connection, since this is present-day and widely-available technology. However, there may be secondary benefit in showing the advantage of Mobile IP as a successor to WAP if both options are capable of demonstration.
Proposed Technical Solution – to be confirmed During clinical application development at CHIME a commercial ISP will be used as the WAP provider to enable rapid testing of the basic screen design and to establish performance. An independent WAP gateway has been recommended by the 6WINIT partners [in D2 Section 8.5] as a means of enhancing security (many commercial WAP providers cache customer WML pages for some days before deletion, which may not be secure). The Krakow (Poland) site has indicated an intention to pursue a secure WAP solution, and their experience will be sought before confirming the approach of the London site.
Outstanding Issues Unknown as yet
Industrial Benefit To the 6WINIT partners, the benefit may be in showing the limitations of what can be achieved with WAP!

2.3.8 Access Network Provision

2.3.8.1 GPRS

Functional Requirement

Wireless GPRS network access is required to demonstrate the "roadside" access to clinical applications. In practice this will be simulated from GPRS test-bed locations.

Proposed Technical Solution

1) The BT GPRS test-bed located at Ipswich and London (UK)

2) The DTAG GPRS test-bed located at Berlin (Germany)

Additional test locations might become available towards the end of the project. However, the above sites will be sufficient to provide proof-of-concept verification.

Outstanding Issues

The availability of GPRS cards ("mobile modems") for each client and drivers for each operating system.

Industrial Benefit

Demonstration of the value of GPRS for the rapid and reliable retrieval of health information via wireless, to help stimulate a health care market for such solutions.

2.3.8.2 WLAN

Functional Requirement

Wireless (WLAN) network access is required to demonstrate the "bedside" access to clinical applications. Although IPv4 WLAN is becoming prevalent now, in the future this is likely to be IPv6. In 6WINIT this kind of access will be simulated from the IPv6 WLAN network at UCL Computer Science.

Proposed Technical Solution

The Lucent Orinoco Wireless LAN and Cisco's Aironet WLAN architectures are described in D1 Section 5.1.

The Wireless 802.11b LAN operational at UCL Computer Science will be the primary test location for the London demonstrator. Secondary connection to other islands of wireless access at other partner sites may be attempted later, possibly utilising 6BONE (see below) or 6NET.

Outstanding Issues – none

Industrial Benefit

Demonstration of an IPv6 wireless methodology suitable for use inside hospitals in the vicinity of medical devices.

2.3.8.3 IPv4 WANs

Functional Requirement

IPv4 WAN is required to demonstrate hospital-based access to the IPv6 clinical applications using legacy networks. In practice this will be routed from UCL Computer Science to the Public Internet, and accessed from inside NHSnet via a managed firewall.

Proposed Technical Solution

Clinical application web services routed from CHIME via UCL Computer Science and the JANET national academic network to the Internet and the NHSnet. 6WIND translation mechanisms have been described above. Security provisions described above might not be fully implementable when using IPv6to4 translation.

Outstanding Issues

The NHS firewall may not permit IP access to the CHIME demonstration server. If this is a problem alternative Internet locations will be used to simulate hospital-based access.

Industrial Benefit

Demonstration of a viable migration approach, and of rigorous IP translation mechanisms.

2.3.8.4 **IPv6 WANs**

Functional Requirement

Native IPv6 distributed access is required to validate the future scenario of widely available IPv6 networks within hospitals. In practice this will be demonstrated within UCL Computer Science using local IPv6 networks, and from fixed connections at other clinical sites such as RUS (Stuttgart), via 6BONE.

Proposed Technical Solution

The UCL IPv6 LAN is well-established, and is connected to the UCL Intranet. With the use of 6WIND IP Edge Devices (described in earlier sections of this report) the CHIME and Computer Science IPv6 islands will be connected through an IPv4 tunnel. This will be in turn connected to the IPv6 LAN at RUS in Germany, via 6BONE. This tunnelled interconnection of IPv6 islands will simulate a homogenous IPv6 WAN.

Outstanding Issues – none

Industrial Benefit

Demonstration of a migration solution that would permit distributed organisations to upgrade their sites to IPv6 without loss of organisation-wide connectivity.

2.3.8.5 **UMTS**

Functional Requirement

Wireless UMTS network access is required to demonstrate the next-generation “roadside” access to clinical applications. In practice this will be simulated from a UMTS test-bed location.

Proposed Technical Solution: Ericsson “Kista Ring”

The routing of network traffic via 6BONE described above can be extended to include the UMTS test-bed near Stockholm (Sweden).

Outstanding Issues

To be identified later

Industrial Benefit

Provide proof-of-concept verification of UMTS access to web-based application services, as market stimulation. Ideally the demonstration will highlight the benefits of UMTS over GPRS.

2.3.9 Access Devices

2.3.9.1 Terminals

Functional Requirement

The various London user scenarios require four different user access devices.

1) an IPv4 desktop workstation, running a web browser

2) an IPv6 desktop workstation, running a web browser

3) a laptop simulating a tablet client, running a web browser

3) a hand-held device, such as a PDA, running a web browser (both IPv4 and IPv6 versions)

Proposed Technical Solutions

Compaq iPAQ: running Linux, IPv4/IPv6 and a web/WAP browser, with a wireless GPRS connection (or UMTS, in Stockholm) or a Wireless LAN connection.

Laptops: running Linux or other operating systems, IPv6, with fixed Ethernet or Wireless LAN connection.

PC: various platforms, running IPv4 or IPv6 or dual stack, a browser, with connection either to IPv6 LAN or IPv4 LAN within a legacy environment.

All the mobile devices (iPAQ and laptop) will require a mobile IPv6 stack. Currently development is being done by the 6WINIT partners with the University of Helsinki's Mobile IPv6 stack (HUT) which is explored in Deliverable 10. The basic functions have been used with both laptops and iPAQs.

Outstanding Issues

IPv6 operating systems and browsers supporting IPSec are not yet available for all devices.

Industrial Benefit

A spectrum of devices is important to show the compatibility of 6WINIT solutions with a wide range of user needs.

2.3.9.2 Security Devices

Functional Requirement

The ideal requirements are for strong authentication and user certification (including access control role-based profiles). A comprehensive security solution would add credibility to the overall 6WINIT technical architecture.

Proposed Technical Solution: PKI's and Smart Cards

Certificate handling has been described above. Coupling the proposed architecture with strong authentication tools (e.g. using tokens or biometric devices) would be ideal.

Outstanding Issues

This may add an unnecessary complexity to the demonstrator

Industrial Benefit

This needs to be confirmed, since the demonstration of these security tools themselves is not the focus of 6WINIT.

2.3.10 Location Awareness

Not required at this site

2.4 Clinical Applications

The primary CHIME clinical application services are a set of middleware components providing controlled access to patient electronic healthcare records (EHRs). Access to these EHRs is provided through a set of web-based applications, each written as Java Servlet scripts executing on the same server as the middleware components. The persistent repositories are themselves distributed within a local area network and accessed by the middleware components using Jini. This overall component architecture has been described in 6WINIT Deliverable 3. The technical configuration of the main server running these components, and serving them via IPv6, is summarised in Section 1.1 of this Deliverable.

Three sets of clinical web applications are under development:

1. Medical summary for hospital care (web browser version)

2a. Medical summary for emergency care (PDA version)

2b. Medical summary and personal diary for patient use (PDA version similar to 2a above)

3. Outpatient clinic application for chest pain and heart failure management (web browser version).

Each of these applications is briefly summarised below, and illustrated using some real screen captures and some mock up screens (as this is work in progress). A previously-developed web application for anticoagulant therapy management was described in Deliverable 3. This is running live at the Whittington Hospital and available as a demonstration application from CHIME to permit early testing of the server configuration whilst the new web applications are being developed.

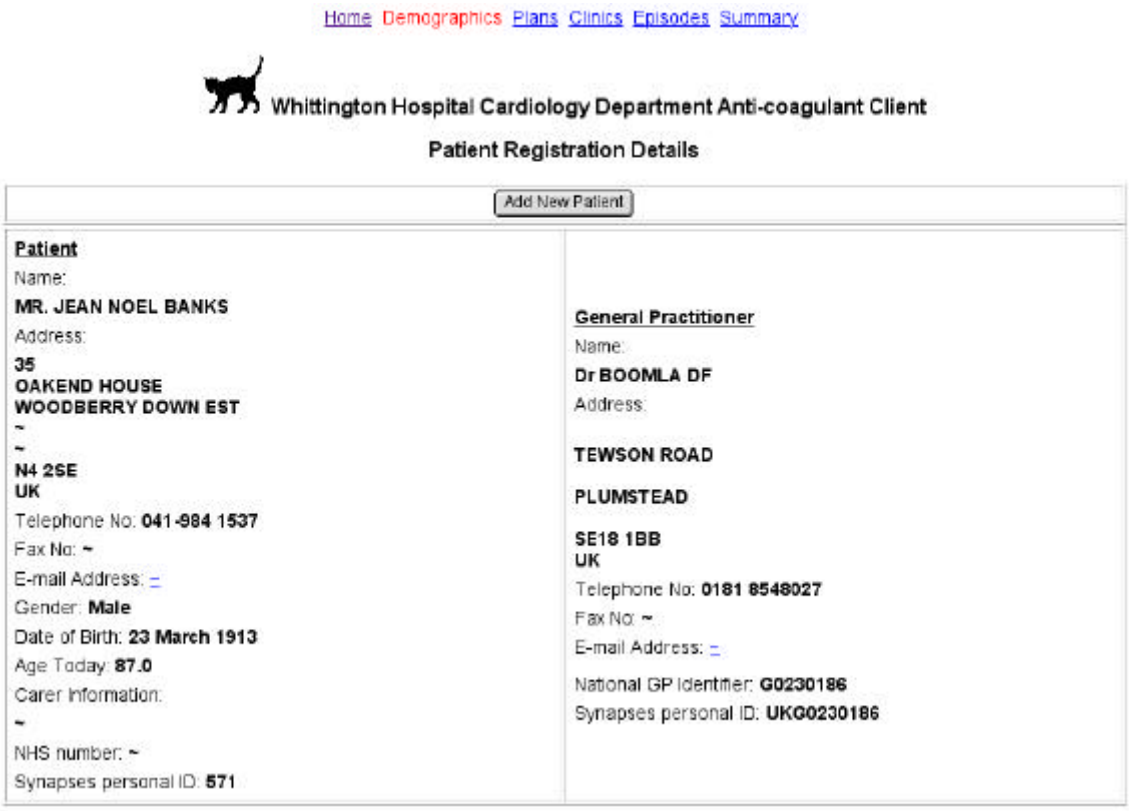
These applications focus on the collection and presentation of health record information, and are not intended to act as an internal departmental system to manage clinic sessions, human or other material resources. The focus of these applications is the support of clinical interactions with the patient's record in an electronic form, for which secure distributed access is of clinical value.

Some elements of the cardiovascular record are being designed in parallel with General Electric / Marquette, relating to the capture of multi-media investigations.

Certain initial screens, such as user log in and patient search screens have been omitted here but are already complete. Some of the screens are presented as tables where a final screen-captured version is not yet ready. Please note that in this document, table font sizes and column widths have been varied to try to keep the tables tidy-looking, and have no design significance.

2.4.1 Medical summary for hospital care (web browser version)

2.4.1.1 Demographics



Consultant cardiologist name	{local drop-down list}
Usual Clinic Location	{local drop-down list}
Transport required	{leave blank if none}

Ethnicity

OPCS category	{British A, Irish B, Other C, White and Black Caribbean D, White and Black African E, White and Asian F, Any other mixed background G, Indian H, Pakistani I, Bangladeshi K, Any Other Asian Background L, Caribbean M, African N, Any other Black background P, Chinese R, Other S, Not Stated Z}
Ethnicity description	{text}
Language spoken if not English	{text}

2.4.1.2 Medical Summary

Several tables all on one scrolling screen. All tables will have the ability to edit an individual row (formal revision process) or to add a new entry (row). Sort order will be on date added in descending order (most recent at the top) unless proposed otherwise below. Many of these summary tables have a fairly rich set of columns, which would not be filled in on every occasion.

Nota Bene

Date	Nota Bene
	{text box}

This is a set of dated text boxes for critical information that any clinician should know when they see the patient. This section could include patient wishes for things like resuscitation policy.

Allergies

Date added	Allergen name	Reaction	Emergency treatment	Precautions to take
date	text	Text	Text	text

Clinical Conditions

Date added	Condition name	Date of onset	Date ended	Current Problem	Current concerns
date	Drop-down list to be confirmed	date	Date	{Y/N}	text

Although a drop-down box will initially limit this table to cardiac conditions, the wider use of the record server may in the long-term mean that other disciplines share this part of the record. It will be important for a whole person perspective to be retained, but also to permit a focus on cardiology for this clinic. If the diagnosis changes over time as more information about patient emerges, the user will have two options:

- to revise the original entry if it now appears to be inappropriate (the original entry will be hidden, but retained in the audit trail), or
- to edit the entry and give it an end date with a comment stating that the condition has evolved, and to create a new entry with the new diagnosis.

Excluded Conditions

Date excluded	Condition name
Date	Drop-down list as above

There seems little point in offering any richer data-set for excluded conditions. Clearly, though, entries can be deleted if the condition subsequently occurs!

Family Conditions

Date added	Condition name	Relationship to patient	Date of Birth	Age today (yrs)	Age at onset (yrs)	Age at death (if appropriate)	Significance
Date	Text	text	date	calculated	numeric	numeric	text

Lifestyle information

Date recorded	Date began	Date ended	Lifestyle item	Amount	Description	Education or advice given
Autofilled today	date	date	Drop-down e.g. smoking, alcohol, occupation, exercise	Text e.g. 12 units/week, 20/day, swimming, piano tuner	text	Text (one day a patient screen might also include a URL)

Optionally sort this table on date ended (to show active lifestyle items first i.e. with no end date, then those in the recent past) or on lifestyle item then date ended (to show trends in smoking, occupation etc over time). The benefit of this table is the consolidated and flexible approach to capturing any kind of lifestyle information. The downside is that the amounts etc. will be free text.

Social services and special needs

Date recorded	Service or need	Date started	Date ended	Comments
date	Text	date	Date	text

2.4.1.3 Medication and prescriptions

Date added	Indication	Drug name	Description of: Strength, units, formulation, route and frequency	Date commenced	Quantity usually prescribed	Any problems, side effects	Date discontinued
		May also be coded: Read, Multilex, BNF ?	As free text for now				

Table could be sorted on date discontinued, then date commenced to show recently-prescribed active medication first, or on date discontinued then indication to permit grouping of active drugs by clinical use.

Drug name could initially be free text or a drop-down list of common cardiac and diabetes drugs. I would favour a drop-down list with ability to then manually put in dose, frequency etc.

2.4.1.4 Investigation results

Completed tests

Date	Procedure Test	Indication	Value Result	Details	Interpretation	Reference or URL
date	text	text	text	Text	text	Later, could be a hyperlink to CARDDAS or a Path lab record system

The URL column is a placeholder for a dynamic link to multimedia investigation reports derived from GE acquisition and reporting equipment.

2.4.1.5 Education and Self-management

Date	Topic	Areas covered	Materials given	Self-management goal	Outstanding issues
Date	text	text	text	Text	text

2.4.2 Medical summary for emergency care (PDA version)

PDA screens will be needed for user log-in and searching for patients using a PDA.

Two variants of the PDA summary are being developed: one for emergency clinicians and one for patients. The results of a patient search might take the user to a differently structured patient home page (the root of their "PDA summary record") depending on their role (patient or clinician).

