ACTS Project AC052

PROSPECT

D21B - Final Requirements Analysis

Document Number:	*AC052/DLT/WP2/DS/P/027/b1*
Contractual Date of Delivery to CEC	*30th June 1997*
Actual Date of Delivery to CEC	*30th June 1997*
Editor:	*Anders Gammelgaard, DELTA*
Deliverable Nature	*R-Public Report*
Deliverable Type	*K-Major Deliverable*
Work Package Contributing:	*WP 2*

Abstract: This document contains requirements for Trial 2 - the final Prospect trial. The requirements come from various sources; end-user's in Prospect Trial 1 and a set of Trial 1 assessors have evaluated the Trial 1 system and suggested enhancements and extensions for Trial 2; implementors have likewise provided feedback; additionally the Prospect Consortium has decided new directions to follow for the next trials. Many requirements can be seen as enhancements to services already provided for Trial 1, other requirements are new - in particular the requirements on mobility, security, performance management and fault management.

Keywords: Trials, End-user Requirements, Project Requirements, Management, Broadband Communication, Tele-education.

Organisations in the Prospect Consortium are:
Broadcom Éireann research Ltd, Delta Danish Electronics Light & Acoustics, Deutsche Telekom Berkom GmbH, DSC Communications A/S, GMD Fokus, IBM Deutschland Informationsysteme, IONA Technologies, L.M. Ericsson A/S, Marben, Tele Danmark A/S, Trinity College Dublin, University College London, UH Communications ApS.

List of Authors

Lennart H. Bjerring	LMD
Ralf Bracht	IBM
Anders Gammelgaard (Editor)	DLT
Michael Höft	GMD
Hervé Karp	MRB
Dave Lewis	UCL
Conor Power	TCD
Cliff Redmond	TCD
Mark Riordan	TCD
Martin Schwetje	DTB
Lars Bo Sørensen	UHC
Thanassis Tiropanis	UCL

Copyright

The Prospect Consortium comprises:

Organisation Name	**Short Name**	**Country**
Broadcom Éireann Research LTD (Prime)	BRI	Ireland
DELTA Danish Electronics, Light & Acoustics	DLT	Denmark
Deutsche Telekom Berkom GmbH	DTB	Germany
DSC Communications A/S	DSC	Denmark
GMD FOKUS	GMD	Germany
IBM Deutschland Informationsysteme	IBM	Germany
IONA Technologies	IONA	Ireland
L.M. Ericsson A/S	LMD	Denmark
MARBEN	MRB	France
Tele Danmark A/S	TDK	Denmark
Trinity College Dublin	TCD	Ireland
UH Communications Aps	UHC	Denmark
University College London	UCL	United Kingdom

Executive Summary

The main aim of Prospect is to develop integrated inter-domain management systems for broadband communications within the context of the envisaged open service market. These management systems are tested through trials that involve real end-users. In order to make trials realistic and demanding and in order to demonstrate the benefits of end-to-end management in heterogeneous environments, Prospect also develops tele-education applications that exploit and depend on the management systems. The trials are consequently disguised as tele-education courses.

The first Prospect trial - Trial 1 - took place in March 1997 and involved course participants from four European countries. In 1997/1998 the Prospect Consortium will conduct two end-user trials, Trial 2.1 and Trial 2.2. These two trials together constitute Trial 2 - the main event in the Prospect project. The present document describes the requirements on the system that will be constructed for these two trials.

Requirements are captured from various sources, the major source being experience from Trial 1 that Prospect conducted in March 1997. Experience from Trial 1 consists of feedback from end-users, reports from a number of assessors and of a thorough analysis that the designers and implementors of the system undertook right after Trial 1. In addition to this Prospect has also decided to extend the system from Trial 1 with new features, most notably with features that support personal communications and security.

The present document just summarises the experience from Trial 1 - a detailed analysis of the trial can be found in [Prospect D53A]. One part of the analysis *does* appear in the present document, however; this part is the response to a set of questionnaires that were handed out to systems administrators; due to technical problems a full integration of all management systems was only possible shortly after Trial 1 and the response to the questionnaires was therefore delayed too much to be included in [Prospect D53A].

This page intentionally left blank

TABLE OF CONTENTS

This page intentionally left blank

Acronyms

(Notice: acronyms for companies within the Prospect Consortium appear at back of the front page)

ABR	Available Bit Rate
API	Application Programming Interface
ARS	Action Request System
ATM	Asynchronous Transfer Mode
B-ISDN	Broadband ISDN
BMSec	Berkom Management Security
CA	Certification Authority
CA	Customer Administrator
CBR	Constant Bit Rate
CCITT	Comité Consultatif International Telegraphique et Telephonique (now ITU-T)
CDV	Cell Delay Variance
CLP	Cell Loss Probability
CME	Conformant Management Entities
CMIP	Common Management Information Protocol
CO	Computational Object
CORBA	Common Object Request Broker Architecture
COS	Common Object Services
CPN	Customer Premises Network
CTD	Cell Transfer Delay
DSI	Desktop Service Integration
ETSI	European Telecommunications Standards Institute
FCAPS	Fault, Configuration, Accounting, Performance and Security
GDMO	Guidelines for the Definition of Managed Objects
GOM	Generic Object Model
GUI	Graphical User Interface
HM	Hyper Media
HTML	Hyper Text Meta Language
HTTP	Hyper Text Transfer Protocol
ICE-TEL	Interworking Public Key Certification Infrastructure for Europe
IDL	Interface Definition Language
IDN	Interface Definition Notation
IETF	Internet Engineering Task Force
IIOP	Internet Inter-ORB Protocol
IP	Internet Protocol
IPv6	IP version 6

ISDN	Integrated Services Digital Network
ISM	Integrated Service Manager
ITU-T	International Telecommunication Union - Telecommunication Standardisation Sector
JMAPI	Java Management API
LAN	Local Area Network
MB	Mega Byte
MBONE	Multicast Backbone
MERCI	Multimedia European Research Conferencing Integration
MIB	Management Information Base
MISA	Management of Integrated SDH and ATM networks
MMC	Multi Media Conferencing
MMTS	Multi-Media Tele-Service
NAP	Network Access Point
NCA	Network Computing Architecture
NMF	Network Management Forum
NTP	Network Time Protocol
ORB	Object Request Broker
OS	Operating System
OSI	Open Systems Interconnection
OSM	Open Service Market
PA	Provider Administrator
PCS	Personal Communications Support
PIN	Personal Identification Number
PLASMA	PLAtform for Secure Multimedia Applications
PN	Public Network
PP	Personal Profile
PSE	Personal Security Environment
QoS	Quality of Service
RACE	Research and Development Programme in Advanced Communications in Europe
RAT	Robust Audio Tool
RC	Random Certificate
R&D	Research and Development
RM	Referenced Model
RSVP	Resource reSerVation Protocol
RTP	Real Time Protocol
SA	Service Architecture
SAG	Subscription Assignment group

SK	Symmetric Key
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
URL	Uniform Resource Locator
USM	User Service Session Manager
TANGRAM	Framework for Development of Telecommunications Applications in Open Distributed Systems
Tcl	Tool Command Language
TCOS	Telesec Chipcard Operating System
TCP	Transmission Control Protocol
TEN34	Trans-European Network (interconnected at min. 34Mbps)
TES	Tele-Educational Service
TESP	Tele-Educational Service Provider
TINA	Telecommunications Information Networking Architecture
TINA-C	TINA Consortium
Tk	Tool kit
TMN	Telecommunications Management Network
TP	Termination Point
TRP	Translation Point
TRUMPET	Inter-Domain Management with Integrity
TS	Time Stamp
UA	User Agent
UAP	User Application
UAP	User Application in the Provider domain
UBR	Unspecified Bit Rate
UM	Usage Monitoring
VBR	Variable Bit Rate
VCI	Virtual Circuit
VIC	Video Conferencing tool
VITAL	Validation of Integrated Telecommunication Architectures for the Long Term
VP	Virtual Path
VPN	Virtual Private Network
VR	Virtual Reality
VRML	Virtual Reality Modelling Language
WWW	World Wide Web

This page intentionally left blank

1 Introduction

The aim of Prospect is to develop management systems for broadband communications. These management systems are tested through trials that involve real end-users. In order to make trials realistic and demanding and in order to demonstrate the benefits of end-to-end management in heterogeneous environments, Prospect also develops tele-education applications that exploit and depend on the management systems. The trials are consequently disguised as tele-education courses.

The first Prospect trial - Trial 1 - took place in March 1997 and involved course participants from several European countries. The requirements on the Trial 1 system are documented in [Prospect D21A] and an evaluation of the trial appears in [Prospect D53A]. For a condensed overview of the Prospect approach, consult [Prospect World].

Trial 2 will test a complicated system. Requirements on this system come from different sources. Experience with the preparation of Trial 1 is one source, user's opinion about the resulting system is another, and Prospect partners' expressed intention for future developments is a yet another source. In this document the available information from each source is compiled and analysed.

All main requirements to the Trial 2 system are documented here. It should be observed, though, that many non-functional requirements are outside the scope of the present document, e.g. the subject and content of Trial 2 tele-education courses and the topology of the backbone network. On the other hand some non-functional requirements *are* described in this report - in particular requirements on the look and feel of graphical user interfaces (GUIs). It should likewise be observed that since several Trial 1 components will be reused in Trial 2, many requirements on Trial 2 have already been described in the requirements analysis for Trial 1 (see [Prospect D21A]).