EHR Summary home page Fred Bloggs (18 Sep 1956)	
Nota Bene Demographic Medical Summary Medication Investigations	
Patient search	Logout

The patient PDA view would have two additional links, and no Nota Bene:

Patient Record Summary home page Fred Bloggs (18 Sep 1956)	
Demographic Medical Summary Medication Investigations Self management plan Patient diary	
Patient search	Logout

The demographic detail screen could be similar to upper (main) portion of the desktop equivalent, but with GP details below the patient details to enable this to fit.

The PDA medical summary views will display the same data as the desktop views, but are accessed via an intermediate screen summarising the key entries "at a glance". This should enable rapid overviews to be gained in an emergency setting whilst permitting "drill down" to the full data-sets.

Medical Summary Fred Bloggs (18 Sep 1956)		
Allergies Penicillin Elastoplast Conditions Heart failure Diabetes Mellitus Nephropathy Excluded conditions Tuberculosis Family history Hypertension Diabetes Mellitus Lifestyle factors Smoking = 20.day Alcohol = nil Occupation = Psychologist Social services & needs Meals on wheels Needs wheelchair Self management plan Urine check for sugar, daily Weekly weight		
Patient search	Patient home	Logout

Notes

Allergies: display all allergen names, in reverse date order (most recent first)

Conditions, all condition names with Date Ended = Null, in reverse date order

Excluded conditions: display all condition names, in reverse date order

Family conditions: display all condition names, in reverse date order

Lifestyle factors: display each Lifestyle Item then <*space*<>*equals*<>*space*> then most recent content value of Amount (if possible! If not then all instances sorted by Lifestyle Item then by date)

Social service & need: Service or Need with Date Ended = Null, in reverse date order

Self management plan: all instances of Topic and Self Management Goal, sorted in reverse date order

Hyperlinks take you to a detail screen, following a standard pattern for all the PDA detail screens, illustrated with Allergies below.

Allergies (2) Fred Bloggs (18 Sep 1956)		
Penicillin Reaction = **Skin rash** Emergency treatment = **Oral antihistamines** Elastoplast Reaction = **Skin rash** Emergency treatment = **Calamine lotion** Precautions to take = **Use Micropore**		
Patient search	Patient home	Logout

Similarly for condition, excluded condition, family conditions, lifestyle information, social services. Blank entries (e.g. Penicillin has no Precautions to take) are not shown, to save space.

Medication Summary Fred Bloggs (18 Sep 1956)		
Bendrofluazide Ventolin Aspirin Allopurinol		
Patient search	Patient home	Logout

Drug names in reverse date order. Hyperlinks take you to the relevant detail screen for that drug.

Investigation Summary Fred Bloggs (18 Sep 1956)		
1.09.2001 Full blood count Result summary = **Normal** 21.08.2001 Chest x-ray Result summary = **left pleural effusion**		
Patient search	Patient home	Logout

Investigations sorted in reverse date order. Top line of display (hyperlink to detail) is date plus Procedure Test name. Result summary value taken from Value Result.

Self Management Plan – no need for an intermediate level summary: go straight to the detail screen

Patient Diary The diary will comprise Date, Topic (free text) and Narrative (free text). To be consistent with other views reverse date order would seem best. The main difference from the other PDA screens is that the patient can make new entries. At present this particular table is not intended in parallel for the desktop view.

2.4.3 Application for chest pain and heart failure management

2.4.3.1 Cardiovascular service referral

Recording date/time	{date time}
Clinic type	{Chest pain, heart failure, OPD, etc.}
Referral source	{Patient's GP, A&E, ward, …?}
Date on the referral letter	{date}
Indication for referral	{text or drop-down list?}
Referral received: via	{post/fax/e-mail/phone/via-patient}
On	{date}
Date of first appointment	{date/time}
Reason for any subsequent postponement	Drop-down list to be confirmed

Hyperlinks to previous referral pages for this patient

DNA Management

Date	Date of appointment	Clinic type	Reason for DNA	Actions taken	Now due to be seen on:
date	date	Anticoagulant etc. (drop-down?)	text	Text	Date/time

2.4.3.2 Cardiovascular Presentation

Date	Default to today's date
Contact with	{user name from login screen info?}
Type of consultation	{local or generic drop-down list?}
Location of consultation	{local or generic drop-down list?}
Episode name	{text}
Background information	{ large text box}
Cardiovascular symptoms	
Chest pain/discomfort symptoms?	{yes,no}
Approximate month of initial onset	{mm/yyyy}
Description of chest discomfort	{large text box}
Heart failure symptoms	{large text box}
Other cardiac symptoms	{large text box}
Respiratory symptoms	{large text box}
Other symptoms	{large text box}
Angina checklist	
Canadian angina score	{I, II, III, IV}
Heart failure checklist	
No of previous admissions with HF	{number, default zero}
Date of most recent admission	{dd/mm/yyyy}
Planned date of discharge (if an inpatient)	{dd/mm/yyyy}
NYHA Class	{I, II, III, IV}

Hyperlinks to previous cardiovascular presentation pages for this patient

The large text boxes are intended to provide the user with an open environment to record positive or important features of the symptoms. We have presently avoided introducing a specific set of boxes separately to capture chest pain location, radiation, duration, severity, precipitating or aggravating factors such as exertion or eating, relieving factors such as GTN etc.. If a checklist is useful, this could be added above the box as a textual checklist and not necessarily presented as a highly structured template.

Similarly, the heart failure symptom checklist could be added as a text prompt for breathlessness, orthopnoea, PND, palpitations, dizziness, chest pain, syncope & pre-syncope, fatigue, cough.

In general, templates take longer to complete and make the screens look busy, and should be used when most items will have an important value (e.g. the examination screen below).

2.4.3.3 Cardiovascular Examination

Cardiovascular Examination	Current values "Please repeat if the same as last time"	Most recent past values	Past values	etc
Date	{greyed out, as date already above)			
Height (m)	numeric			
Weight (Kg)	numeric			
"Calculate BMI" button	Fills in: height/(weight squared)			
Respiratory rate (per min)	numeric			
BP: systolic	numeric			
BP: diastolic phase 4	numeric			
BP: diastolic phase 5	numeric			
Clinically anaemic	{yes / no}			
Stigmata of hyperlipidaemia	{none, corneal arcus, xanthoma, xanthesalma}			
Chest wall tenderness	{present / absent}			
Oedema extent	{none, ankles only, below knees, to the knees, above knees, sacral oedema, anasacra}			
JVP height (cm)	numeric			
Carotid pulse rhythm	{regular, regular with ectopics, totally irregular}			
Carotid pulse character	{normal, weak, collapsing, slow-rising}			
Apex Beat	{normal, displaced, impalpable}			
Peripheral Pulses	{normal, abnormal}			
Site of any arterial bruits	{text}			
Lung crepitations	{absent, bases only, beyond bases}			
Other abnormal respiratory system findings	{large text box}			
Other abnormal examination findings	{large text box}			

Heart Auscultation

Date	Murmur site	Murmur type	Added heart sound
	{apex, lower left sternal edge, upper left sternal edge, right upper sternal edge}	{ejection systolic, pan-systolic, late systolic, early systolic, mid systolic, soft systolic, short systolic}	{third, fourth, third and fourth, ejection click, late systolic click, opening snap, pericardial rub}

The above Heart Auscultation table will permit the recording of more than one murmur or added heart sound, and will also show the global history of these recordings to permit changes or new sounds to be recognised as such.

2.4.3.4 Assessment and Management

Conclusion	{large text box}
Further assessment details	{large text box}
What the patient has been told	{large text box}
Review plans	
Date	{date time}
Where	{GP/outpatients/Home visit/Admit now/By phone}
By whom	{text}
Items for review	{large text box}

Hyperlinks to previous assessment and management pages for this patient

Planned tests

Date planned	Procedure Test	When planned	Intended location	Intended actor	Indication	Planning status
date	text	Date time	text	Text	text	{Intended Scheduled Cancelled Done}

Sort table on Planning Status: reverse alphabetical order (i.e. Scheduled tests at the top)

2.4.4 Progress and intended timescale

The web applications described above are intended both as demonstrators for 6WINIT and as real operational applications at the Whittington Hospital. The data model, screen layout and functionality of the applications have all been designed in partnership with the anticipated real clinical users at the hospital, and confirmed and documented by the development team.

Java servlet development is in progress, alongside some performance and concurrency improvements in the record server middleware components themselves.

The web applications will be completed by late January, and will be tested by end users inside the hospital in parallel to establishing the 6WINIT demonstration server at CHIME. This latter demonstration will use fictitious patient records and will not therefore need to be rigorously secured. A full working IPv6 version of the components described in this Deliverable is expected by March or April 2002, with some limitations of the security features in that initial deployment.

The final phase of development from April 2002 will be the implementation of access control services closely tied to the record server itself, and the interworking with any authentication and certification services advocated by the 6WINIT technical partners.

3 KRAKOW CLINICAL DEMONSTRATOR

3.1 User Scenarios

The following access scenarios describe the various technical settings in which healthcare staff or patients may need to access medical information (radiology and personal data) and hospital medical services via 6WINIT networks. An earlier description of the Krakow clinical scenarios was published in 6WINIT Deliverable 3. Figure 2 sketches the four clinical applications at Krakow site and the nine scenarios of their usage depending on the available connectivity and end-device.

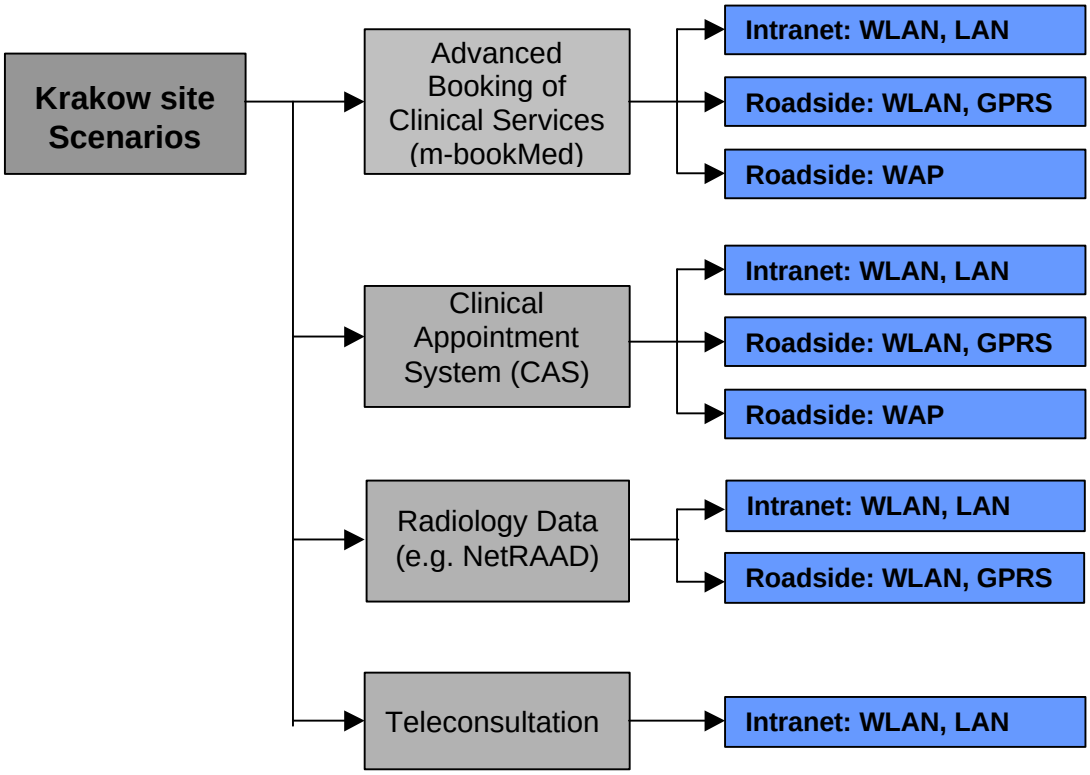


Figure 2: The nine user scenarios at Krakow clinical site

3.1.1 Hospital intranet access to advanced clinical services booking system (m-bookMed)

Clinical information requirement Hospital staff needs easy access to information on availability of the medical examination equipment and to booking examinations on this equipment, alongside with the time of personnel: doctors, nurses or helper staff operating this equipment. A possibility of entering emergency information like equipment failures, staff absence, etc. with automatic generation of appropriate messages for all parties involved (patient, doctor, nurses, etc.) is also desired. A Web-based application called m-bookMed is being developed for this purpose. It will be available throughout a wired and wireless network infrastructure for desktop PCs, laptops and PDAs (iPAQ PocketPCs).

Device and location The m-bookMed system will be installed in JP II hospital. It will be available inside the hospital's intranet from all computers connected to the hospital LAN and WLAN. There is no additional mobility requirements in this scenario.

Security All intranet users of m-bookMed will be authenticated by the hospital's LDAP-based users' database. The web browser – web server connection needs to be secured (i.e. encrypted), e.g. by means of https protocol suite.

Telecommunications pathway The desktop PCs, laptops and iPAQs will be connected to the IPv6 wired and/or wireless network infrastructure in the JP II Hospital, so they will be able to access the m-bookMed system directly over the hospital IPv6 intranet.

QoS The need here is primarily for reliability of connection. The data are mostly character based and performance or bandwidth are not of concern. Some small amount of graphics will be applied to provide a good-looking and to ease the use of web pages. The speed of both 802.11b wireless LAN and 100BaseT wired LAN is much more than the system can make use of.

Intended demonstration It is intended to demonstrate operation of the m-bookMed system over the WLAN and LAN networks in the JPII hospital.

3.1.2 Home/street multi-access to clinical services booking system (m-bookMed)

Clinical information requirement: The GP-doctor, nurse or patient needs to make, check or update the clinical services booking information for a particular patient from any public location including the patient's home or a street. A Web-based application called m-bookMed is being developed for this purpose. It will be available throughout WLAN and GPRS for laptops and PDAs (iPAQ PocketPCs) equipped with appropriate extension cards.

Device and location: When users need to view the data on a PDA, they may be kilometres away from their own place of work and then a connection via GPRS is used or they may be very close to the hospital or any other public place (e.g. an airport), where a WLAN connectivity is active. It is assumed that they will not need to roam while connected. It is planned that the GPRS connection of iPAQs will be implemented with the GISMO network adapters which can operate both on 802.11b and GPRS.

Security: All users will be authenticated by the hospital's LDAP-based users' database. A trustworthy transport mechanism needs only to be established between the server and end-user web browser (e.g. using a secure http connection like ssl).

Telecommunications pathway The PDA will be connected to a WLAN or a GPRS service. The connection between a GPRS phone and PDA may be implemented in two ways, depending of the PDA's operating system. For Linux (the only one which supports IPv6) UMM will use:

- GISMO card for IPAQ (no test with Linux done yet)
- IRDA or Bluetooth connection to the GPRS phone (no test with Linux done yet)

Tunnelling of IPv6 packets in IPv4 is envisaged as currently IPv6 connections cannot be delivered natively by GPRS.

QoS The need here is primarily for reliability of connection. The data are mostly character-based and performance or bandwidth are not of concern. Some small amount of graphics will be applied to provide a good-looking and to ease the use of web pages.

Intended demonstration It is intended to demonstrate this WLAN or GPRS access from test-bed locations in Krakow. It will be also possible to expand the demonstration to other sites if 6Bone connectivity to the GEANT IPv6 network is provided.

3.1.3 Roadside (WAP) access to the m-bookMed clinical services booking system

Clinical information requirement The GP-doctor, nurse or patient needs to check (but not change) the data held by the m-bookMed clinical services reservation system (including e.g. appointments and medical examinations booked by the patient), running on a server in the JP II Hospital, from any public location including the street. A WML-based (WAP) application is being developed for this.