Trial 2 will in fact consist of two trials: Trial 2.1 and Trial 2.2. The main reason for this split is that ATM links from the James project will only be available until February 1998. Trial 2.1 will take place before the end of this period in order to be able to exploit existing ATM links. For Trial 2.2 other network infrastructure will be sought, such as existing Internet and EuroISDN or other high speed network infrastructure such as TEN34. Although this split is really motivated by a change in infrastructure, Prospect has decided to pursue different goals in the two trials. Trial 2.1 will mainly be focused around consolidating, restructuring and slightly enhancing the system from Trial 1 whereas Trial 2.2 will expand into new user and management features- in particular into management services that support mobility and security.

Notice that "Trial 2" will be used throughout this document to stand for "Trial 2.1 and Trial 2.2". Specific reference to Trial 2.1 or Trial 2.2 will only be made when distinguishing between these two trials is important.

This document has the following structure. First the requirements from Trial 1 end-users are analysed. Then requirements from within the project are presented. These are requirements that arose either as reactions to experiences in developing and operating the Trial 1 system, new ideas for including extra functionality into the system or recent developments from other projects and standards bodies. These project requirements are presented in two chapters: the first addressing functional areas, the second addressing services and components from Trial 1.

2 End-user requirements

Experience from Trial 1 has been collected in deliverable D53A. Notice, however, that only a preliminary assessment of the management systems has been done in D53A; problems with the integration of Trial 1 management systems caused a delay in the assessment process, a delay that hindered the material to be included in D53A. Instead section 2.2 and Annex A in the present deliverable contain the relevant material.

2.1 Requirements from TES end-users

The following is just an excerpt of main conclusions on Trial 1. Full details can be found in D53A. The evaluation stems both from end-users' feedback to questionnaires and from a set of evaluators who observed Trial 1.

Analysis is obviously needed to derive requirements from the feedback from end-users. In many cases the feedback takes the form of proposals for new directions to follow rather than firm requirements on desired functionality. Experimentation is needed and Prospect will therefore conduct a number of pre-trials before Trial 2 - just like Prospect did before Trial 1.

Notice that eventually teachers will be real end-users; in Trial 1 and the pre-trials before Trial 1, though, they were members of the Prospect Consortium. Input from teachers has therefore not been counted as input from end-users and input from the teachers is presented instead in sections 3 and 4 of this document.

2.1.1 Tools

The Netscape browser was used in Trial 1 to enable end-users to log in and move around within the virtual course facilities and to fetch the course material; the functionality of the browser had been extended through a set of Java applets and Javascripts. Communication between end-users was mediated by the audio/video tools RAT and VIC. Main conclusions on these tools are:

Audio was generally working well, but a few times the connections were unstable. The RAT panel also occasionally gives erroneous or conflicting information. Both these problems apparently only happen when one or more PCs participate in an audio session. In Trial 2 the RAT implementation for PCs should therefore be enhanced so as to reach same quality as its present implementation for Solaris.

Video quality was not perceived as being sufficient. Especially the participants missed a larger and more synchronised picture of the teacher during lectures. Screens with only 256 colours loose their colour map allocation when mouse focus is moved from one window to another, causing a distracting flickering effect. In Trial 2 the TES system must automatically detect screens with this few colours and start VIC in an appropriate mode. Alternatively only video cards with sufficient colours should be used.

The shout tool was frequently used and was felt to be a good supplement to audio/video communication. It should be enhanced, though. All messages should be printed to a fixed message window that is brought to front each time a message arrives; sending replies should also be facilitated compared with the present implementation where a user has to compose an entirely new message when replying.

Shared white boards were used extensively by the participants, but should be enhanced in several ways. The facilities to point were not sufficient; each student should be given a default pointer that can display continuous mouse-movements; furthermore, some users mentioned that it is difficult to control movements with the mouse carefully enough. Enhanced pointers should therefore be developed. Pointing should also be supplemented with other tools for focusing attention to particular parts of a page. It was also mentioned that each participant could be given an additional white board where personal notes and sketches can be put down, but only if such a white board can serve its purpose better than pen and paper.

2.1.2 Contact between participants

Participants feel that there is little social contact with other students. This has the consequence that students get afraid of interrupting lectures with questions and that they appear to be quite inactive initially in group work. It was suggested that the very first session in a course should be devoted just to getting acquainted with the tools and the other participants.

The participants still find it difficult to figure out what is really going on during a course - even though the course environment contains cues about who is where. In a few cases it took a long time before it was detected that some machine had failed and in one lecture the teacher did not discover that nobody could see that he was changing slides; it could help to introduce indicators that repeatedly check that everybody has reached a common stage. Likewise, during lectures the students found it difficult to figure out how much the other students understood, and this also made them afraid of interrupting for asking questions. In general methods should therefore be sought that can provoke and stimulate active student participation.

A nice feature in real life discussions is that people can immediately split into smaller groups if they so desire. This was not possible in Trial 1, where the participants in each group were determined in advance.

More careful control should be exercised over the communication tools. In lectures e.g. there should be a default mode where the teacher's image is displayed in high quality. If somebody poses a question, this image should change to the questioner. Group work could similarly use a timer to switch between participants as long as nobody says anything, and change to "video follows audio" when people start to discuss. Furthermore, in lectures it would be a good idea to introduce a faster mechanism for interrupting the teacher than using the shout button.

2.1.3 Concentration

The participants felt that it was difficult to concentrate. There were many reasons for this. In general people feel it difficult to concentrate in front of a screen - it would be nice if especially pages in the self-study modules could be printed out, so that the binding to the screen could be loosened a bit. There was also too much background noise in some of the offices - people enter and leave the office or the telephone rings. If possible such noise should be eliminated. A dedicated work environment would be preferable.

2.1.4 Miscellaneous

In group exercises there should be more links to other course material that has already been presented. This may pose a problem, though, since the course facilities are structured like a building where you enter and leave rooms. Using links to already presented material should therefore bring up the material in a way that makes it apparent that the material is a digression from the normal course of events. Putting the material in a separate pop-up window might be an idea. Also, browsing through such already seen material may call for the usual go-back mechanism found in web-browsers - a feature that was deliberately excluded from the course environment in Trial 1. .

The font size should be increased in many parts of the self-study modules.

2.2 Requirements from TES administrators

The management system for the tele-education service was trailed in a separate event after the actual Trial 1. In the following the main results are presented. The evaluation is merely based on interviews of management users and reports from observers.

2.2.1 Graphical User Interface

Main criticism of both management users and observers was the missing help-function in the application windows. It was felt to be very difficult to fill in the fields without having access to additional explanations. A context-sensitive help-function would ease the use of the system and would allow administrators to work with the system without being guided by tutors or manuals. In addition, a road map through the system would be helpful, especially for beginners.

It was felt that the layout of application windows has to be improved. In many windows selection lists would ease choosing of names and IDs. Users also encountered problems when displaying the fixed-size fonts on their platform. Some buttons are still sensitive during operation of an operation, although the application is busy. It was suggested to change the shape of the cursor to indicate that an operation is currently executed.

Most users complained about the slow performance of the interface. Sometimes it took several minutes until the management application responded to an action. One reason for the bad performance was the slow connection from the client to its management server over the public Internet. But examinations undertaken afterwards unveiled that even in an ideal environment, both client and server running on a high-end workstation, some actions took a few seconds or more. Further investigation revealed that the main reason for the long delays came from a misconfiguration of the TES service during Trial 1.

Quite often the users encountered problems because the system reported faults the users were not able to understand. This behaviour on the one hand stems from incomplete implementation of interface and management system, on the other hand from insufficient testing procedures. Detailed prescriptions for implementation and testing are recommended in order to ensure high quality of the software components.

2.2.2 Functionality

Nearly all users stated that the functionality of the subscription management interfaces is sufficient. TES customer administrators mostly used user and site management functions. Functions for displaying customer and service information, however, were found to be unnecessary. TES provider administrators used all provided functions equally. Generally, all end-users appreciated the on-line ordering capability provided by the management system.

On the other hand, most users stated that the accounting management functionality should be extended. Provisioning of rates and bills is important and essential, but in addition access to detailed usage data would be beneficial. For instance, usage data per user and per service may be helpful in order to compare service utilisation by different students.

Part of the questionnaire for administrators was the question how users assess the importance of a number of management functions. The results are presented in the following list (9: very important - 0: not important):

on line subscription and de-subscription to the service	8
automatic installation and configuration of the service	6.5
changing subscription details, e.g. adding new users and sites	9
on line payment of the course	8
receiving charging information, e.g. rates and bills	6
receiving accounting information, e.g. service usage per user	9
receiving performance information, e.g. network load	4.5
receiving notifications about violations of service level agreements	7
receiving security related notifications, e.g. failed authentication	7

As mentioned above, on-line subscription and the possibility to change subscription details and to get access to accounting information have highest priority. But on-line payment of the service and security management is also regarded as very important. In an extra question end-users were asked how they assess the technology currently used for e-commerce over the public Internet. All users stated that the available technology is not secure enough, but they would use these procedures as soon as they become verifiable secure. Therefore, a detailed investigation of combined security and e-commerce technology is recommended and it should be examined whether an e-commerce extension is feasible.