Device and location They will need to view the data on a hand-held device (mobile phone), and may be some kilometres from their own place of work but will not need to roam while connected.

Security The user will need to be authenticated and verified. LDAP is used in the m-bookMed medical system for patient/doctor authentication. The connection needs to be secured (i.e. encrypted). To this end SSL (Secure Socket Layer) and WTLS (Wireless Transfer Layer Security) is used.

Telecommunications pathway The hand-held device will need a connection to a GPRS service provided by a GSM/GPRS operator, and onward routing to the server at JP II Hospital via the WAP Server at UMM Computer Science.

QoS The need here is primarily for reliability of connection. The data are character based and performance or bandwidth are not of concern.

Intended demonstration It is intended to demonstrate this GPRS access from test-bed locations in Krakow and probably in Ipswich or London, if BT or other UK operator provides a 6Bone connectivity to the GEANT IPv6 network.

3.1.4 Hospital Appointment Clerk's intranet access to Clinical Appointment System (CAS)

Clinical information requirement The appointment clerk needs to add, remove, change, verify and approve the patient's appointment data in the CAS outpatient clinic appointment system for medical examinations and tests. The appointment clerk also requires access to patient personal data and has a need of adding, reviewing or approving it. All data are held on the CAS server in the JP II Hospital and accessed from location inside the hospital's intranet. A Web-based application is being developed for this.

Device and location The CAS system will be installed in JP II hospital. It will be available inside the hospital's intranet from all desktop PCs, laptops or iPAQ PocketPC computers connected to the JP II Hospital LAN and WLAN. There is no additional mobility requirements in this scenario.

Security The appointment clerk must be authenticated – here CAS will use methods such as login/password and/or smart cards with PKI. Each request performed by the clerk will be authorized according to the policy based on the accessibility of respective web pages. The web browser – web server connection needs to be secured (i.e. encrypted), e.g. by means of https protocol suite.

Telecommunications pathway The desktop PCs, laptops and iPAQs will be connected to the IPv6 wired and/or wireless network infrastructure in the JP II Hospital, so they will be able to access the CAS server directly over the hospital IPv6 intranet.

QoS The need here is primarily for reliability of connection. The data are mostly character based and performance or bandwidth are not of concern. Some small amount of graphics will be applied to provide a good-looking and to ease the use of web pages. The speed of both 802.11b wireless LAN and 100BaseT wired LAN is much more than the system can make use of.

Intended demonstration It is intended to demonstrate operation of the CAS system over JPII hospital WLAN and LAN networks.

3.1.5 Home/street multi-access to CAS (Clinical Appointment System)

Clinical information requirement The patient needs to check and change its medical appointment data held in the CAS web-based clinical appointment system at the JP II Hospital server, from any public location including a patient home or a street.

Device and location When users need to view the data on a PDA, they may be kilometres away from their own place of work and then a connection via GPRS is used or they may be very close to the hospital or any other public place (e.g. an airport), where a WLAN connectivity is active. It is assumed that they will not need to roam while connected. It is planned that the GPRS connection of iPAQs will be implemented with the GISMO network adapters which can operate both on 802.11b and GPRS.

Security The user will need to be authenticated and verified (e.g. via login/password and/or PKI), and their connection needs to be secured (i.e. encrypted, e.g. by means of https protocol suite). The authorization is based on the accessibility of respective web pages.

Telecommunications pathway The PDA will be connected to a WLAN or a GPRS service. The connection between a GPRS phone and PDA may be implemented in two ways, depending of the PDA's operating system. For Linux (the only one which supports IPv6) UMM will use:

- GISMO card for IPAQ (no test with Linux done yet)
- IRDA or Bluetooth connection to the GPRS phone (no test with Linux done yet)

Tunnelling of IPv6 packets in IPv4 is envisaged as currently IPv6 connections cannot be delivered natively by GPRS.

QoS The need here is primarily for reliability of connection. The data are mostly character-based and performance or bandwidth are not of concern. Some small amount of graphics will be applied to provide a good-looking and to ease the use of web pages.

Intended demonstration It is intended to demonstrate this WLAN or GPRS access from test-bed locations in Krakow. It will be also possible to expand the demonstration to other sites if 6Bone connectivity to the GEANT IPv6 network is provided.

3.1.6 Roadside (WAP) access to Clinical Appointment System

Clinical information requirement The patient needs to check (but not change) the data held by the CAS outpatient booking system (including e.g. patient's personal data, a list of available medical examinations, visits requested by the patient), running on a server in the JP II Hospital, from any public location including the street. A WML-based (WAP) application is being developed for this.

Device and location They will need to view the data on a hand-held device (mobile phone), and may be some kilometres from their own place of work but will not need to roam while connected.

Security The user will need to be authenticated and verified. Standard login/password mechanism is used in the CAS medical system for patient authentication. The connection needs to be secured (i.e. encrypted). To this end SSL (Secure Socket Layer) and WTLS (Wireless Transfer Layer Security) is used.

Telecommunications pathway The hand-held device will need a connection to a GPRS service provided by a GSM/GPRS operator, and onward routing to the server at JP II Hospital via the WAP Server at UMM Computer Science.

QoS The need here is primarily for reliability of connection. The data are character based and performance or bandwidth are not of concern.

Intended demonstration It is intended to demonstrate this GPRS access from test-bed locations in Krakow and probably in Ipswich or London, if BT or other UK operator provides a 6Bone connectivity to the GEANT IPv6 network.

3.1.7 Hospital intranet access to medical radiology database

Clinical information requirement The cardiologist or nurse specialist needs to add, review or update the radiology medical data of patients (e.g. those attending a cardiac outpatient clinic) by accessing the NetRAAD server and its database (which are operational at the JP II Hospital) via a web browser. NetRAAD has been adapted for this purpose to work under IPv6. Alternatively, a Java-based client application able to display DICOM images and text tags (see 3.1.8) could be used, e.g. in emergency cases for consultations, as it will be possible to run it either on a laptop or a PDA. This Java-based client application is currently under development at UMM.

Device and location The users will use laptops or desktop PCs situated in the JP II Hospital's LAN in most cases, but – occasionally – there will be a need to access NetRAAD from a device (typically a PDA) placed in the hospital's WLAN connectivity area.

Security The accessibility of particular information will be based on authentication by means of users logins and passwords. The connections need to be secure (i.e. encrypted). NetRAAD itself covers the authentication issues, while transmission path encryption is going to be performed by a HTTP server.

Telecommunications pathway A laptop or desktop workstation will typically need to access the NetRAAD IPv6 server over the JP II Hospital intranet. Mobile devices (either PDAs or laptops) can also benefit from a WLAN when accessing the database from inside the hospital intranet.

QoS In this application area the most important needs are reliability and quality of connection. However, the volume of radiology data could result in very large DICOM files, thus making bandwidth a very important issue especially for wireless connections. In order to constrain the bandwidth requirements of clients, NetRAAD provides them with lower-quality (JPEG-compressed) reference images useful for browsing over the database.

Hardware requirements For diagnostic purposes, high resolution of end-user terminal screen is required as well as its compliance with the DICOM 3.0 specification (see its Chapter 14: Greyscale Standard Display Function). It is also worth noticing that most of contemporary handheld devices do not meet these standards. Moreover, it has been observed that the iPAQ's power consumption is extremely high when working in a WLAN environment.

Intended demonstration It is intended to demonstrate accessing the NetRAAD database with usage of both a web browser and the Java-based client application inside the John Paul II Hospital LAN and WLAN intranet.

3.1.8 Home/street emergency multiaccess to patient's medical radiology database

Clinical information requirement The GP doctor, nurse or ambulance worker needs to review (but not change) the DICOM encoded radiology data and basic medical summary of an accident victim or other emergency care patient, held on the NetRAAD radiology database server in JP II Hospital, from any location. In such cases, the hospital's data would be helpful when accessed for reference. A lightweight DICOM viewer integrated with hospital database browser dedicated to PDA devices is being implemented for this application. In some cases, the client can be used inside the hospital, as described in 3.1.4.

Device and location In this scenario, handhelds will be the most frequently used devices. Occasionally, the medical staff could use laptop computers. GPRS can seen as the most frequently available communication infrastructure nowadays, although we expect WLAN to become more available in public places in the near future.

Security Due to public network usage, the security mechanisms should be very strong. The user will need to be authenticated and verified (e.g. via token or PKI), and the connection needs to be secure (i.e. encrypted). The authentication issues are covered by NetRAAD itself, while transmission path encryption is going to be assured by means of https protocol suite performed by an HTTP server.

Telecommunications pathway A mobile device will need connection to GPRS service, which will be provided by GSM/GPRS service providers (Polkomtel Plus GSM in demonstrations). A gateway to the NetRAAD system working at the John Paul II Hospital will be provided, operated and maintained by the Institute of Computer Science of UMM.

QoS The most important needs of this application area are reliability and quality of connection. The volume of radiology data could result in very large DICOM files, thus making bandwidth a critical issue. In order not to make the client very bandwidth consuming (especially due to low bandwidth of GPRS networks), NetRAAD provides them with lower quality (JPEG compressed) reference images useful for browsing over the database. It is under consideration to implement a mechanism allowing users to specify their area of interest on DICOM image thus decreasing amount of data to be downloaded.

Hardware requirements For diagnostic purposes, high resolution of end-user terminal screen is required as well as its compliance with the DICOM 3.0 specification (Part 14: Grayscale Standard Display Function). It is also worth noticing that most of contemporary handheld devices do not meet these standards. Moreover, it has been observed that the iPAQ's power consumption is extremely high when working in a WLAN environment.

Intended demonstration It is intended to demonstrate GPRS and WLAN access from various testbed locations in Krakow. It will be also possible to expand the demonstration to UK or other sites if 6Bone connectivity is provided to the GEANT IPv6 network.

3.1.9 Video/audio streaming from emergency action place in hospital area

Clinical information requirement The doctors, nurses need to communicate by sending video and audio between different wards/departments/buildings in the hospital. It could be important when an urgent consultation is required during emergency action and the specialist staff is not in the same building. It is often necessary to send not only audio but also video to the specialist PDA or laptop and get the advice back. For this solution a Java-based teleconference/teleconsulting application is being developed.

Device and location The teleconferencing application takes mainly the advantages of JMF, Jini and Jiro. The staff will need to use PC, laptop or iPAQ Pocket PC devices situated in the WLAN of JPII Hospital in order to communicate with each other. There will also be a PC dedicated for Lookup Service, Deployment Station with installed Teleconferencing Service. This PC will also be the centralised downloading point for Teleconferencing Java jar files. There are no mobility requirements for this application.

Security The user will be authenticated and authorised. Instead of using Jiro's Security Service it is desirable to exploit LDAP solution over hospital Ipv6 intranet. The present implementation of Jiro's Security Service is neither stable nor mature.

Telecommunications pathway The laptops and iPAQs, connected to IPv6 WLAN network inside the JP II Hospital will communicate with each over. The communication will be established after prior registration into the system. Each device will have installed a Lookup Service browser that enables downloading of Teleconsulting Service's proxy. The Teleconsulting Service will keep track of all events in the system, especially of appearance of new users that want to hold a conference. After agreement on parameters among conference participants the audio/video streaming is accomplished via JMF-RTP API.

QoS There is a need here for high bandwidth of connection. The connection should support high quality to transport video and voice without substantial degradation. Also the demand is on high performance devices that need to handle real-time coding/decoding of streams. It is a very hardware-demanding application.

Intended demonstration It is intended to demonstrate this video and audio streaming communication in test-bed locations in JP II Hospital in Krakow. Purposeful are tests on stream delays and video/audio quality, and whether they are acceptable.

3.2 Technical Architecture

Figure 3 below shows the architecture of the Krakow site. The actual testbeds are: fixed and wireless networks of UMM Computer Science (development and first phase of testing) and the intranet of John Paul II Hospital (the actual demonstrator). The clinical application services located at JP II Hospital are delivered through IPv6 infrastructure routed in 6in4 tunnels via the UMM network and onward to 6Bone.

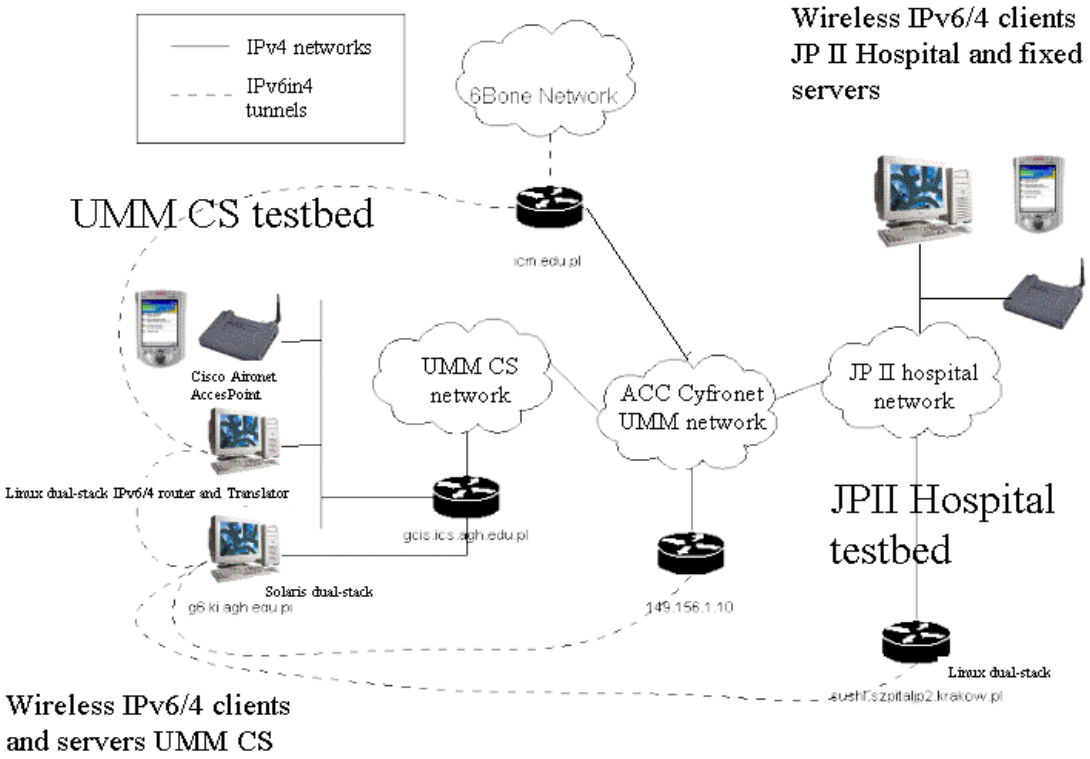


Figure 3: Network architecture of the Krakow demonstrator site

The communications pathway involves the use of some IPv4 networks, such as the UMM campus network (actually the Krakow MAN ATM backbone) IPv6 networks exist within the JP II Hospital and UMM Computer Science, including wired and wireless LAN based on 802.11b standard.

Linux with iproute package and IPv6 support has been used for Ipv6 traffic tunnelling when the transmission is made over existing IPv4 networks. Among all available technologies the 6in4 tunnelling in SIT technology has been used. On a Linux system located in UMM (CS Department) there are two access tunnels to 6BONE network configured. On the other side, tunnelling between JP II Hospital, ACC Cyfronet and UMM is done via software run on the Solaris 8 dual stack platform located in UMM CS. Between both systems (tunnel endpoints) – Linux and Solaris – an internal tunnel is also set up as they are located in different IPv4 networks.

WAP access scenarios will require translation to enable IPv4 “legacy” access from WAP phones to IPv6 servers. A Socks64 translator running on Linux is situated at UMM CS

Security requirements include end user authentication, encrypted data flows and probably also certificate handling.

3.3 Technical Component Descriptions

Note: this section draws on previously published material in 6WINIT Deliverables 1 and 2, and new Deliverables 8, 9 and 10. References are given to additional technical descriptions in these deliverables, using the notation style [D1 Section x.y.z].

3.3.1 IPv6 Transition Mechanisms

3.3.1.1 Tunnelling

Functional Requirement

Native IPv6 services from the main application server will need to be tunnelled via IPv4 from UMM Computer Science to JP II Hospital using MAN internet access Intranet. Additional tunnel(s) may be required for remote connectivity to other IPv6 islands via 6BONE.

Proposed Technical Solution: iproute tool run on Linux platform, Sun Solaris 8

Linux with iproute package and IPv6 support has been used for Ipv6 traffic tunnelling when the transmission is made over existing IPv4 network. Among all available technologies the 6in4 tunnelling in SIT technology has been used.

On a Linux system located in UMM (CS Department) there are two access tunnels to 6BONE network configured. On the other side, tunnelling between JP II Hospital, ACC Cyfronet and UMM is done via software run on Solaris 8 dual stack platform located in UMM CS. Between both systems – Linux and Solaris – an internal tunnel is also set up.

Outstanding Issues - none

Industrial Benefit

This installation provides proof of concept validation of the IPv6/4 tunnelling mechanisms within the Linux system and Sun Solaris.

3.3.1.2 Translation

Functional Requirement

a) IPv6 to IPv4 translation may be required to permit access from hand-held (PDA) running WindowsCE and from cellular phones to the native IPv6 services via GPRS transmission.

b) Some scenarios involve users having access to the native IPv6 services using only IPv4 clients from within IPv4 networks (e.g. from inside a JP II hospital intranet, accessed via UMM gateway to the public Internet and to 6BONE network).

Proposed Technical Solution: a) Socks64 Translator or b) 6WIND IP Edge Device

[D2 Section 2.5, D9 Section 2.6]

a) Several kind of IPv4-v6 translators are possible: IP header translation, this technology works in the IP layer and replaces the IPv4 header by an IPv6 header (similar to NAT, Network Address Translator). TCP relay is another technology that works in the TCP layer, and relays an IPv4 TCP connection to an IPv6 TCP connection, and vice versa, regardless of the application protocol used over TCP. TCP connection is terminated at the TCP relaying host. This technology is used in socks64 translator. Package socks64 is installed on a host (Linux) that has configured tunnelling and assures co-operation between existing IPv4/IPv6 services located in public network and IPv6 medical clients.

b) The dual stack in the Edge Device should soon include a translation mechanism that allocates a temporary IPv4 address to a dual stack host in the IPv6 network when it is required for IPv4 communication. IPv4 user devices will access clinical applications via this temporary IPv4 address rather than the IPv6 address of the main clinical server. [D2 Section 2.1.1]

Outstanding Issues

Interoperation between 6WIND, Socks64 Translator and other IPv4 applications.

Industrial Benefit

This installation provides proof of concept validation of the translation mechanisms within the 6WIND Edge Device and Socks64 Translator.

3.3.2 Security Mechanisms

3.3.2.1 VPNs using IP Routers

Functional Requirement

To provide an encrypted channel of communication between the clinical applications server and the end-user (possibly including the use of wireless devices). Certificate-based key management needs to be implemented e.g. via Public Key Infrastructure. [D10 Section 4.1]

Proposed Technical Solution: a) 6WIND IP Edge Device or b) CISCO IOS (IP Plus) and c) some PKI implementation (to be decided)

6WIND routers are able to create IPsec tunnels over IPv6 connections, including also the possibility of being certified by a PKI. [D8 Section 3, D10 Section 4.2] Usage of these devices will be considered if they are made available to Krakow site by 6WIND. This will be negotiated at the Basel project meeting.

Solutions available in the CISCO IOS will be also considered and evaluated.

UMM is also investigating several software PKI implementations to be used throughout the project, including the one from the University of Murcia.

The key management methodology for the demonstrator will be decided later, balancing the practical needs to provide a small and stable number of certificates with the wish to demonstrate a realistic and scalable scenario. A VPN will be established between JPII Hospital and the UMM Computer Science, to users connected via fixed LAN and WLAN. Ideally the VPN will extend to remote users connected via the Internet both using a fixed address and using GPRS.

Outstanding Issues

How to establish a VPN through to fixed and mobile users using native IPv4 devices connected via the public Internet (and possibly GPRS).

Industrial Benefit

Proof of concept verification of the Edge Device IPSec functionality and demonstration of a secure infrastructure for future adoption by regional health care networks.

3.3.2.2 **Road Warrior**

Functional Requirement

To provide an authenticated and encrypted channel of communication between the clinical applications server and the end-user specifically supporting the use of mobile devices connected via GPRS. Although PKI certificate-based security will be needed in real deployment situations, authentication using a pre-exchanged (public) RSA key would be the preferred method for a demonstration.

Proposed Technical Solution: IABG in partnership with 6WIND

IABG and 6WIND will collaborate to validate a mechanism to support the authentication and certificate/key management approach for mobile users whose IP address is allocated only at the time of connection. [D8 Section 3.2]

Outstanding Issues - none

Industrial Benefit

The collaboration will verify a technical approach that could inform IETF on potential modifications to IPSec to support Mobile IP. Component interoperability between IABG and 6WIND might lead to other future collaborations.

3.3.2.3 **Firewall**

Functional Requirement

The JPII Hospital-hosted clinical applications dual-stack server (running RedHat Linux 7.1) needs to be protected from hostile attack including unauthorised access and denial of service attack.

Proposed Technical Solution: Linux 2.4 with iptables package

The extension of security issues is possible due to the opportunities to filter IPv4 packets. The built-in features enable base traffic filtering based on IP addresses, kind of protocol, port numbers (kind of services). The extensions in filtering offer examination of TOS field and TCP flags. These can limit the amount of opening connection packets (SYN flag). It is also possible to generate dynamic rules based on actual packet counters in order to protect against DoS attacks.

The code responsible for filtration has been recently upgraded with IPv6 support. This enabled usage of all above described rules.

The protections (IPv4/6 filters) will be implemented in access node serving 6BONE network as well as JPII Hospital network in order to protect hospital's local network and medical data against unauthorized access.

Outstanding Issues

Mobile IP security measures will need to be managed separately

Industrial Benefit

Verification of code for filtering IPv6 traffic, provided with linux iproute package.

This feature is an important "by-product" of the VPN, as a demonstrated security solution for regional health networks.

3.3.3 Mobile IPv6

3.3.3.1 **MIPv6 Home Agent**

Functional Requirement

Users need to be able to reliably connect to the clinical applications server from a mobile (non-roaming) device whose Care of (IP) Address is dynamically provided by an ISP or other foreign network. [D8 Section 2, D10 Section 2.2.1]

Proposed Technical Solution: Helsinki University's mobile IPv6 stack implementation

The apparent functionality of Mobile IPv6 protocol is that it provides the user transparent host-mobility on IP-protocol level. Hosts can be moved between different subnets in the Internet but are still reachable by their original IP address.

The specification of mobility support in IP protocols stack is not finished yet and some of its points as e.g. support for security (IPSec) with AH (authentication header) are still in development phase. Nevertheless this solution is being deployed to MIPL project. After finishing the specification no extensive rewriting of the MIPL code will have to be done.

UMM carries experiments with the Helsinki University's mobile IPv6 stack implementation (http://www.mipl.mediapoli.com) on the mobile hosts, since this is widely believed to be amongst the most progressive work on mobile IPv6 stacks. [D8 Section 2, D10 Section 2.2.2.1]

Outstanding Issues

This function is in progress. The developed software match as closely as possible the functionality described in the IETF Mobile-IPv6 draft, but it may occur that it will not be interoperable between different implementations of mobile IPv6 running on other operating systems than Linux.

Industrial Benefit

To be confirmed

3.3.3.2 **802.11b Access**

Functional Requirement

Users need to be able to reliably connect to the clinical applications server from a wireless LAN, using a laptop or PDA.

Proposed Technical Solution: Cisco Aironet Access Point

The Cisco Aironet Access Point is used at the border between wired Ethernet and wireless networks based on 802.11b. This technology has been tested and is able to provide wireless access to devices using Ipv6 protocol. Notebooks and PDAs has been equipped with PCMCIA Cisco Aironet adapters and the access to wireless network is supported with Access Point. [D2 Section 4.2.1.2]

The deployment of wireless Ipv6 network will guarantee the mobile users access to medical applications located in JP II hospital.

Outstanding Issues

Testing of this functionality is in progress.

Industrial Benefit

To verify this "commercial-off-the-shelf" technical solution.

3.3.3.3 GPRS

Functional Requirement

Users need to be able to reliably connect to the clinical applications server from a mobile (non-roaming) hand-held device or mobile phone. This will include the need for wireless access via GPRS.

Proposed Technical Solution: Gismo Device, Ericsson R520m

Gismo is an expansion pack for Compaq iPAQ hand-held which has the ability to access three different kinds of networks: GPRS, GSM and 802.11b. Ericsson R520m mobile phone has built-in GPRS module and may be used as a WAP browser or a modem for laptop computer.

Outstanding Issues

Gismo is unavailable so far; but it should be at the beginning of the year 2002.

Provision of IPv6 over GPRS depends on GSM/GPRS provider and Polkomtel does not support it now.

Industrial Benefit

To be confirmed

3.3.4 QoS

3.3.4.1 TAG

Not required at Krakow site

3.3.4.2 JMF

Functional Requirement

The proposed user scenarios place only a limited demand for QoS functionality, primarily for reliability. However, the teleconsulting clinical application will include the use of multimedia data requiring high bandwidth and high performance capability, so an opportunity to test this could be engineered.

Proposed Technical Solution: JMF 2.1.1a (the currently available version)

The JMF API extends the framework to provide support for capturing and storing media data, controlling the type of processing that is performed during playback, and performing custom processing on media data streams. In fact JMF does not support any QoS mechanisms, we can only try to transmit data with e.g. desired bit rate, frame rate, etc, but the application does not guarantee that these parameters will be performed. JMF supports control over media processing and rendering.

Outstanding Issues

Problems with native code that must exist during runtime so downloading it with Jini's Lookup Service does not solve the problem as the application will already be run. The native code can diminish the Jini's downloading features as could be introduced to the teleconsulting application.

Industrial Benefit

Enable the development of media streaming and teleconferencing applications in Java.

3.3.4.3 DiffServ

Not required at Krakow site, since all the 6WINIT demonstration traffic between the JPII Hospital and UMM can go in dedicated ATM PVCs in the Krakow MAN.

3.3.5 Signalling Gateways – SIP

3.3.5.1 SIP

Not required at this site

3.3.6 Multimedia Conferencing Gateways

1.3.6.1 Jini, Jiro

Functional Requirement

The requirements are for session invitation, parameter negotiation that will be performed with Jini/Jiro event notification mechanisms.

Proposed Technical Solution – to be confirmed

The finder application from OKI Inc. (http://www.okilab.com/jini/finder/) will be used as a lookup service browser. This browser supports displaying graphical user interfaces for well-known interfaces. The browser will be the means for contacting the lookup service browser and downloading the conferencing tools.

JDK1.4 installed on Linux platform as the one supporting IPv6.

Outstanding Issues

Unknown as yet

Industrial Benefit

Demonstration of the value of usage Jini/Jiro technologies for spontaneous networking.

3.3.7 WAP Gateways

3.3.7.1 UMM WAP Gateway

Functional Requirement

There is considerable attraction to making patients' booking of clinical services available to them using a WAP phone or a PDA using a WAP connection, since this is present-day and widely available technology.

Proposed Technical Solution

At present all WML-based medical applications use the Nokia WAP Server. In the future the Ericsson WAP Gateway will be tested, if made available by Ericsson PL. For security reasons IPsec connection is established between UMM Nokia WAP Server and GSM/GPRS provider (Polkomtel SA) infrastructure. The UMM WAP Gateway solution is described in D2 Section 8 and D8 Section 5. The Nokia WAP Server and Ericsson WAP Gateway/Proxy are described in D2 Section 8.2.

Outstanding Issues

The current solution is inherently IPv4. Ericsson PL has not delivered the Ericsson WAP server in IPv6 version.

Industrial Benefit

Business application of the UMM's medical WAP solutions (using WAP Gateway) will be considered by the JP II Hospital and GSM/GPRS providers in Poland. To the 6WINIT partners, the benefit may be in showing the limitations of what can be achieved with WAP.

3.3.8 Access Network Provision

3.3.8.1 GPRS

Functional Requirement

Wireless GPRS network access is required to demonstrate the "roadside" access to clinical applications.

Proposed Technical Solution

The GPRS infrastructure across Poland (access delivered by GSM/GPRS provider Polkomtel SA operating the Plus GSM network)

Outstanding Issues

As for now, UMM uses only 2 GPRS-activated SIM cards for tests. More extensive test in the JPII hospital will require purchase more cards.

Industrial Benefit

Demonstration of the value of GPRS for the rapid and reliable retrieval of health information via wireless, to help stimulate a health care market for such solutions.

3.3.8.2 WLAN

Functional Requirement

Wireless (WLAN) network access is required to demonstrate the "bedside" access to clinical applications. Although IPv4 WLAN is becoming prevalent now, in the future this is likely to be IPv6. In 6WINIT this kind of access will be demonstrated at the Krakow site in IPv6 WLAN networks at the JPII Hospital UMM Computer Science.

Proposed Technical Solution Cisco's Aironet 802.11b WLAN

Cisco's Aironet WLAN architectures is described in D1 Section 5.1.

The Wireless 802.11b LAN operational at UMM Computer Science will be the primary test location in Krakow. For demonstration purposes a WLAN can be established at the JPII Hospital. Secondary connection to other islands of wireless access at other partner sites may be attempted later, possibly utilising 6BONE (see below).

Outstanding Issues – none

Industrial Benefit

Demonstration of an IPv6 wireless methodology suitable for use inside hospitals in the vicinity of medical devices.

3.3.8.3 IPv4 WANs

Functional Requirement

IPv4 WAN is required to demonstrate hospital-based access to the IPv6 clinical applications using legacy networks. In practice this will be routed from UMM Computer Science to the MAN and Internet served by ACC Cyfronet, and accessed from JPII Hospital via ATM (IPv4) connection to Cyfronet.

Proposed Technical Solution

Clinical application located in JP II Hospital are accessible through ATM connection. This connection is set to main node in backbone network – ACC Cyfronet. The traffic from this centre is available through connection to MAN network connecting UMM and CS department. This network supports only IPv4 traffic, hence IPv6 traffic needs to be tunnelled with mechanisms described in the section 3.3.1.1.

Outstanding Issues

The JPII hospital edge firewall that filters IPv4 traffic was not able to transmit IPv6 tunnelled traffic. Therefore the UMM-JPII end-node is connected before the firewall. This problem enforced implementation of filtering on the end-node, because it was not secured by the main firewall.

Industrial Benefit

Demonstration of a viable migration approach, and of rigorous IP translation mechanisms.

3.3.8.4 IPv6 WANs

Functional Requirement

Native IPv6 distributed access is required to validate the future scenario of widely available IPv6 networks within hospitals. In practice this will be demonstrated within UMM Computer Science using local IPv6 networks, and from fixed connections at other clinical sites via 6BONE tunnels.