According to the assessment of the end-users, performance or Quality-of-Service (QoS) management should also be supported by the management system. In an additional question the administrators were asked to rate several performance management functions. It was strongly recommended to link rates and QoS levels, i.e. to charge based on the QoS level provided. A Service Level Agreement (SLA) should be concluded and violations against this agreement should be reported to the customer automatically. However, dynamically changing the QoS level is of less importance.

Administrators were also asked which fault management functions they want to be included in the management system. Generally, it was felt that fault detection and recovery is a responsibility of the service provider. Hence, detailed fault reports to the customer are unnecessary. On the other hand, a policy how to handle service malfunctions is needed and may be included in the service contract. Most wanted functions are: immediate support, e.g. contact to help desk personnel and notification of scheduled or estimated service down-time by the provider.

Additional management functionality may be needed in order to provide the customer with the capability to connect to the service from different locations and terminals. End-users were asked to state which types of mobility they expect. Role mobility, i.e. a person is able play different roles like student or teacher simultaneously, and personal mobility, i.e. the ability to connect to the service from different locations e.g. from their office and their home, are regarded as the most important types of mobility.

Finally, two other valuable recommendations have to be mentioned. A lot of administrators daily encounter problems when installing software components. Therefore, it is not surprising that easy-to-use installation and configuration procedures are requested. Administrators also proposed to log all interactions between the customer and the service provider. This could be useful especially if disagreements between customer and provider exist.

3 Project requirements - management functions

Preparation of Trial 1 provided much experience to the Prospect team. Some of this experience directly lead to requirements on the Trial 2 system. In parallel with the preparation of Trial 1 Prospect also discussed and decided on which new directions to follow in the next phase of the project. All such requirements originating from within the Prospect project are documented in the present section and in section 4. The focus in the present section is to identify and outline the different management functions that will be supported in Trial 2 - new functions for PCS support, fault handling, QoS management, security and enhanced functions that deal with security and subscription and allows accounting and usage information to be retrieved.

3.1 Personal Communications Support

As stated in the project proposal, one of the objectives of Prospect is to introduce Personal Communications Support (PCS) for Trial 2. PCS mainly covers two areas:

1. Mobility
2. Personalisation of services

Before investigating how to support each of the above aspects it is necessary to identify them more clearly. In this section, the different kinds of mobility are defined, personalisation of services is investigated and some high level requirements and scenarios are produced.

3.1.1 State of the art

Various kinds of mobility have been identified in Prospect, the main ones being personal, terminal, session and role mobility.

- Personal mobility allows for a person to move between different terminals.
- Terminal mobility allows for terminals to move between different Network Access Points (NAP).
- Session mobility is a concept borrowed by TINA which allows a user to suspend a service session and resume it from a different terminal.
- Role mobility allows for a role (e.g. a service administrator or a personal tutor for the students of the TES service) to move to another person. For example, the attribute of the service administrator role can move from one service operator in the morning to another operator in the afternoon so that a group of operators can carry this role in shifts. The parameters according to which a role can move from person to person need not necessarily be time; it could also be the identity of the caller, the number of calls each role-holder received over a period of time, and others. Roles can be divided to service independent roles, like the service administrator, or service dependent roles, like the personal tutor of the TES service.

The location of a role is the ID of the person that a role is attached to at each moment.

The location of a person is the ID of the terminal that a person wishes to start a service from at any moment.

3.1.1.1 Personalisation

Personalisation of services concerns the use and maintenance of Personal Profiles (PP) which can allow persons to configure their service environments in the most desirable way. For example, a person can specify in this profile a list of potential callers which can contact this person any time, while all the other callers not included in this list can be redirected to an answering machine type of service. Related work has been conducted in RACE-II, TINA and TINA auxiliary projects on PCS.

3.1.2 Requirements

In Prospect personal mobility was given the highest priority together with role mobility which addresses interesting management aspects. For these kinds of mobility the following entities are involved: roles, persons and terminals.

There is a requirement for unique IDs which can allow a role to be identifiable, locatable and therefore, mobile. In the role associated with a particular service, the scope of the role IDs is confined within a service provider. In the service dependent roles the management of role IDs can be left up to the service provider. For service independent roles the management of the role IDs can either be left to the service provider or it can be standardised, e.g. the role ID 23 can be for the service administrator of any service. There is no requirement in Prospect for role IDs to be standardised.

There is a requirement that persons and terminals have unique IDs which can allow them to be identifiable, locatable and easy to authenticate and therefore, mobile. Since a person or a terminal can be involved in more than one service their IDs have to be provider independent. This brings up a requirement for an enterprise entity that will manage the assignment of provider independent IDs to persons and terminals. This entity can either be the Prospect Trial 1 VPN provider, the Security provider or a special Personal Communications Support (PCS) provider. Prospect decided that the option of a PCS provider was the cleanest and the most reasonable one.

In order to support personal mobility a provider independent entity has to delegate for the person for the transactions with different services providers’ systems that the person is subscribed to. This entity has to hold the customisable personal preferences and intelligence regarding the handling of service invitations that a person can receive (e.g. call redirect, call barring, etc.). Therefore, a single, service provider independent User Agents (PCS-UA) and associated Personal Profiles (PCS-PP) for the users is required. The PCS-UAs can communicate directly with the service provider's systems or via the Trial 1 provider specific UAs in Prospect.

The PCS-UA can also hold the location of a person. It is important to have one PCS-UA per person so that the location of a person has to be maintained in only one place. This requirement is also important for security reasons.

There is a strong requirement in Prospect for end-users to be able to subscribe to services independently if they wish to and not only via the Tele-education service (TES). Therefore, the functionality and the interfaces of the Trial 1 UAs have to be maintained. The Trial 1 UAs can be extended with additional functionality and an additional interface that can support the communication between the PCS-UAs and the existing Trial 1 UAs of each service provider.

In terms of personalisation, if a person is accessing a service provider specific UA directly, the personal profile maintained by that UA is used. If a person is accessing a service provider specific UA via the PCS-UA, the PCS-PP overrides all other personal profiles.

3.1.3 Scenarios

The objective of the following scenarios is to depict enterprise entities and outline the information exchanged among them in order to support role mobility. Apart from the enterprise entities, some functional components are also outlined in order to give an insight into system design requirements.

The following scenarios do not comprise a specification but rather a high level requirements analysis for the system model for Trial 2.

3.1.3.1 Trial 2 considerations

The biggest change in the scenarios of Trial 2 is the introduction of a call model for setting up service sessions. This means that a user should be able to invite other users directly and set up service sessions with them. The call model is necessary in order to demonstrate: the concept of personal mobility, i.e. that of one end-user being able to contact (invite, or call) another end-user regardless of their location (the terminal they are attached to).

In the Trial 2 scenarios, end-users can invite others to take part in a communications session via their PCS-UAs. The location of the end-users is held by their PCS-UAs. The location of an end-user can be given by a PCS-UA only to trusted parties.

Out of the four identified kinds of mobility, personal and terminal mobility - which are related to access to services - can be provider independent; this means that they can be provided by a separate provider/stakeholder. On the other hand, role mobility is more tightly coupled with the provider of a service, i.e. the provider must continuously update the mapping of role ids to user ids according to several and diverse parameters (e.g. time of day, priorities). Therefore, role mobility can be service independent for roles of the kind “service-administrator”, “service-operator”, or service dependent for general roles like the “tutor-on-call” of the tele-education service.

3.1.3.2 Entities

A number of entities are involved in the following scenarios:

- End-user Home Application: is the end user application installed on the home terminal of an end-user.
- End-user Office Application: is the end-user application installed on the office terminal of an end-user.
- User Location Server: is the database that holds the location of the PCS-UAs. It is used by the PCS-UAs of other users in order to contact the PCS-UA of a user they wish to invite to a service session. In the case that the location of a PCS-UA is transparent this entity can be replaced by the CORBA naming service or a broker.
- Role Location Server: is the database that holds the location (user IDs) of the role holders (i.e. the mapping of role id to user ids). It is owned by the TES provider who also has the responsibility of assigning appropriate roles to tutors in a way which is not shown in the scenarios.
- PCS-UA: is a user agent that delegates for an end-user in the service providers’ domain. It contains the end-users preferences, for example who can contact the user at specific times. It also contains the location of the end-user in terms of the terminal id they are attached to.
- Provider Management System: is the entity that implements the service management functions of the service provider.
- Provider Service System: is the entity that implements the service itself that is provided.

3.1.3.3 Tutor role mobility

This scenario involves a tutor that holds the role of tutor-on-call. The role can be passed from tutor to tutor according to time of day, etc. A student indicates to his user agent to start a service session with the tutor-on-call. Subsequently, a service session is set-up with the tutor who is holding the “tutor-on-call” role at that moment.

In these scenarios it is assumed that the role of “tutor-on-call” is assigned to tutors by the TES provider. The management interactions required for this are not shown in the scenarios.

The terms “person”, “user” and “end-user” are considered synonymous and they are used interchangeably in this document.

3.1.3.3.1 Road map

Scenario PCS_3_1 in Figure 1 gives a high level view of a tutor role mobility scenario. Other detailed sub-scenarios are represented as boxes (PCS_3_2, PCS_3_3, PCS_3_4, PCS_3_5). PCS_3_2 and PCS_3_3 of these sub-scenarios are specified as an example in Figure 2 and Figure 3.