Proposed Technical Solution: Dedicated ATM PVC connection, 6in4 tunnels

In practice the access from native IPv6 will be done via dedicated ATM PVC connection. This connection will enable the creation of virtual channel that transmits IPv6 traffic without encapsulation between local UMM network and JP II Hospital network. In future an analogue connection will be used to create non-tunnelled connection to 6BONE node in Poznan.

The IPv6 traffic to the medical centres to which such native IPv6 transmission would not be possible via dedicated ATM PVC connection, it will be accomplished through tunnelling mechanisms.

The other cross-country connections will be realised with 6in4 SIT tunnels which configuration is described in section 3.3.1.1. This tunnelled interconnection of IPv6 islands will simulate a homogenous IPv6 WAN.

Outstanding Issues – none

Industrial Benefit

The demonstration of solutions that integrate IPv6 applications with existing IPv4 WANs without changing the WANs structure and configuration. Additionally testing the ability of integration IPv6 technologies with the most popular WAN technology – ATM.

3.3.8.5 **UMTS**

Functional Requirement

Wireless UMTS network access may be required to demonstrate the next-generation “roadside” access to clinical applications. In practice this can be simulated from a UMTS test-bed location.

Proposed Technical Solution: Ericsson “Kista Ring” (to be confirmed)

The routing of network traffic via 6BONE described above can be extended to include the UMTS test-bed near Stockholm (Sweden) if such demonstration is decided by the consortium.

UMTS is unlikely to appear in Poland as a public service within the project's timeframe.

Outstanding Issues

To be identified later

Industrial Benefit

Provide proof-of-concept verification of UMTS access to web-based application services, as market stimulation. Ideally the demonstration will highlight the benefits of UMTS over GPRS.

3.3.9 Access Devices

3.3.9.1 Terminals

Functional Requirement

The various Krakow user scenarios require four different user access devices.

1) a desktop workstation, running a web browser and/or Java/JMF

2) a laptop computer, running a web browser and/or Java/JMF

3) a hand-held device, such as a PDA, running a web browser and/or Java (both IPv4 and IPv6 versions)

4) a mobile phone with WAP browser.

Proposed Technical Solutions

PC: running Linux, Windows, IPv4 or IPv6 or dual stack, a browser with IPv4 and IPv6 support, Java 1.4, JMF

Laptops: running Linux or Windows NT and 2000 with IPv6 stacks, with fixed Ethernet, Wireless LAN or GPRS connection through mobile phone, a browser with IPv4 and IPv6 support, Java 1.4, JMF.

Compaq iPAQ: running Linux or WinCE, IPv6/IPv4 and a web browser, with a wireless GPRS connection (Gismo or Ericsson R520m) or a Wireless LAN connection (Gismo or Cisco Aironet 350).

Ericsson R520m GSM/GPRS phone.

Outstanding Issues

IPv6 not yet available for WinCE, and not stable on Windows

Industrial Benefit

A spectrum of devices is important to show the compatibility of 6WINIT solutions with a wide range of user needs.

3.3.9.2 Security Devices

Functional Requirement

The ideal requirements are for strong authentication and user certification (including access control role-based profiles). A comprehensive security solution would add credibility to the overall 6WINIT technical architecture.

Proposed Technical Solution: Gemplus smart cards and scanner

Gemplus smart card scanner offers comfortable solution for users to authenticate.

Outstanding Issues – none

Industrial Benefit

This needs to be confirmed, since the demonstration of these security tools themselves is not the focus of 6WINIT.

3.3.10 Location Awareness

Not required at this site

3.4 Clinical Applications

The Krakow site clinical applications to be demonstrated in 6WINIT are JPII Hospital clinical services provided as a set of middleware components providing controlled access to hospital medical and administrative data. Access to these data is provided through a set of web-based applications, with the server side written in Java/J2EE technologies, running on servers operating in JPII hospital and (at least in the development phase) at UMM. Access to databases is organised with EJB application servers. The session EJB beans implement business logic and co-operate with entity EJB beans accessing data stored in the databases. The data presentation logic is separated from data processing that makes easier the adaptation of the systems to changing requirements of end-user devices.

The primary user interface of those clinical applications is a web browser or a WML browser. The two exceptions are: the lightweight Java DICOM viewer and the multimedia teleconferencing system that requires a JMF based application installation on end-user terminal. Jini Lookup Server is used in the latter case to support dynamic uploading of the needed user interface.

The following sets of clinical web applications with their available access schemes are under development in Krakow:

1. m-bookMed: an advanced system for booking clinical resources (web browser - laptop/PDA access)
2. m-bookMed (WAP read-only access)
3. Clinical Appointment System: simplified outpatient booking (web browser - laptop/PDA access)
4. Clinical Appointment System (WAP read-only access)
5. Hospital radiology application for cardiac and cardiovascular diseases management (web browser - PC/laptop access)
6. Emergency application for cardiac and cardiovascular diseases management (Java viewer - PDA access)
7. Emergency teleconsultation (Jini/Jiro application - laptop/PDA access)

Each of these applications is briefly summarised below, and illustrated using some main screen captures.

3.4.1 m-bookMed: Advanced clinical resources booking system (web browser - laptop/PDA version)

The m-bookMed system combines characteristics of a publicly available internet portal and an application which is able to serve confidential medical information for authorised users. The information available will include health care services in general, examinations and services offered by the hospital and other hospital specific information and advertisements. A key functionality of m-bookMed is electronic mobile booking of hospital services and resources, including the equipment and the time of hospital personnel: doctors, nurses and helper staff. All this functionality will be addressed to a broad group of users: the clients, i.e. GPs and patients individually, as well as the serving hospital staff. The system has an automatic notification support. Patients will be informed about important events concerning them (e.g. examination cancelled due to equipment failure or personnel absence) in the way they prefer (e.g. mail, SMS).

Figure 4 shows a screenshot of the main administration page of m-bookMed system. The system is currently under development so a PDA screenshot is not yet available.

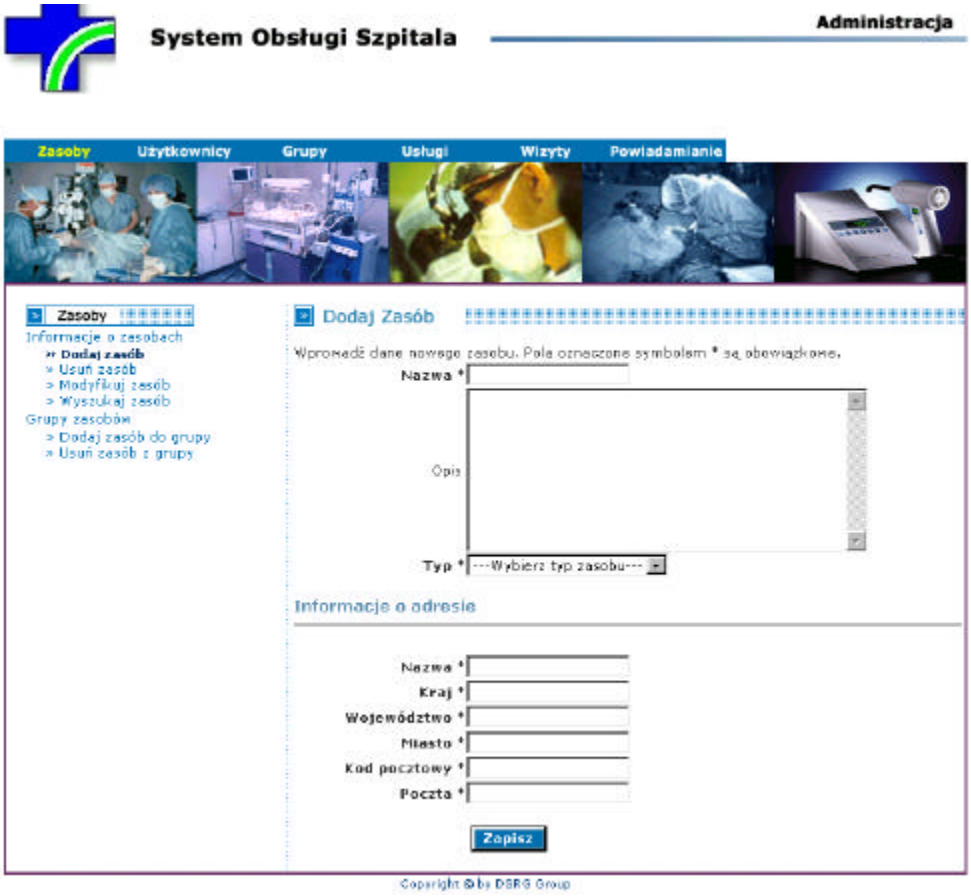


Figure 4: Screenshot of the main window of m-bookMed

3.4.2 WAP read-only access to m-bookMed clinical resources booking system

The advanced system for booking medical services (m-bookMed) is equipped with a WML interface (without graphics and with reduced amount of available information).

Before using m-bookMed (Fig. 1 below), we have to authorise in the system. First phase is choosing a profile: doctor, patient or guest (Fig. 2). The next one is authentication (Fig. 3, 4), with a login and password (letters of password are replaced with star symbol '*'). Finally, we can browse the available data (e.g. patient data or visits/bookings) (Fig. 5, 6).

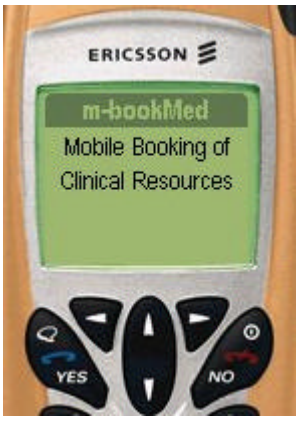


Fig 1.

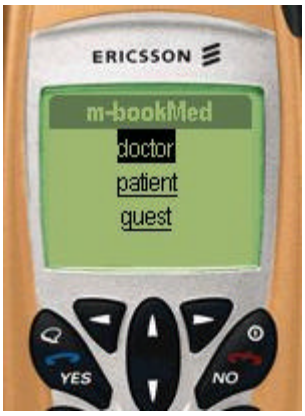


Fig 2

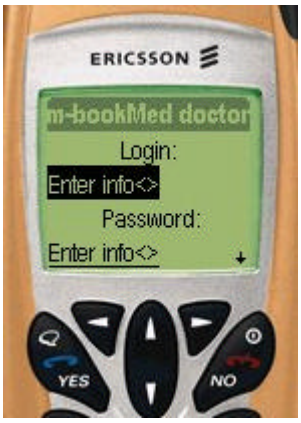


Fig 3.

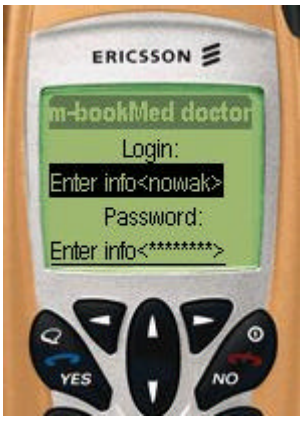


Fig 4.

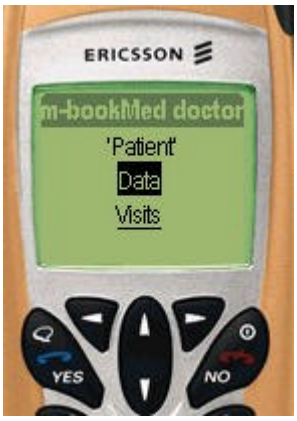


Fig 5 .

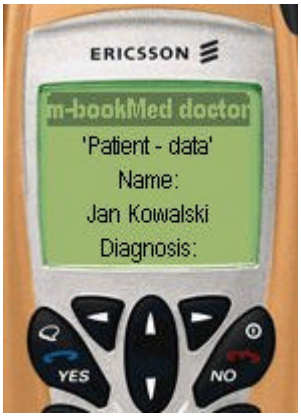


Fig 6.

3.4.3 Clinical Appointment System (web browser - laptop/PDA version)

CAS (Clinical Appointment System) is a registration system that allows a patient to make an appointment with a doctor for a specific medical examination using remote access to a database containing list of medical examinations and doctors that are able to perform them. The difference between CAS and m-bookMed is that CAS is much simpler and provides only a subset of the functionality of m-bookMed. In particular, CAS does not provide automatic support for matching dates of appointments, forwarding that responsibility to a human (the Appointment Clerk).

Figure 5: CAS welcome web page

Before registering for an examination with CAS every patient has to create his/her own profile. Using given identity and access code the patient is able to logon to the system and then make an appointment with a doctor.

The patient is first of all capable of choosing the medical examination type, as well as a doctor who is servicing it, and then make an appointment. The patient can also manage his or her appointments. He or she is able to preview all planned and finished services that he or she will take or have taken part in. The patient can change the appointment conditions such as a servicing doctor or time for any future appointment. The patient is informed when some problem occurs at the clinic, effectively postponing a medical examination.

From the clinic side there is an Appointment Clerk who interacts with a patient. The Appointment Clerk approves patient's requests checking when a doctor is able to perform the medical examination that the patient applied for. The Appointment Clerk sends the timing information to the patient through the patient profile web page this way informing him or her about the appointment.

Special situations such as a patient cancellation of a requested appointment or a clinic-derived problem are served as well.

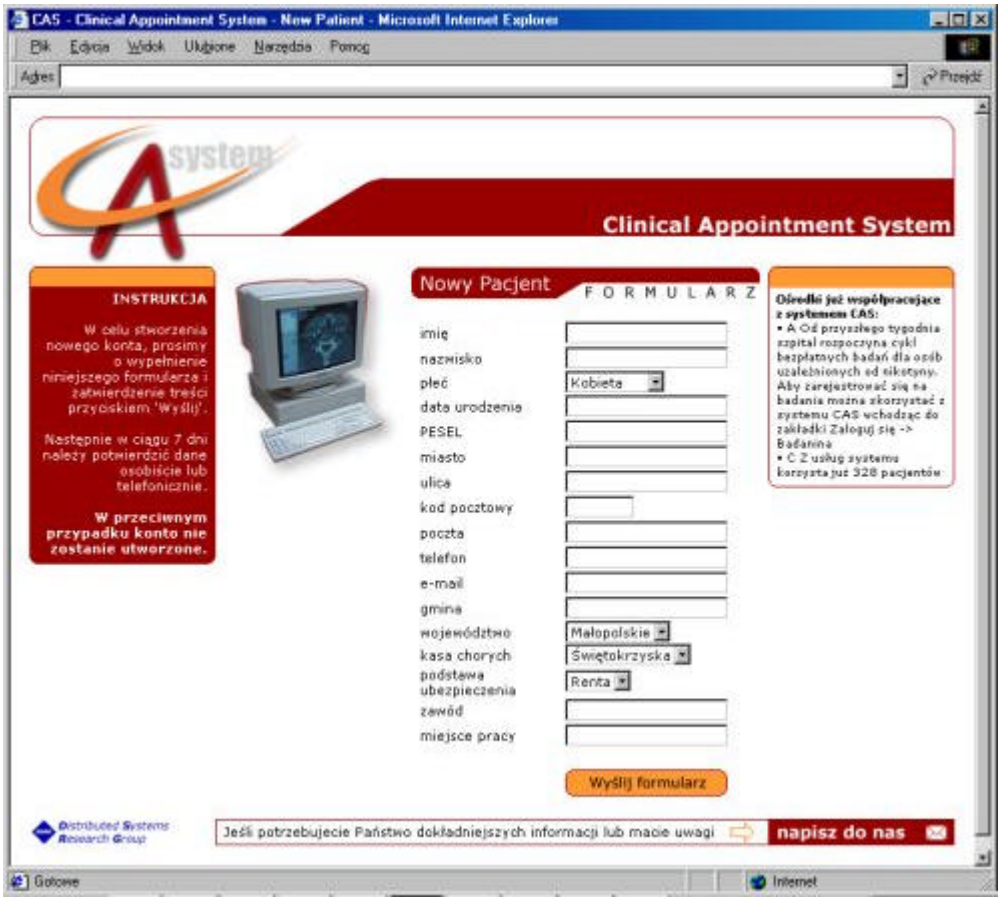


Figure 6: New patient web page in CAS

3.4.4 Clinical Appointment System (WAP read-only access)

The Clinical Appointment System (CAS) is also equipped with a WML interface (without graphics and with reduced amount of available information).

Before using CAS (Fig. 1 below), we have to authorise in the system. First phase is choosing a profile: doctor, patient or guest (Fig. 2). The next one is authentication (Fig. 3, 4), with a login and password (letters of password are replaced with star symbol '*'). Finally, we can browse the available data (e.g. patient data or visits/bookings) (Fig. 5, 6).

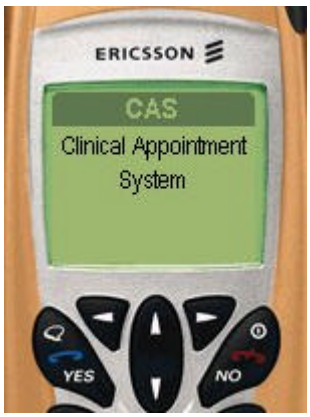


Fig. 1

Fig. 2

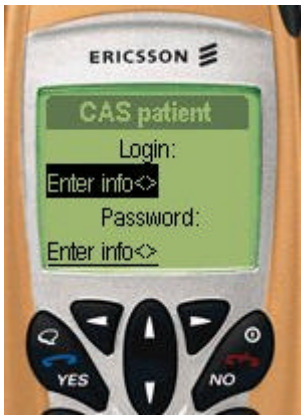


Fig 3

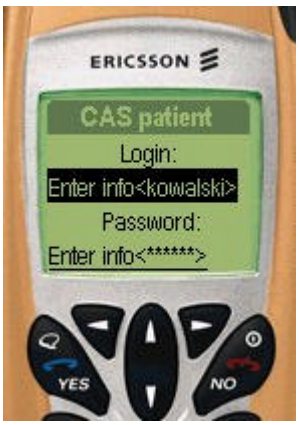


Fig. 4

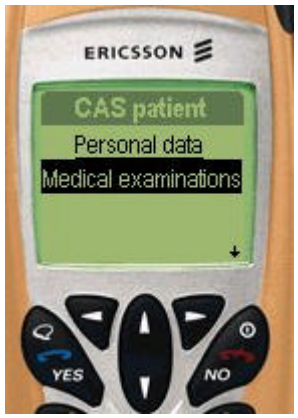


Fig. 5

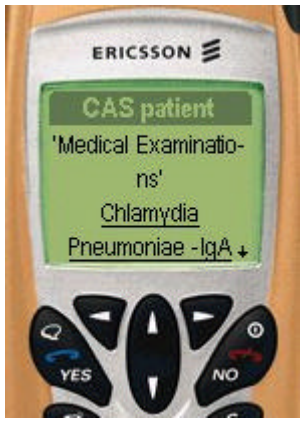


Fig 6

3.4.5 Hospital radiology application for cardiac and cardiovascular diseases management (web browser - laptop/PDA access)

NetRAAD (Network Radiology Acquisition Access and Distribution) is a sophisticated system giving access to medical information via HTTP protocol. HTML pages are generated on a basis of users' requests using partially server-side tools (CGI scripts) and client-side mechanisms like the JavaScript language. DICOM images can be displayed only if an external viewer has been configured, otherwise they are stored onto disk. A couple of sample screenshots is presented in Figure 7 and Figure 8.

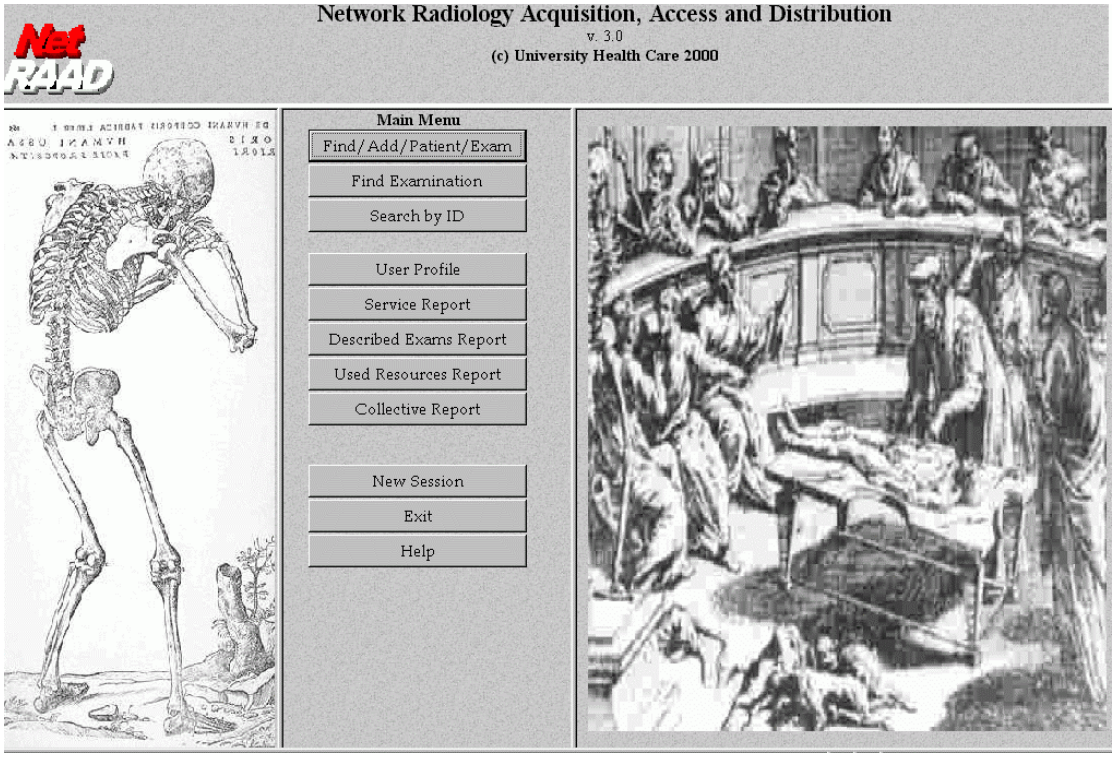


Figure 7: Initial screen of the NetRAAD system's viewer

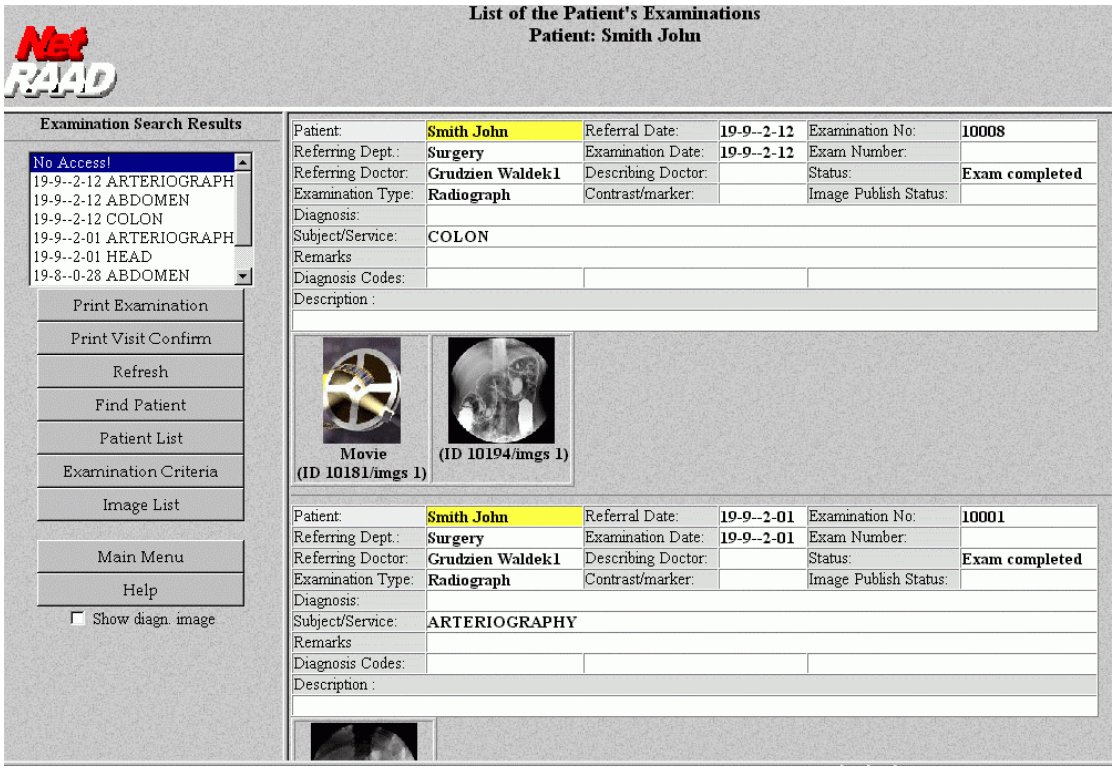


Figure 8: View of results of patient's examinations in NetRAAD system viewer

As an alternative, one can use the Java lightweight DICOM viewer integrated with hospital database browser, described in section 3.4.6.

Inside the NetRAAD system, the overall information regarding patient and his/her studies is stored in a SQL-compliant database. The information is organized in a few tables containing among other things:

- patient's personal data: first name, last name and sex – patient table
- diagnosis and remarks – exam table
- short description and references to flatfile and deepfile – image table. A flatfile is a referential image lossy-compressed – useful only while looking through contained images. The diagnosis should be performed using corresponding deepfile – image stored in DICOM format.

WWW pages generated by NetRAAD were designed and are quite well suited for HTML viewers running on desktop or laptop computers, but almost impossible to be shown on PDA machines equipped with small displays.

3.4.6 Emergency application for cardiac and cardiovascular diseases – PDA version

The goal of that application is to allow doctors to have access to medical data, mainly in the form of DICOM images, on their handheld equipment. Communication means may vary depending on the location of the doctor – from a GPRS/UMTS link outside the hospital to high-bandwidth intra-building network both wired and wireless inside hospital.

A very thorough review of existing PDA devices and DICOM software as well as consultations with medical technicians and doctors using DICOM in their everyday work were the main step when determining the system prerequisites. As a result, the following conclusions has been drawn:

- There is a need to create a new DICOM viewer. It will only need a replacement of the unit responsible for frontend generation while reusing NetRAAD's database and parts of it interface.
- The Java language have been chosen as an implementation language in which the project will be developed, because of its portability between multiple PDA platforms and ease of integration with Jini/Jiro technology are the most important advantages.
- The application should co-operate with existing NetRAAD system working in JP II Hospital.

The first phase of application development has been successfully finished. All tasks bound with communication with NetRAAD system has been implemented. The current release can display DICOM images as well as run an external DICOM viewer (e.g. Osiris on desktop computers or reViewMD on iPAQs) in order to perform more advanced operations such as overlay editing, zooming, displaying animated images and so on. This functionality is going to be included in the next release of the internal viewer which has been developed although the option of running external viewers will remain.

The typical scenario of the application usage includes:

1. Connecting to database and authenticating in it using a doctor's password.
2. Entering a patient's full name or, alternatively, name pattern. As a result, all matching records are displayed. This enables a doctor to choose an individual patient's name.
3. Selecting one of the records the study consists of. This causes downloading a corresponding exam data, which can be browsed. The data consists of the description stored in the database and series of reference (JPEG-compressed) images bound with the exam.
4. Downloading the diagnostic DICOM image. After choosing the appropriate medical image the DICOM file is downloaded. This happens only on doctor's demand in order not to burden the communication link with a big amount of data.

The described sequence of actions is presented as a screenshot in Figure 9.

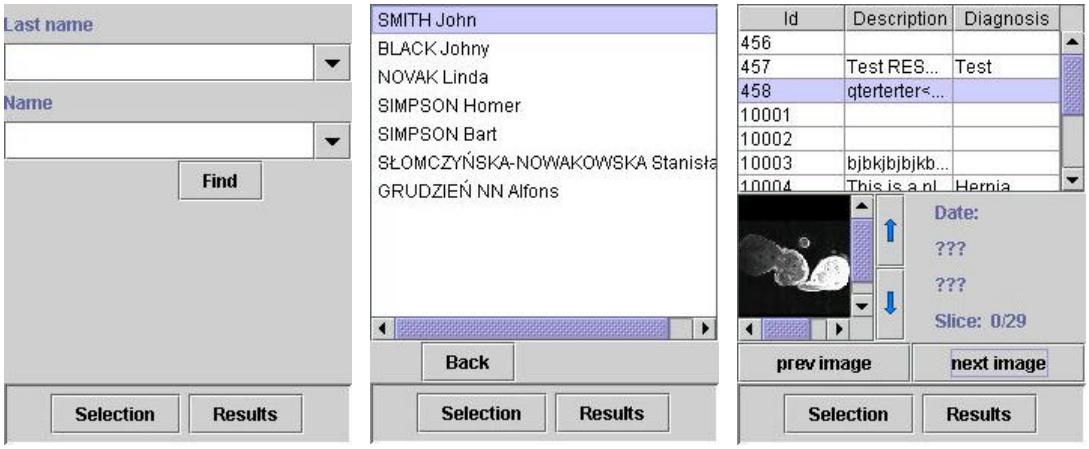


Figure 9: Screenshot from the Java lightweight client application (with DICOM viewer), running on a PDA

Figure 10: Screenshot of the DICOM viewer of the Java lightweight client application running on a PDA

3.4.7 Emergency teleconsultation (laptop/PDA access)

The Emergency Teleconsultation application serves the medical personnel to communicate with each other (e.g. give advice in complex cases) by setting up and managing multimedia conferences, especially in emergency cases, regardless of the location of key personnel (experts). Sometimes there are situations when an expert is not in the place of action but is inside the hospital WLAN. Assuming that he has a PDA running a Teleconsultation application it is possible to exchange opinions.

When doctorB wants to get an advice from doctorA, he/she selects from his list doctorA and clicks the "Invite" button. DoctorA nevertheless of his place and access device is notified about this with some sound and blinking “ball” (look at the bottom of the screen shot shown below).

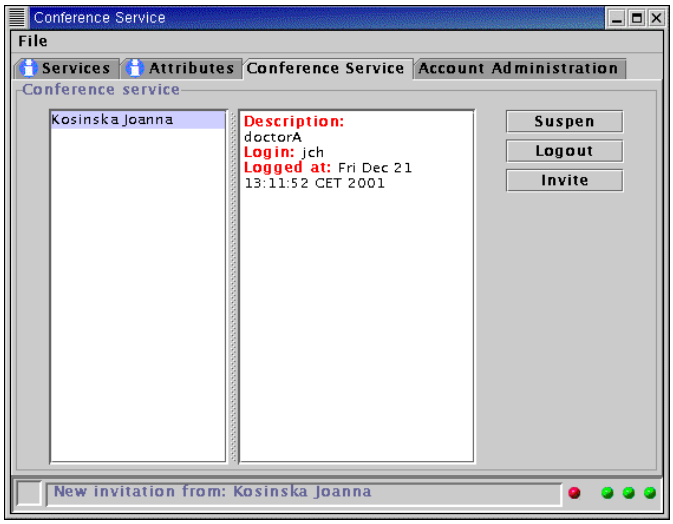
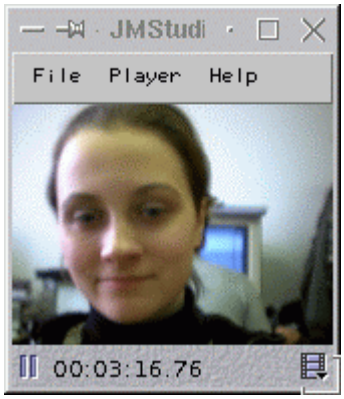


Figure 11 : Teleconsultation application: invitation screen

When clicking the ball, the doctor is informed about who wants to contact him/her and what is the matter. After accepting the call, the audio and/or video devices and streams are started.