Notation: Regular expressions notation is used in these scenarios. Wherever an asterisk (*) appears, it means that an operation can be performed zero or more times.

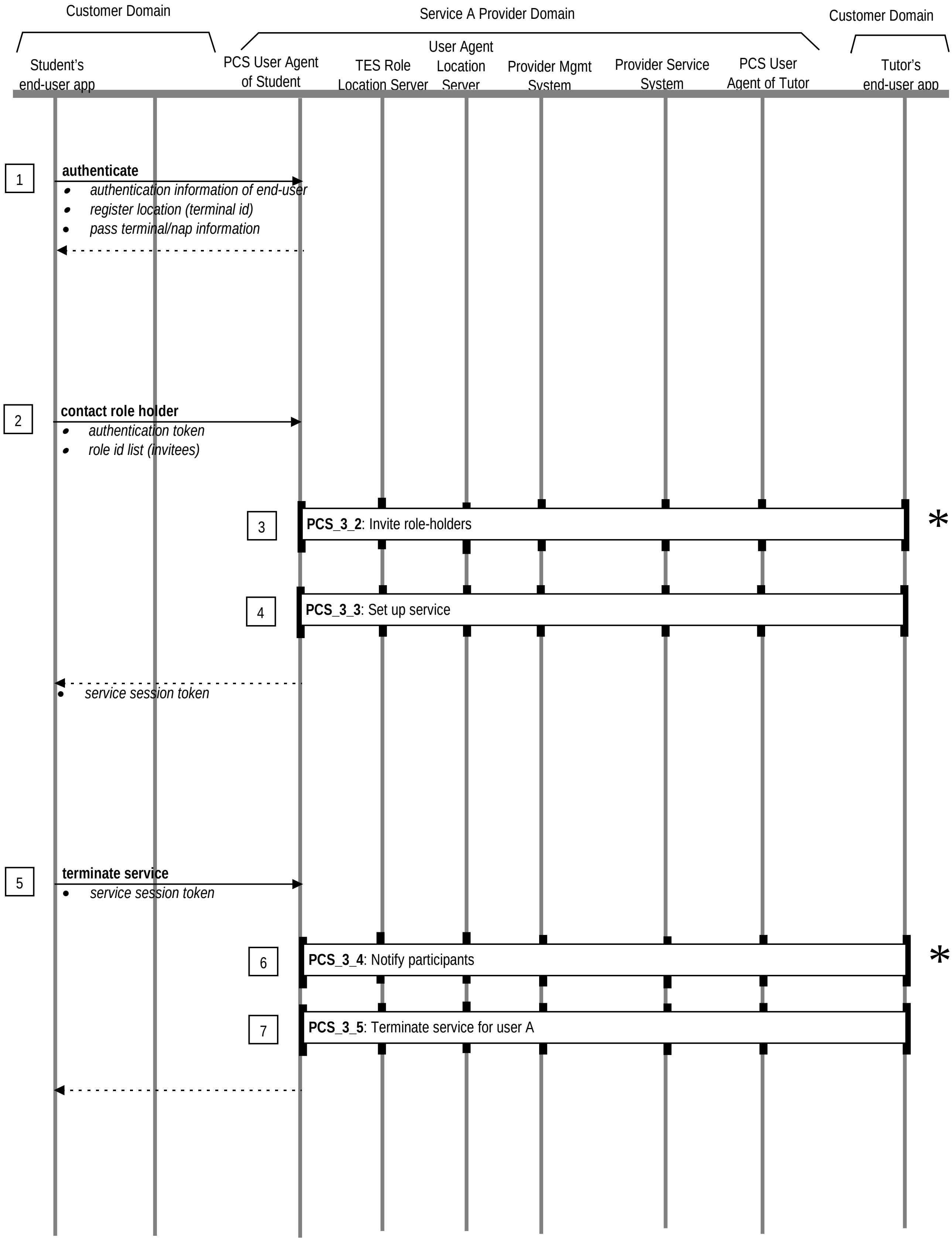


Figure 1: Scenario PCS_3_1; tutor role mobility

3.1.3.4 Scenario PCS_3_2

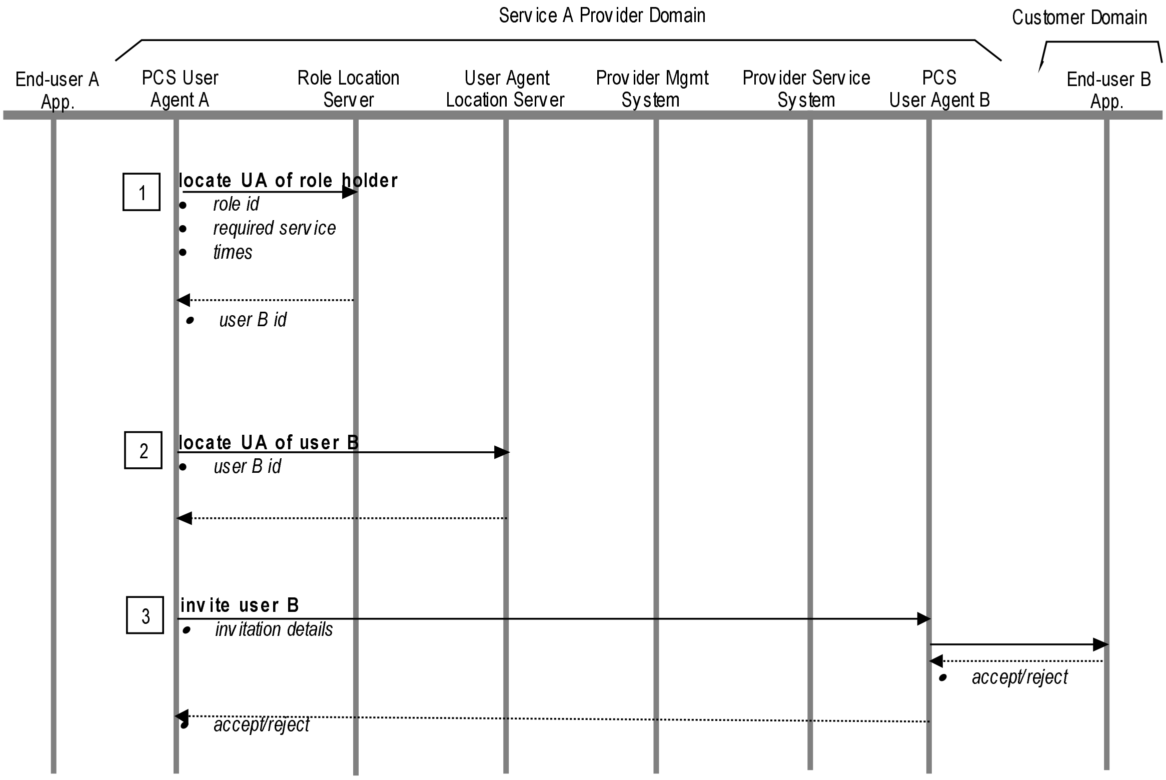


Figure 2: Scenario PCS_3_2; invite role-holders

3.1.3.5 Scenario PCS_3_3

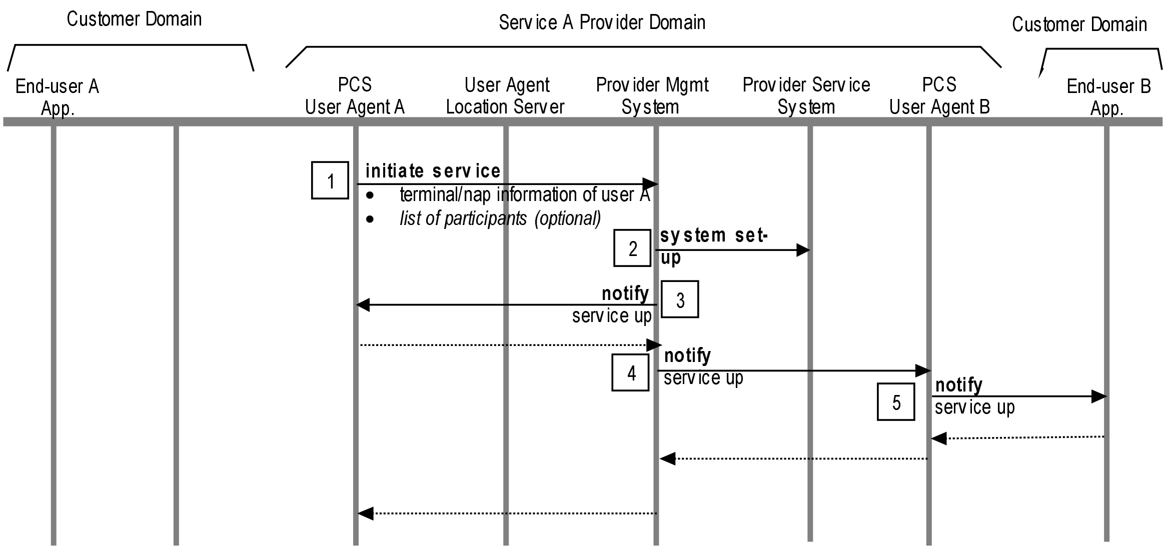


Figure 3: Scenario PCS_3_3; set up service

3.1.3.6 Service independent roles mobility

This scenario involves a service operator that holds the role of the administrator-on-call. The role can be passed from operator to operator according to time of day, etc. A student indicates to his user agent to start a service session with the administrator-on-call. Subsequently, a service session is set-up with the operator who is holding the “administrator-on-call” role at that moment.