From the technical side, there will be a Lookup Service installed at a server in the hospital intranet that would store the software and send it to the client if needed. The user has on its desktop an icon symbolising the Lookup Service Browser that would download the Teleconsulting proxy (visible as a GUI). If the client wants to be seen by the Teleconsulting system it has to register to it. Only those clients are able to hold a conference. The registration is logged in a repository for further usage, and all already registered clients are notified of a new user. Information of any kind

of user's state change (e.g. suspend, logout) is logged, and other participants are notified of such change.

The session announcement, invitation, quality adjustment, etc. is accomplished via Jini/Jiro event notification mechanisms. The streaming is accomplished through JMF-RTP API. There are possibilities of both unicast and multicast conferences.

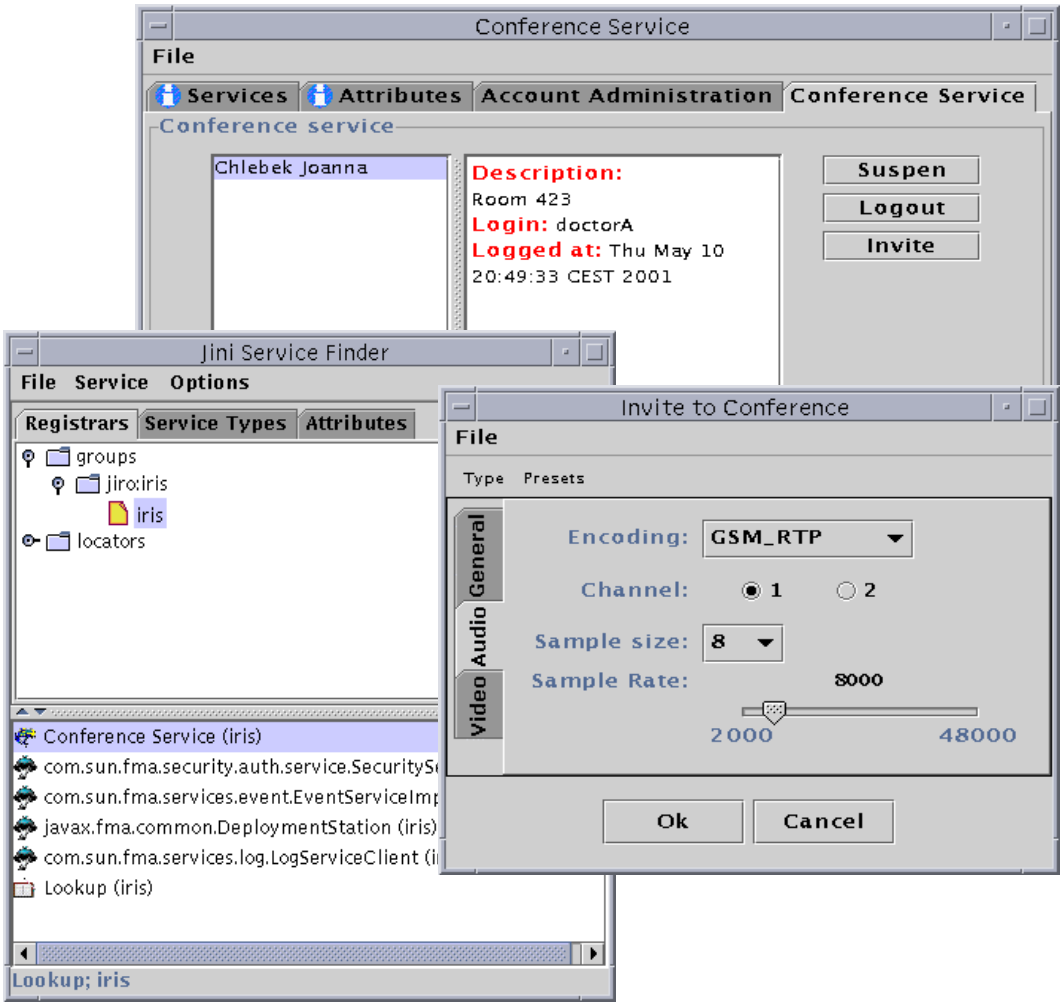


Figure 12: Screenshot of the Java/Jini/Jiro emergency teleconsultation application (set-up tools)

4 TÜBINGEN CLINCAL DEMONSTRATOR

4.1 Guardian-Angel-System (GANS)

6WINIT is demonstrating a real-time telemedical system (GANS) providing remote medical help to emergency physicians. The systems will make emergency patient care safer. The demonstration (chapter 3.4.) has multiple screens and is connected to the Tübingen University Hospital via a wireless IPv6 link. The screens show the emergency room (ER) in Tübingen, monitors of the patients` vital signs and live-video of a simulated incident. The cameras in the ER can be controlled remotely. Doctors at the exhibition (medical experts) offer remote advice on dealing with the incident.

The clinical scenario of the GANS application is already described in some details in Deliverable D3.

4.1.1 Clinician needs

The clinician in the GANS-Centre needs live video streams from the treatment room or ambulance. In addition he will need a full-duplex audio connection. To be able to judge the patient fast and without having to ask too much, there is a demanding need to get the vital signs of the patient monitors in their original appearance. The ideal situation would be to get the stored patient vital sign trends in addition to the live signs, the clinical information requirement, and the application/screen to be accessed. As the scene may be very hectic and a lot of movement of the personnel involved may take place, it seems necessary that the GANS can remotely control the camera (pan, tilt, zoom) and probably adjust the audio mix outward. An additional document scanner could be used for certain problems.

4.1.2 Proof of concept and further development

The GANS system will be tested and further developed between RUS and UKT and possibly other 6WINIT partner sites. The GANS demonstration at the IST 2001 conference event (see pictures at the end) has clearly shown the feasibility of this approach. New technical elements (see 3.3 below) will be introduced as they become available.

.

4.2 Technical Architecture

Not being a formal element of 6WINIT, the development of the GANS application is carried out in close co-operation with and exploitation of 6WINIT results evolving over the project's duration. At present, the GANS target architecture is based on a J2EE and JMF standard software environment according to the following figure:

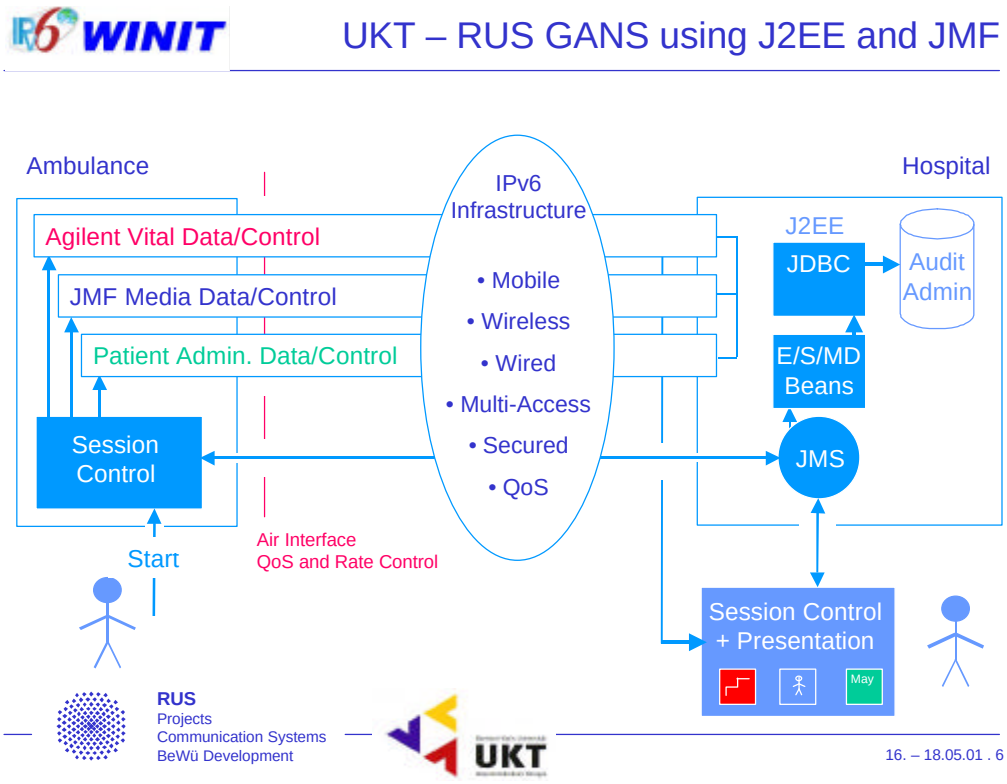


Figure 13: Guardian Angel System (GANS) target architecture

Following this exploitation and adaptation strategy, at the IST conference in Düsseldorf, December 3rd - 5th, 2001, a first approximation of the GANS target architecture was demonstrated. In addition to the very good acceptance of the demonstration by the general public and local and international politicians, the main technical achievements around and of this demonstration have been the following:

- Establishment of a normal (Mobile) IPv6 network within the German 6Bone infrastructure between Stuttgart and the German 6Bone centre Münster for initial IPv6 tests and eventually between Tübingen and Düsseldorf.
- Worldwide first successful operation of JMF video for JDK1.3.0 release on Linux from BlACKDOWN over JDK 1.4 using IPv6 over Linux Kernel version 2.1.2 on Red Hat 7.1; this application was not yet mobile.
- Transferring and controlling the GANS Vital Data over Ericsson's "Multi-Access" implementation of Mobile IPv6
- A successful workshop with Ericsson Nomadic Lab, Helsinki, and Ericsson Telebit, Aarhus, held in Stuttgart and Tübingen providing for the integration of these initial GANS components with Ericsson's MIPv6 Multi-Access platform, the latter providing seamless

handover between GPRS-WLAN-Ethernet, Home Agent (HA) functionality via the AXI Router from Ericsson Telebit and IPv6 routing.

The IST conference demonstration set up between Tübingen and Düsseldorf is shown in the following figure. The 'Ambulance' in Tübingen was represented by the UKT Patient Simulator theatre, the latter allowing for a realistic interaction scenario of the 'doctors' located at the simulated 'UKT Hospital' in Düsseldorf.

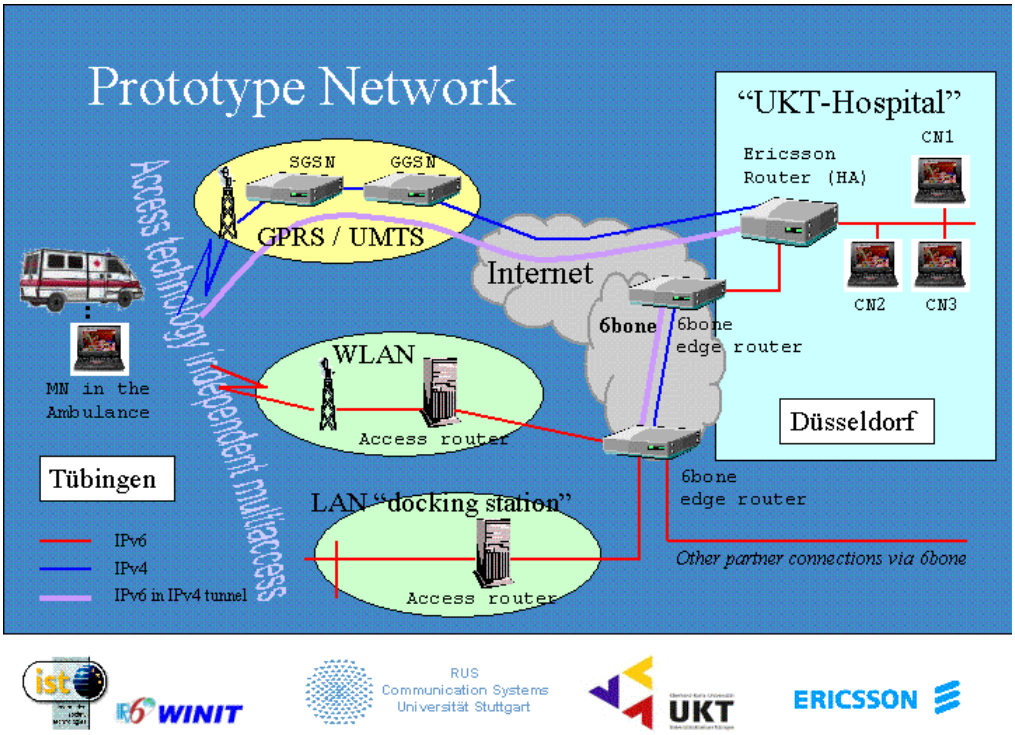


Figure 14: Guardian Angel System prototype at the occasion of the IST 2001 conference Düsseldorf , December 3-5, 2001

4.3 Technical Component Descriptions

4.3.1 IPv6 Transition Mechanisms

4.3.1.1 Tunnelling

Functional Requirement

Mobile/wireless and/or wired IPv6 services from the Ambulance will need to be tunnelled via IPv4-GPRS and 6BONE to the UKT Hospital. Additional tunnel(s) may be required for remote connectivity to other IPv6 sites.

Proposed Technical Solution: Ericsson's Multi-Access technology (possibly) including Ericsson's AXI router and possibly a follow-on device.

Outstanding Issues: TBD

Industrial Benefit: The IST 2001 demonstration provided a convincing proof of concept validation of Ericsson's solutions for the IPv6/4 tunnelling mechanisms both in the mobile and/or wired/wireless case.

4.3.1.2 Translation

Functional Requirement: -

4.3.2 Security Mechanisms

4.3.2.1 **VPNs using IP Routers**
Functional Requirement: Eventually, the GANS application does require 'all' state-of-the-art security mechanisms
Proposed Technical Solution: GANS security will be provided by a combination of 6WINIT developed network layer mechanisms and such which are inherent in the J2EE framework the latter possibly supported by the work of UCL concerning the usage of the university of Murcia IPv6 enabled PKI infrastructure.
Outstanding Issues: Use/deploy (Ericsson's) network-layer related mechanisms and (possibly)Integrate University of Murcia PKI and J2EE
Industrial Benefit: As application server usage is definitely a must in many commercial environments, the integration mentioned above would be of real importance for the acceptance of IPv6 in such environments.

4.3.2.2 **Road Warrior**
Functional Requirement: -

4.3.2.3 **Firewall**
Functional Requirement: The GANS J2EE application server needs to be firewall protected also at IPv6 level.
Proposed Technical Solution: No special solution envisioned so far.
Outstanding Issues: -
Industrial Benefit: -

4.3.3 Mobile IPv6

4.3.3.1 **MIPv6 Home Agent**
Functional Requirement: The GANS application as such does require Mobile IPv6 i.e. especially MIPv6.
Proposed Technical Solution: UKT-RUS will pursue the successful co-operation with 6WINIT partner Ericsson; see above 1.2
Outstanding Issues: -
Industrial Benefit: -

4.3.3.2 **802.11 Access**
Functional Requirement: It is assumed, that in hot-spot locations MIPv6 WLAN access is beneficial .
Proposed Technical Solution: Ericsson's Multi-Access; see above.
Outstanding Issues: -

Industrial Benefit: -

4.3.3.3 GPRS

Functional Requirement: Mobile IPv6 wireless access is essential for the GANS application.