In these scenarios it is assumed that the role of “administrator-on-call” is assigned to operators by the TES provider. This scenario is very similar to scenario PCS_3_3. The only difference is the nature of the role which in this case is service independent.

3.2 Fault Handling

From time to time, problems or malfunctions occur in all systems. These include failures in communications networks and services. Problems caused by failures have an adverse effect on the quality of service perceived by network and service users. Therefore, fault and performance management are closely related. Nevertheless, Prospect has chosen to focus on the handling of faults which arise in equipment and software systems of telecommunication services.

3.2.1 State of the art

The management of problems in service systems has two aspects: their handling after emergence by both service provider and customer, and their detection and recovery solely performed by the service provider. The former is often referred to as trouble administration or trouble ticketing, the latter could be called failure recovery handling and is an important task in systems, network, and application management. State of the art within both aspects are discussed next.

3.2.1.1 Trouble Administration

In several standards trouble administration functions and systems are described, e.g. in the ITU-T Recommendation X.790 [ITUT790] and in the NMF Trouble Administration Requirements Specification [NMF 501]. These standards deal with creation, resolution, clearing, closing, and archiving of trouble reports, also known as trouble tickets.

The ITU X.790 standard defines trouble management as trouble reporting and tracking between so-called Conformant Management Entities (CMEs), which interoperate co-operatively towards resolution of a trouble. Since this standard is based on TMN principles, both an agent and a manager role is defined. While in a manager role a CME manages problems and any corresponding trouble reports, in an agent role the CME is responsible for resolving a problem that has been raised to it by a manager role CME. A CME may act as manager and agent simultaneously. X.790 describes requirements on a trouble administration system and presents a detailed model of such a system. This object model is specified using GDMO.

In contrast to the ITU-T standard, the NMF document is restricted to the definition of the business context for customer to service provider trouble administration. Trouble administration is seen as a workflow application in which trouble reports are processed by operators in the customer’s and the provider’s domain. The specification is technology-independent, i.e. NMF does not prescribe use of TMN technology.

At present, a number of products for trouble administration are available in the marketplace. For example Remedy’s trouble ticketing system ARS [Remedy] is based on a workflow application and integrates workflow server and clients with a database. Remedy offers a WWW client and a help-desk extension. Open APIs provide integration of various technologies, e.g. TMN and CORBA. For instance, with IBM’s Fault Management Extension to their TMN platform [IBM], CMIP notifications can be submitted directly to the Remedy ARS in order to create trouble tickets.

3.2.1.2 Fault Recovery

Fault reporting and detection is subject for specification in all standardisation bodies and consortia in the telecommunication sector. In the following, the outcome of the main activities in this field is presented. It is worth mentioning that in this context fault recovery and configuration management are considered to be closely related. However, the actual resolution of a detected problem, e.g. re-configuration of the service, is out of scope of this section.

In the ITU Recommendation X.733 [ITUT733], one out of a series of TMN functional specifications, the so-called alarm reporting function is defined. Managed objects, specified in GDMO, may send CMIP notifications of the specific type alarm. Five basic categories of alarms are defined: communication alarm, quality of service alarm, processing error, equipment alarm, and environmental alarm. Besides the alarm type, the probable cause and severity of an alarm is specified. This function is largely used in agents controlling networks and network elements.

In addition to plain alarm reporting, telecommunications providers recently demand powerful algorithms for correlation of alarms. Today's telecommunications networks consist of thousands of network elements, adapter cards, and connections, hierarchically organised in a tree-like structure. In case of malfunction of a network component, a number of dependent elements and connections will also send problem reports. This may lead to an avalanche of alarms, a human operator is not able to control. A possible solution is the deployment of an expert system which uses pre-defined rules to correlate alarms in the network [Talarian], [IBM]. Alarms from dependent components can then be suppressed so that the detection of the origin of a problem is made easier.

Each network node and service application must be capable of sending an alarm if a problem emerges. In TMN agents controlling networks and network elements status attributes are defined for each managed object, i.e. for each network component. The agent sends CMIP notifications of the alarm type e.g. if the status attribute changes. Control facilities like status attributes or control interfaces must be available for all service components, for hardware components as well as for software components.

Several other standardisation bodies took this into account when specifying management facilities for system components. X/Open has defined a set of services specifically for distributed systems management [X/Open]. This specification complements the CORBA COS standard, in particular the Life Cycle Service, in order to ease the development of management applications controlling hardware and software resources in distributed environments.

3.2.2 Requirements

3.2.2.1 Trouble Administration

In [ITUT790] and [NMF501] sets of technical and functional requirements are described. In the following the most important ones are listed.

Trouble Report Creation:

1. A customer should be able to initiate a request that a trouble report on a resource or service be created by a service provider using a interoperable interface.
2. A service provider should be able to notify the customer about the creation of a trouble report on a resource or service based one of the following scenarios.

   a. a service provider management system detects a trouble and automatically generates a trouble report

   b. a person in the customer's organisation reports a trouble to the service provider by a procedure other than using the interoperable interface, e.g. a telephone call.

3. A service provider should be able to crate a trouble report to specifically notify the customer that planned maintenance will be carried out at a given time and that all or parts of the service, resource, network, or system will be inaccessible during that time.
4. If the service provider rejects the trouble report, the customer should be informed.
5. Both customer and service provider should be able to group trouble reports together, e.g. to indicate a common problem.
6. The customer should be able to supply a priority to indicate the urgency for resolution of the trouble.
7. The customer should be able to request a commitment time, e.g. the time at which the service provider either arrives on site or clears the trouble.

Trouble Report Tracking:

1. A customer should be able to track the progress of a trouble report to resolution. The customer should be able to request the trouble report state from the service provider. The service provider should be able to notify customer of changes to the trouble report.
2. The trouble report should maintain a running account of information on the activities taken to diagnose, test, and repair the trouble.

Trouble Report Management:

1. It should be possible for a customer to escalate a trouble report. Escalation levels can only increase, not decrease.
2. It should be possible for the service provider to defer work on a trouble report. For example, it may be necessary to suspend repair work because access to the faulty resource has been prevented by the customer.
3. The customer should be able to provide the required repair completion time and obtain from the service provider the expected repair time, and subsequently the actual repair time.
4. The service provider should be able to indicate to the customer whether the repair activity covered by the present trouble report is billable.
5. It should be possible for either service provider or customer to maintain trouble report history.

Trouble Report Clearing and Closure:

1. A customer should be able to request the cancellation of a trouble report.
2. The customer should be allowed to verify that the trouble is cleared prior to the closure of the trouble report by the service provider.
3. The actual cause of the trouble found, together with the solution provided, should be recorded in the trouble report.

3.2.2.2 Fault Detection and Recovery

The following functional requirements cover alarm reporting, alarm correlation, and component controlling. As mentioned above, the actual fault recovery is not addressed here.

Alarm Reporting:

1. Alarms should be collected from different systems, network elements, and service applications in an uniform manner.
2. All alarms should be stored automatically in logging facilities. An alarm retrieval function should be provided to allow operations on alarms in the alarm log, e.g. escalation.
3. There should be a minimum of six different severity levels for alarms (according to [ITUT733]): cleared, indeterminate, critical, major, minor, warning. Severity of an alarm should be increased if escalation occurs.

4. It should be possible to choose which types of alarms occur in the alarm list. Filtering criteria may be alarm severity, origin, time and date, or a combination of these.
5. Whenever an alarm is shown in management system an operator should have the possibility to create a trouble ticket.
6. Alarm management should consist of the following basic functions: initiate and terminate alarm reporting, suspend and resume alarm reporting, retrieve single alarm and alarm summary.
7. The alarm management function should also allow the automatic execution of user-written command procedures when particular alarm conditions occur.
8. It should be possible to define thresholds for numeric measurements, e.g. statistical values, traffic measurements. An alarm should be generated if the value of such a measurement crosses the pre-defined threshold, in any directions.

Alarm Correlation:

1. It should be possible to define parent-child relationships between different types of alarms. These relationships may be based on the hierarchical dependencies within the network, e.g. a network connection depends on adapter cards which in turn depend on their power supplies.
2. Alarms should be correlated with previous alarms if they were received within a pre-defined period of time, the so-called correlation window.
3. Child alarms should be marked by a separate flag or should be suppressed by the management system.

Component Controlling:

1. Each service component, i.e. all hardware and software components, should provide control facilities like status attributes or control interfaces.
2. Dedicated control components should be responsible for supervision of all service components in their administrative domain.
3. It should be possible to query the overall status of a component. It should also be possible to get detailed information if necessary.

3.2.3 Scenarios

In the following scenarios are presented describing Trouble Administration from the customer's viewpoint and Fault Management from the provider's viewpoint. The scenarios for Trouble Ticketing are based on those described in the NMF Trouble Administration Requirements Specification [NMF501].

3.2.3.1 Trouble Administration

It is assumed that both customer and provider have access to interoperable trouble administration systems.

1. Customer delegates to one provider - no feedback desired

The customer identifies a problem and determines that it is not related to services or equipment within their domain of control. He further knows which service provider is responsible for the repair of the problem. The customer delegates from their internal trouble ticket system to the service provider and has no desire for information flow back into their tracking system.

2. Customer delegates to one provider and requires feedback

The customer identifies a problem and determines that it may involve a specific provider's service or equipment. The customer delegates a trouble ticket to the specific service provider that is responsible for the problem, but demands status back to their trouble tracking system. In some cases the customer may be interested in intermediate status, or may only be interested in an update when the trouble ticket is closed.

3. Customer delegates to multiple providers

The customer has a problem with service and is unsure of the source. In this case tickets may be delegated to multiple service providers simultaneously. The customer may have no desire for information flow back or may demand status updates and further notifications.

4. Provider informs customer - end-user originated

End-users of a network service may report problems directly to the provider, e.g. via telephone. But thereafter the provider continues to report to the trouble administration system of the customer as for scenario 2.

5. Provider informs customer - provider originated

The provider may detect service affecting faults before the customer reports them. These are notified by the provider to the customer. Thereafter they may be tracked as for scenario 2.

6. Provider informs customer - scheduled down-time

The trouble reporting system may be used by the provider to notify the customer of scheduled down-time. The customer does not control this trouble management process in the ordinary way, but merely observes passively.

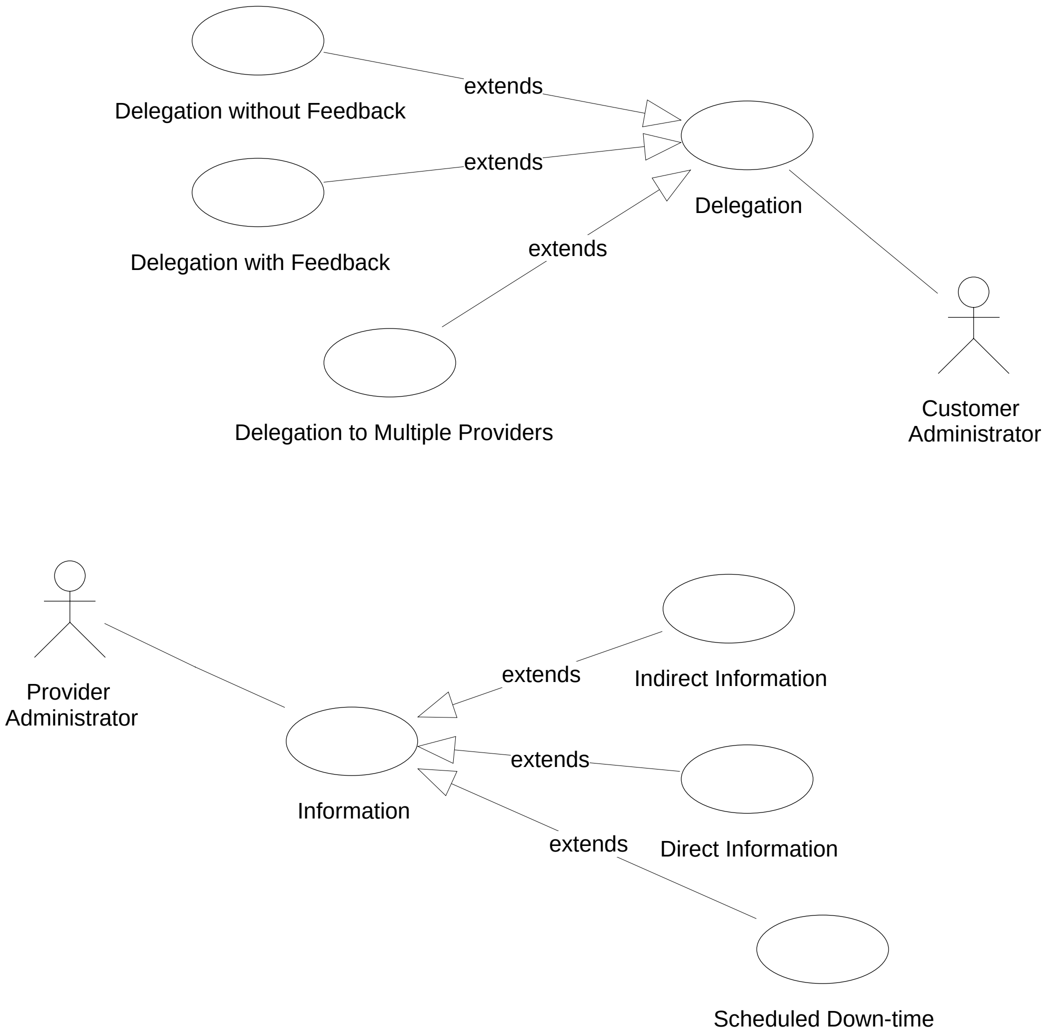


Figure 4: Use Case Diagram for Trouble Ticketing Scenarios

3.2.3.2 Fault Detection and Recovery

In the following scenarios interaction of a service provider operator with service components is described. The interface used may either be a simple graphical user interface or an autonomous, intelligent component.

1. Service component reports malfunction

A service component reports that a requested operation could not be executed. A possible reason for this malfunction may be included in the report. Recipient of this notification is the operator of the service, or his management interface, respectively.

2. Service operator gets status of all service components

The service operator may get an overview of all components, in particular may query status of components and of the entire system. The system may be displayed graphically and status of components may be coded using different colours.

3. Service operator gets detailed status of a certain component

A certain component needs to be checked by the service operator. Besides status information the report may include log records and usage statistics.

4. Service operator search for cause of problem reports from components

Having received several alarms from service components, the service operator may search for a common cause. After invocation of the problem detection procedure, the management system may poll several service components in order to locate the problem. For this purpose, various algorithms may be executed, e.g. alarm correlation.

5. Service operator recovers a service component

Having detected the cause of service failure (see scenario 4), the service operator may shut-down and restart or reconfigure a service component. This scenario may also include moving software components between different hosts, i.e. shutting down a perfectly running component and restarting it on another server. Reasons may be problems with other components or equipment.

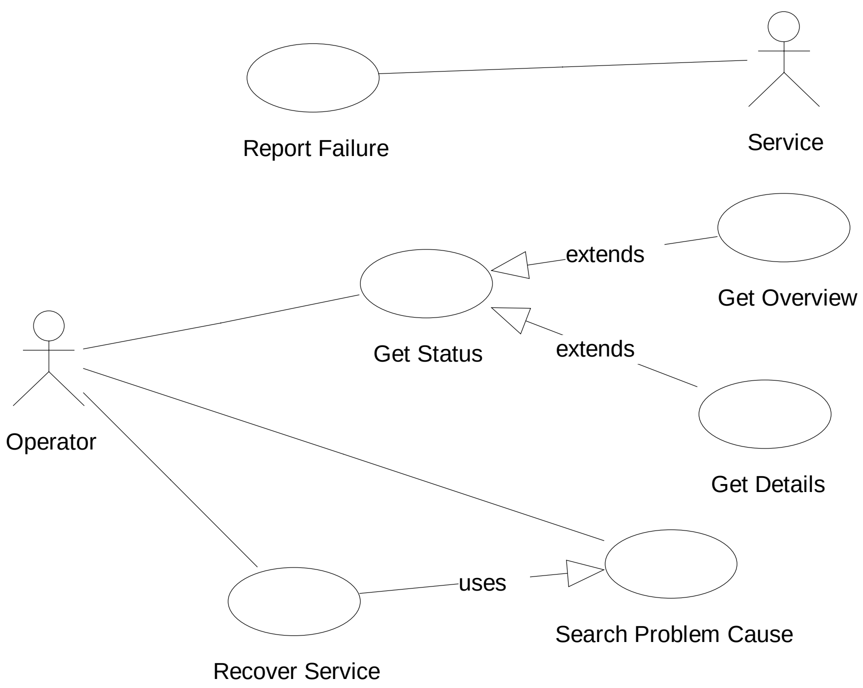


Figure 5: Use Case Diagram for Fault Detection

3.3 Quality of Service Management

Management of Quality of Service (QoS) will be an important part of Prospect Trial 2. This section first described state-of-the-art within QoS management, and next clarifies the directions that are crucial to Prospect Trial 2.

3.3.1 State of the art

QoS management is a topic that has recently attracted a lot of interest. The topic has only played a subordinate role in standards, however. “QoS in standards is covered briefly - this is not because it is unimportant (on the contrary, we argue that it will be highly significant), but rather because little work has yet been done.” [Sloman]. The book from Morris Sloman, “Network and Distributed Systems Management” has been published in 1994 but since this year the situation has not changed a lot. Numerous working groups are looking deeply at this management area although there is no consensus even on a clear definition of main terms.

Sloman stresses the diverse and ubiquitous requirements on QoS management in modern applications: “New classes of distributed application are being developed, such as distance learning, desktop video-conferencing and remote multimedia database access. These applications are characterised by their highly interactive nature and their significant use of multimedia information transfer. In these applications, communication requirements are extremely diverse, and demand varying levels of service in terms of parameters such as latency, bandwidth and jitter. Furthermore, for digital video and audio communications it is often a requirement that levels of service are *guaranteed.*"

In the Open Service Market (OSM) for Telecommunication Services as for all other markets quality of service is essential in the relation between a Customer and a Provider. It corresponds to a vision of the Customer and determine his level of satisfaction regarding the service provided. This does not mean that QoS is only subjective, not at all. A customer needs to get common references (or parameters) that can be compared between Providers.