Proposed Technical Solution: Ericsson's Multi-Access - i.e. MIPv6 over GPRS; see above. In addition to GPRS, UKT-RUS will also explore forthcoming UMTS test beds both within and outside of 6WINIT (RUS as partner of IST project MobyDick will establish an UMTS TDD cell at Stuttgart University).

Outstanding Issues: To further downsize the GANS application to GPRS capabilities in a meaningful way..

Industrial Benefit: GANS is basically an 'up-stream-oriented' application (the Mobile Node is sending more data up-stream ...). Help to make 'up-stream-oriented' professional applications more visible and accepted.

4.3.4 QoS

4.3.4.1 TAG

Functional Requirement: -

4.3.4.2 JMF

Functional Requirement: In the GANS target architecture a QoS framework both for the Best-Effort and DiffServ case are foreseen.

Proposed Technical Solution: After the mainly syntactical exercise of the inclusion of a frame-dropper module in the JMF chain, in order to assure a sufficient quality of the different GANS data streams, RUS will continue the integration of QoS modules into JMF (both for the Best-Effort, BE, and DiffServ case)

Outstanding Issues: TBD

Industrial Benefit: -

4.3.4.3 DiffServ

Functional Requirement: 'DiffServ for GPRS'.

Proposed Technical Solution: RUS will closely co-operate with and work on Ericsson's DiffServ RMD framework; see D10, '5.2 DiffServ Resource Management in IP-based Radio Access Networks'

Outstanding Issues: To develop appropriate use cases in the context of available infrastructures – e.g. GPRS version, end systems and/or GSGN involvement,

Industrial Benefit: QoS

4.3.5 Signalling Gateways – SIP

4.3.5.1 **SIP**
Functional Requirement: -

4.3.6 Multimedia Conferencing Gateways

Functional Requirement: -

4.3.7 WAP Gateways

Functional Requirement: At present, the usage of handheld devices in the ambulance such the iPAQ are under consideration.
Proposed Technical Solution: Assuming an iPAQ-type of device in the ambulance, a Bluetooth connection and Web-to-WAP conversion as developed by the 6WINIT partner UMM will be studied.
Outstanding Issues: TBD
Industrial Benefit: TBD

4.3.8 Access Network Provision

4.3.8.1 **GPRS**
Functional Requirement: At present, GPRS is the initial high-degree-mobility technology for GANS. It is also required, that the Mobile Node gets a standard (routable IPv4/v6) addresses. A NAT based GPRS provision is not sufficient to reach the Hospital-Home-network from the Ambulance-Mobile-Node. This condition was fulfilled in the German T-Mobile case.
Proposed Technical Solution: Ericsson's Multi-Access technology; see above.
Outstanding Issues: see above 3.3.3.3
Industrial Benefit: -

4.3.8.2 **WLAN**
Functional Requirement: see above 802.11
Proposed Technical Solution: -
Outstanding Issues: -
Industrial Benefit: -

4.3.8.3 **IPv4 WANs**
Functional Requirement: (At present) required for the GANS application.
Proposed Technical Solution: UKT - RUS are sufficiently well connected to the existing German and International Research infrastructure; the German T-Mobile GPRS service uses standard IPv4 addresses; see 1.3.8.1
Outstanding Issues: -
Industrial Benefit: -

4.3.8.4 **IPv6 WANs**
Functional Requirement: International connectivity to reach 6WINIT co-operation and demonstration partners.
Proposed Technical Solution: At present, 6Bone is sufficient
Outstanding Issues: Inclusion of more 6Bone partners in GANS(-related) scenarios.
Industrial Benefit: -

4.3.8.5 **UMTS**
Functional Requirement: see 3.3.8.1 with respect to the addressing capabilities:
Proposed Technical Solution: Assuming IPv6 as *the* network protocol for 'GPRS/UMTS'.
Outstanding Issues: -
Industrial Benefit: -

4.3.9 Access Devices

4.3.9.1 **Terminals**
Functional Requirement: The GANS application requires the following terminals • Portable (Agilent) patient monitor connected via a serial link to the Mobile Node MN (notebook) in the ambulance; Ericsson's Multi-Access MIPv6 software. In the final scenario, the MN will also capture and deliver Audio and Video. • In the Hospital-Home-network a workstation (notebook, PC) delivering the Vital Data from the ambulance and running the bi-directional audio and the unidirectional video from the ambulance (Linux) • An iPAQ-type of control terminal in the ambulance is under consideration (Linux) • In the target scenario, at the hospital a J2EE server (Linux)
Proposed Technical Solution: In co-operation mainly with 6WINIT partner Ericsson their Multi-Access software (and follow-on development based on the University of Helsinki's Mobile IPv6 stack (HUT)) will be used on Linux.
Outstanding Issues: IPv6 operating systems and browsers supporting IPSec are not yet available for all devices.
Industrial Benefit: A spectrum of devices is important to show the compatibility of 6WINIT

solutions with a wide range of user needs.

4.3.9.2 **Security Devices**
Functional Requirement: The ideal requirements are for strong authentication and user certification (including access control role-based profiles).
Proposed Technical Solution: PKI's and possibly Smart Cards. Coupling the proposed architecture with strong authentication tools (e.g. using tokens or biometric devices) would be ideal.
Outstanding Issues: Introduction of PKI
Industrial Benefit: This needs to be confirmed, since the demonstration of these security tools themselves is not the focus of 6WINIT.

4.3.10 Location Awareness

Functional Requirement: At present under consideration
Proposed Technical Solution: Initial discussions with 6WINIT partner VTT.
Outstanding Issues: TBD
Industrial Benefit: -

4.4 GANS at IST 2001 - towards clinical applicability

Beyond its technical achievements, the demonstration at IST 2001 showed that the concept of the GANS is viable. Visiting clinicians and the teams in Düsseldorf and Tübingen were convinced that such a system could be very helpful to enhance care of critically ill patients, undergoing problems which are not sufficiently treatable by the local medical team.

The team of UKT, RUS, Ericsson and others was able to perform multiple live tele-coaching sessions from Düsseldorf, Germany to the UKT hospital emergency room, where the simulator underwent several severe clinical problems.

The following pictures of the IST2001 demonstration show the various technical, medical and PR-aspects of the Guardian Angle System. The 6WINIT GANS demonstration booth (Fig. 14-17) was attracting a lot of interested and interesting people. There were school classes as well as the European Commissioner for Enterprise and the Information Society Erkki Liikanen among the visitors.

Figure 15: The 6WINIT GANS demonstration booth - always surrounded

Figure 16: The overall view of the 6WINIT GANS booth at IST2001

Whenever needed, the team of UKT, RUS, Ericsson and others was able to perform live telecoaching sessions between Düsseldorf and Tübingen hospital, where the patient simulator underwent several severe clinical problems.

The demonstration showed a local medical team in an emergency room in Tübingen Hospital (IPv6 PATIENT VIDEO in Figure 16) trying to treat a patient in a life threatening situation. While the patient's state was getting worse, the medical team in Tübingen called the medical experts in Düsseldorf. The combination of online-video, online-audio-connection (via phone) and vital data (VITAL DATA MONITOR in Figure 16) enabled the expert to evaluate the emergency immediately and give helpful advice to the team on spot. Due to this telecoaching it was possible to save the patient's life.

From the medical point of view, the particular importance of the setting is the availability of these different data without any interference and delay. This allows the expert to act as if he were on the scene himself.

Figure 17: The 'patient' in Tübingen and its vital data as seen in Düsseldorf - JMF/JDK1.4/IPv6 and Ericsson's Multi-Access MIPv6

Figure 18: The Ericsson Multi-Access control screen in Tübingen - transmitted via MIPv6 (1), local low-rate video transmitted to Tübingen (2), low-rate video transmitted from Tübingen (3) - all transmissions via MIPv6 in Ericsson's Multi-Access implementation

Beyond its technical achievements, the demonstration at IST 2001 showed that the concept of the GANS is viable. Visiting clinicians and the teams in Düsseldorf and Tübingen were convinced that such a system could be very helpful to enhance care of critically ill patients undergoing problems which are not sufficiently treatable by the local medical team.

5 ACRONYMS AND ABBREVIATIONS

2G	Second Generation Mobile Telecommunications (including GSM and GPRS technologies)
3DES	Triple Data Encryption Standard
3G	Third Generation Mobile Telecommunications (including WCDMA/UMTS technology)
3GPP	3rd Generation Partnership Project
6WINIT	IPv6 Wireless INternet IniTiative
AAA	Authentication, Authorisation and Accounting
ACC	Academic Computer Centre "Cyfronet", a part of the UMM
ACL	Asynchronous Connectionless Links
ADPCM	Adaptive Differential Pulse Code Modulation
AF	Assured Forwarding
AH	Authentication Header (IPsec)
AIIH	Assignment of IPv4 Addresses to IPv6 Hosts
ALAN	Application Level Active Networking
ALG	Application Layer Gateway
AM_ADDR	Active Member Address
AN	Active Networking
ANP	Anchor Points
AP	Access Point
API	Application Level Interface
AR	Access Routers
AS	Application Server
ATM	Asynchronous Transfer Mode
BACK	Binding Acknowledgement
BAKE	Binding Authentication Key Establishment
BD_ADDR	Bluetooth Device Address
BGP	Border Gateway Protocol
BGW	Border Gateway
BNEP	Bluetooth Network Encapsulation Protocol
BSS	Base Station System
BU	Binding Update
CA	Certificate Authority
CBR	Committed Bandwidth Rate

CCU	Clinical Care Unit
CEN	Comité Européen de Normalisation
CHIME	Centre for Health Informatics and Multi-professional Education
CHTML	Compact HTML
CLI	(1) Calling Line Identification
	(2) Command Line Interface
CN	Correspondent Node
COPS	Common Open Policy Service
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CRL	Certificate Revocation Lists
CRTP	Compressed RTP
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CSP	Cryptographic Service Provider
DAO	Data Access Objects
DCF	Distributed Co-ordination Function
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DIAC	Dedicated Inquiry Access Code
DMZ	Demilitarised Zone
DNS	Domain Name Server/System
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DSSS	Direct Sequence Spread Spectrum
DSTM	Dual Stack Transition Mechanism
DTI	Dynamic Tunnelling Interface
DTMF	Dual-Tone Multi-Frequency
DiffServ	Differentiated Services
DoS	Denial of Service
Dx	6WINIT Deliverable x
ECG	Electrocardiogram/graphy
EEP	Execution Environment for Proxylets
EF	Expedited Forwarding
EHR	Electronic Healthcare Record
EJB	Enterprise JavaBeans Components

EPR	Electronic Patient Record
ESP	Encapsulation Security Payload
ETRI	Electronics and Telecommunications Research Institute
ETSI	European Telecommunications Standards Institute
FDD	Frequency Division Duplex
FHSS	Frequency Hopped Spread Spectrum
FQDN	Fully-Qualified Domain Name
GANS	Guardian ANgel System (UKT-RUS)
GB	Gigabyte (10^9 bytes)
GEK	Group Encryption Key
GGSN	Gateway GPRS Support Node
GIAC	General Inquiry Access Code
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GSN	GPRS Support Node
GTP	GPRS Tunnelling Protocol
GW	Gateway Routers
HA	Home Agent
HCSS	Health Care Service System
HI	Host Identity
HLR	Home Location Register
HMIP	Hierarchical Mobile IP
HTML	HyperText Mark-up Language
HTTP	HyperText Transfer Protocol
ICMP(v6)	Internet Control Message Protocol
ICP	Internet Content Provider
ICU	Intensive Care Unit
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Multicast Protocol
IGP	Internet Gateway Protocol
IKE	Internet Key Exchange
IMS	Interactive Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol

IPSec	IP Security Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Information Society Technologies
ITU	International Telecommunications Union
IntServ	Integrated Services
J2EE	Java 2 Enterprise Edition
JDBC	Java Database Connectivity
JPEG	Joint Photographic Experts' Group
JSP	Java Server Pages
KLIPS	Kernel IPSec Support
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LI	Lawful Interception
MAN	Metropolitan Area Network
MDML	Market Data Mark-up Language
MGW	Media Gateway
MIP	Mobile Internet Protocol
MIP WG	Mobile IP Working Group
MN	Mobile Node
MSC	Mobile Service Centre
MT	Mobile Terminal
Mb/s	Megabits per second
NAI	Network Access Identifier
NAPT-PT	Network Address Port Translation - Protocol Translation
NAS	Network Access Server
NAT-PT	Network Address Translation - Protocol Translation
NHS	National Health Service (United Kingdom)
NRN	National Research Network
O&M	Operations and Management
OCSP	Online Certificate Status Protocol
PAN	Personal Area Networking
PCM	Pulse Code Modulation

PDA	Personal Digital Assistant
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PDP	Packet Data Protocol
PDR	Per Domain Reservation
PDU	Protocol Data Unit
PEP	Policy Enforcement Point
PHB	Per-Hop Behaviour
PHR	Per-Hop Reservation
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PPP	Point-to-Point Protocol
PS	Paging Servers
PSK	Phase Shift Keying
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RADIUS	Remote Access Dial-in User Server
RAN	Radio Access Network
RAS	Remote Access Server
RAT	Robust Audio Tool
RFC	(Internet) Request for Comments
RMD	Resource Management in DiffServ
RMI	Remote Method Invocation
RODA	Resource Management in DiffServ On DemAnd
ROHC	Robust Header compression
RSA	Rivest-Shamir-Adleman (encryption algorithm)
RSVP	Resource ReSerVation Protocol
RTCP	RTP control protocol
RTP	Real Time Transport Protocol
RUS	Rechenzentrum Universität Stuttgart
SA	Security Association(s)
SADB	Security Association Database
SCEP	Simple Certificate Enrolment Protocol
SCO	Synchronous Connection Oriented
SCS	(1) Secure Conference Store

	(2) Service Capability Server
SGSN	Serving GSN
SGW	(1) Signalling Gateway
	(2) Security Gateway
SIIT	Stateless IP/ICMP Translation Algorithm
SIP	Session Initiation Protocol
SN	Service Network
SNMP	Simple Network Management Protocol
SPD	Security Policy Database
SRTP	Secure Real Time Transport Protocol
SSL	Secure Socket Layer
SecGW	Security Gateway
TB	Tunnel Broker
TCP	Transmission Control Protocol
TDD	Time Division Duplex
TDD	Time Division Duplex
TE	Terminal Equipment
TEID	Tunnel Endpoint IDentifier
TEIN	TransEurasia Information Network
TLA	Top Level Aggregator
TS	Tunnel Server
ToS	Type of Service
UAC	User Agent Client
UAS	User Agent Server
UCL	University College London
UDP	User Datagram Protocol
UKT	Universitätsklinikum Tuebingen
UMM	University of Mining and Metallurgy (Krak¢w, Poland)
UMTS	Univeral Mobile Telecommunications System
UR	User Registries
UTRA	Universal Terrestrial Radio Access
VJ	Van Jacobsen
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VPN	Virtual Private Network
VTT	Technical Research Centre of Finland

VoIP	Voice over IP
W3C	World-Wide Web Consortium
WAE	Wireless Application Environment
WAN	Wide Area Network
WAP	Wireless Application Protocol
WCDMA	Wideband Code Division Multiple Access
WDP	Wireless Datagram Protocol
WEP	Wire Equivalent Privacy
WLAN	Wireless Local Area Network
WML	Wireless Mark-up Language
WTA	Wireless Telephony Application
WTLS	Wireless Transport Layer Security
WWW	World-Wide Web
XHTML	Extensible Hypertext Mark-up Language
XML	Extensible Markup Language