A particularity of the OSM environment is the complexity to define QoS in terms of generic parameters. This is due on one side by the broad type of services and applications provided on the market, and on the other side the complexity of these applications. Today applications become distributed and moreover a service can be based on chain of Service Providers.

Another element that brings more confusion in the definition of QoS is based on the fact that if a Service Provider wants to guarantee an end to end level of quality for a service it is necessary to manage all the resources used by the application, this means the Network resources as well as the OS resources. Most of the works, that has been carried out, have looked only at one side of the problem.

In general, the issue has been considered from two distinct perspectives: one looking more to the network side and another looking more to the application and OS side. The importance of integrated QoS management is currently being examined in greated detail, for example in the work with the QoS Broker [Nahrsted]: "To provide applications with end to end guarantees, network resource management alone is not sufficient, particularly when endpoints become more sophisticated (such as workstations with rich device support, multiprocessing, and multiple users). This suggests a need to balance resources among the application, network and operating system at the endpoints, and between endpoints and the network." The solution to this complex task corresponds to a QoS Broker defined this way: "The QoS Broker entity is an endpoint resource manager that orchestrates needed resources for tasks in the application and transport subsystems and negotiates with network resource management and the remote QoS Broker. To orchestrate resources and support the decision-making process (the brokerage process), the broker entity must have access to all profiles." [Nahrsted].

It is worth noting that new technologies such as Java and CORBA suggest an integrated way of accessing all resources used by an application; this can be viewed as a possible future solution to the problems mentioned. Innovative experiments in this direction can be expected in the near future.

3.3.1.1 QoS Management

Looking at QoS in terms of measurement and quantification is a necessary task though not sufficient. It is also necessary to define the QoS management, which is defined by [Sloman] as "the concrete realisation of required levels of QoS in a real system". The analysis from the book comes to the following headings to be considered for QoS management: the headings of specification, mapping between layers, negotiation, resource allocation, admission control, performance maintenance, performance monitoring and policing and re-negotiation.

QoS specification is concerned with defining required levels of QoS which are interpretable by a system. QoS specification contains information on actions to take if the requested QoS levels are violated.

QoS mapping performs the function of automatic translation between representations of QoS at different system levels and thus relieves the user of the necessity of thinking in terms of low-level dimensions. For example, an user at the flow level may express a jitter dimension in terms of a statistical variance in arrival of video frames and this could be translated at the lower level into a requirement for an absolute bound on ATM cell jitter smoothing buffer of certain size.

The *QoS negotiation* function is responsible for analysing an activity onto components and finding a composite of the individual QoS levels supportable by those components which is necessary and sufficient to realise the QoS of the complete activity. When an activity is initiated, the negotiation function asks each component to state the level of QoS it is able to provide. Then depending on the results, it assigns particular QoS levels to each component (or reports back to the initiator that the activity cannot be supported).

In practice, *resource allocation* is often closely associated with QoS negotiation because it is often the case that low-level system components can only determine whether or not they are capable of supporting a given level of QoS by actually requesting the necessary resources and noting the outcome of the request.

To maintain an agreed level of QoS it is often not sufficient to statically dedicate resources to an activity at QoS negotiation time as described above. Instead dynamic *QoS maintenance* is frequently required to ensure that the required performance of individual system components is kept within bounds.

QoS monitoring is used to allow each level of the system to track the ongoing QoS levels achieved by the lower layers and compare them with the initial requirement.

QoS re-negotiation is commonly initiated in response to the receipt of a degradation indication, it is also requested in a number of other situations. For example, an user may simply wish to conserve global system resources by downgrading a low-priority activity.

This analysis from [Sloman] looks very useful in the task of defining requested management activities for guarantee of QoS in distributed systems.

3.3.1.2 QoS in standards

“QoS support in the OSI-RM is limited to statically defined parameters intended to be supported at the session and transport layers. To enable applications to access QoS facilities, the OSI upper layers (application and presentation layers) simply map QoS parameters through to the lower layers unchanged.” [Sloman]. The parameters are classified as either performance-oriented (throughput, transit delay, residual error rate, establishment delay establishment failure probability, transfer failure probability, resilience release delay, release failure probability) or non-performance-oriented, which do not directly affect the performance of the communications but are concerned with protection, priority and cost QoS categories.

It is clear that QoS support in the OSI standards is severely limited when related to the generality of QoS in distributed systems.

The CCITT has recognised the need for QoS configurability in the emerging standards for broadband integrated services digital networks (B-ISDN) which are to be based on ATM technology. As a result of this recognition they have issued a series of draft recommendations known as the I-series recommendations which define a fairly comprehensive set of QoS parameters at the ATM layer. The major service-related limitation here is the lack of consideration of how traffic characterisation at the ATM layer can be derived from user QoS needs at the transport layer and above.

The essential characteristics of the current state of QoS provision in the major standards may therefore be summarised as follows: incompleteness, lack of mechanisms to support QoS guarantees, lack of overall framework.

3.3.1.3 QoS at the Network level

Provision of QoS management at the service management level is based on the possibility to manage the network resources at the network level and through all the layers.

Concerning ATM, significant research is being undertaken in the ATM arena to design networks which are consistent with QoS provision. Typical QoS measures include average cell loss probability (CLP), cell transfer delay (CTD) and cell delay variance (CDV). Network resources of interest include bandwidth requirements at each physical link, as well as buffer space and processing capability at each switching node.

ATM has five service classes:

- CBR (Constant Bit Rate), which emulates a leased line, providing very tightly constrained delay and designed for applications which can use a fixed bandwidth pipe,
- VBR (Variable Bit Rate)-real-time, which attempts to constrain delay for applications whose bandwidth requirements vary,
- VBR-non-real-time, intended for variable bandwidth applications without tight delay constraints,
- UBR (Unspecified Bit Rate), which most closely approximates the best effort service of traditional IP,
- ABR (Available Bit Rate), which uses a complex feedback mechanism to control loss.

Some service classes are also supported by the IP Version 6:

- guaranteed, which provides a mathematically guaranteed delay bound,
- predictive delay, which provides a probabilistic delay bound,
- controlled delay, which merely tries to provide several levels of delay which applications may choose between.

Independently of the service classes supported by IPv6, a new protocol has been proposed to enable network resources to be reserved for a connectionless data stream: RSVP (Resource reSerVation Protocol).

Some drafts from IETF are already looking at IP Integrated Services with RSVP over ATM [Berson], [Garett].

Nevertheless these technologies are not in a mature state and a deeper evaluation of which of these technologies can be used within Prospect therefore needs to be done.

3.3.1.4 Conclusion

Valuable work on specific aspects of QoS management has already been carried out and much more work is in progress. Nevertheless, there is a still a lack of standards that address fully integrated QoS management. Progress in this direction can be obtained if international fora such as NMF or TINA-C take this management area into account and provide input to standardisation organisations.

Of particular importance is the development of a common understanding on service performance and the standardisation of service performance definitions.

3.3.2 Scope of QoS within Prospect

Full provision of QoS management for telecommunication services is very complex and probably many years away. In Prospect, which aims at addressing several management disciplines and their interplay, only partial results will be obtained. Therefore, it is of prime importance to address the scope QoS management within Prospect and to clearly defined what QoS functionality will be provided and how such functionality is correlated with technological constraints in the project.

Prospect does not aim to develop new services; instead the plan is to develop and add service management functionality on top of already available products for the provisioning of the network and service infrastructure. This means that the scope of QoS work within Prospect is limited by these whatever can be done with these products. Moreover, in order to guarantee end-to-end Quality of a Service all resources used by the service must be carefully controlled. For instance it might be crucial to control OS resources such as memory or to interfere with OS strategies for process scheduling. Such aspects are likewise beyond the scope of Prospect.

As the aim of Prospect is concentrated on the network than management of the applications it must be emphasised that control of the OS resources from the application used in Prospect trials is beyond the scope of the project.

Nevertheless, the end-user or the application should have the possibility to request a specific QoS, so it is necessary to provide a way of mapping “user interface” requests to the QoS management.

The main objective regarding performance management in Trial 2 would be investigating how existing QoS control schemes, e.g. those of the IETF and ATM Forum could be managed using the systems being developed in Prospect, in particular those based on the TINA service architecture. In particular Trial 2 could provide a valuable experiment and definition of QoS within the Open Service Market, many topics have to be investigated as: definition of a Service Level Agreement, negotiation for QoS using One-stop-shopping paradigm, interactions with accounting and subscription, etc.

The objectives of Prospect regarding QoS management and performance reporting are:

- Identification of the generic and service specific measures, which are relevant to support of a service, or a chain of services, provided by a Service Provider to a Customer. This would include which QoS information can be used in a generic manner and which is specific to the network QoS control scheme used.
- Integration of the QoS management support into the Prospect system model. Identification and specification of the impact on the other areas (Subscription/Configuration, Accounting, Fault Management).
- Definition of a framework for service independent SLA and Performance Report management.
- From an evaluation of the available network technologies enhancement of the Prospect network infrastructure allowing support of QoS.
- Specification of a mapping between information provided by the network elements (Network Performance) and information provided at the service level to the Customer defining the QoS, and through intervening value-added service providers.

3.3.3 Requirements

Customers would prefer to get performance that is consistent. That is, they would like to be able to compare the performance of their many providers and suppliers, which today is not possible because each supplier uses different performance terms, and each term represents different measures. Availability, for example, is a term that is used very differently by different providers and suppliers.

Providers also see a benefit to negotiating common elements of a SLA to reduce the number of unique arrangements they must accommodate with individual customers.

General requirements for Performance Reporting:

- Automated performance reporting, reducing the amount of human intervention for collecting data, generating reports and exchanging report information by using automated processes.
- Generic performance reporting interface between customer and service provider, independent of the type of service.
- Common framework and definitions for performance reports and SLA between customer and service provider and a set of common definition of terms for service performance.
- Security and confidentiality, this is not a specific requirement from Performance Reporting

Specific Requirements:

- Specification of a mapping between information provided by the network elements and information provided at the service level to the Customer. This requirement is specific as the network level corresponds to the one to be used by Prospect, which could be IP over ATM or IP.

Other requirements concerning QoS derived directly from the objectives proposed in the section above.

There is an open issue concerning the Prospect Enterprise Model defined in Trial 1, it has not been clearly defined if the Customer establishes a contract with the VPN provider or the VPN provide the necessary links to the Customer based on the contract negotiated between the VPN provider and the TES provider.

This issue will have an impact and will permit to define, regarding to the Customer, who is responsible of the QoS, the VPN provider or the TESP (in a one-stop-shopping manner).

3.3.4 Scenarios

The following scenarios could be applied to Prospect Trial 2:

1. Definition of a SLA (Service Level Agreement) during the subscription phase and its effect of network QoS configuration (could use MISA QoS routing technique).
2. Re-negotiation of the SLA.
3. Impact of a service failure regarding the SLA (impact on the performance reporting, billing, etc.).
4. Tracking delivered Service Level Quality against Service Level Agreements for different service types.
5. Performance reporting received by the customer on a periodic basis.
6. TES user accessing the services (negotiation of the call parameters, impact of QoS on billing, update of the performance reporting information).
7. Degradation of performance during a session, SLA violation (impact on performance reporting and billing, re-negotiation).
8. Failure during the session (impact on performance reporting and billing).
9. The monitoring of requests for QoS guarantees from users and the automatic modification of network configuration to handle this according to some combination of the customer’s SLA and some (possibly changeable) policy, i.e. dynamic network planning to support required connection rejection probabilities.

3.4 Security

This section contains an analysis of requirements for security.

First, an overview is provided of security components already integrated in Prospect Trial 1. This is a basis for further developments - which will be discussed subsequently.

3.4.1 State of the art - Security in Prospect Trial 1

The Security Service provides the security technology to extend the main services in Prospect, e.g. the Tele-Education, HM, MMC and WebStore services, by security. The security functions are integration in the services to realise and support authentication between UAP/ISM and UA in the access session as a first feature.

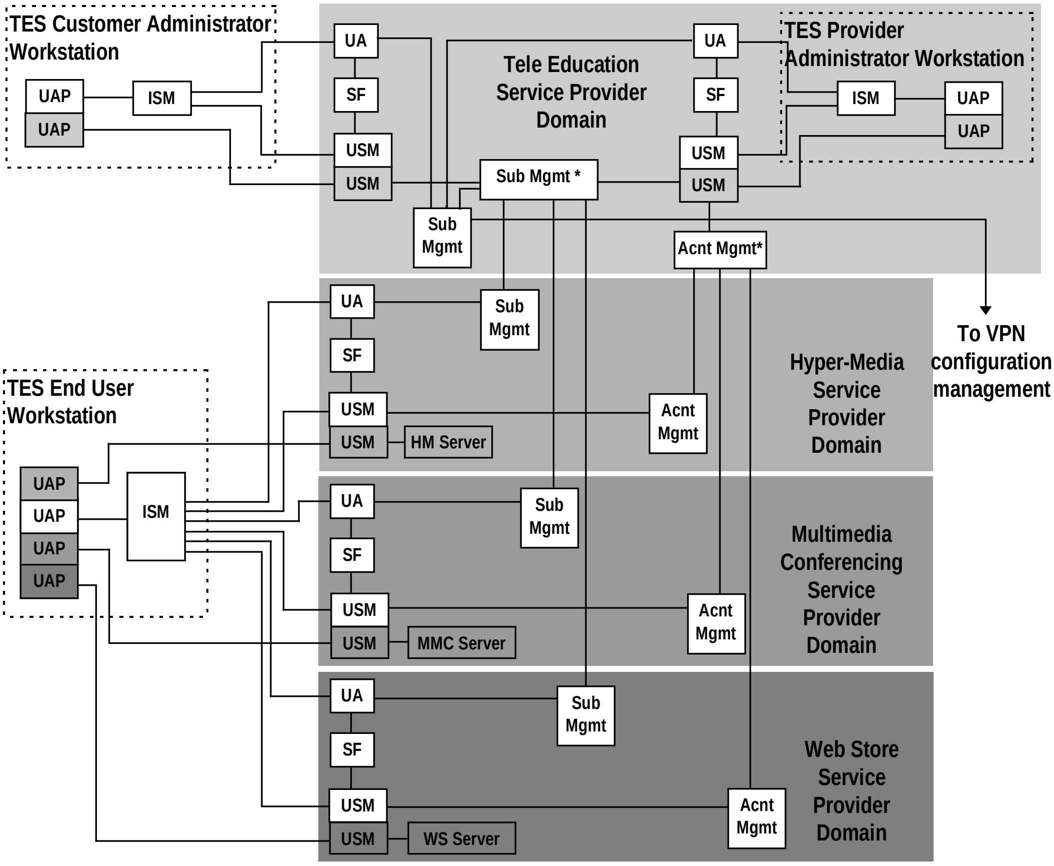


Figure 6: Service independent and service specific components

In contrast to the other services in Prospect, the security service has to be considered slightly differently since it is orthogonal to other services, i.e. it applies to all of them. It is not used directly by an end-user and has to be as transparent as possible for an end-user.

For Prospect Trial 1 it was decided to have authentication as a first security feature and therefore there is the need for a certification functionality which offers the adequate key management. The cryptographic keys which are provided by the central certification authority (at DTB) are used to support a 1-way authentication protocol in the access session of the services as a first security solution for Trial 1. So it is possible that only authentic end-users get access to specific services in Prospect.

As mentioned above it was intended to establish a Prospect certification authority (CA) which provide cryptographic keys, unique user ID's and additional information in X.509 certificates [ITUT509] for all security relevant domains.

These asymmetric pairs of keys and additional information for each user are generated centralised at the CA and are provided off-line on a TCOS chipcards and additional floppy disks (optional as a pure software solution). This means there is no direct contact between user and CA to request these information in Trial 1. In a later version it is also possible to distribute a Manager tool to the different Prospect locations in order to provide a user controlled management for keys.

3.4.2 Certificate and key management for Prospect Trial 1

In the 'pre-service' phase the Security Service Provider uses the security management tool (BMSec) for certification and key management. It consists of three components: CA-Manager, CA-Agent and PSE-Manager.

The certification authority at the Security Service Provider has to generate all PSE's (Personal Security Environment), chipcard and software based, for all users and for the security relevant domains. This means that the CA has to generate an asymmetric key-pair and to initialise the TCOS chipcards, so that each user gets his unique user-ID (in form of a distinguished name) together with the required key pair, embedded in the appropriate certificate, signed with the CA's private signature key. Some additional information is stored in a directory on a floppy disc and these information have to be integrated in the SecuDE security environment which has to be installed at the UA (User Agent in the customer domain) and UAP (User Application in the Provider domain).

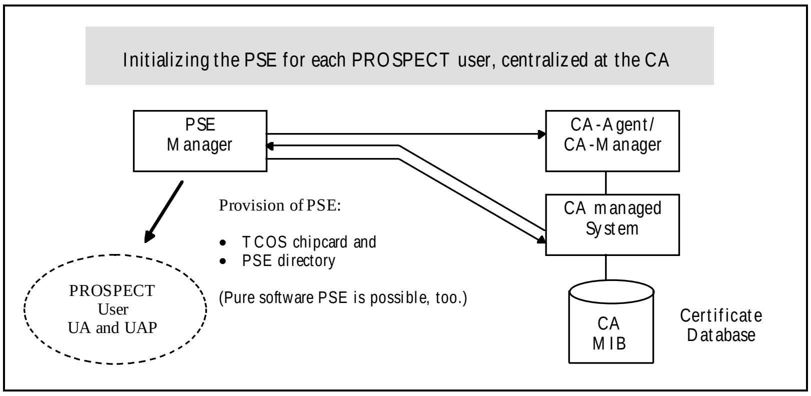


Figure 7: Certificate and key management

(For more details see also, 'A Prospect of Security in the Open Service Market')

Then the SecuDE security software libraries have to be installed at the UA (UserAgent) and at the UAP (UserApplication) sides. These steps are the presupposition to realise the authentication which will be described below. The authentication is based on the provided functionality of the SecuDE tool, together with the chipcard for the users. So the end-user can use his card for authentication purpose without taking care of the basic security technology the functionality relies on.

The SecuDE 5.0 crypto tool is developed by GMD TKT and offers a easy to use API to integrate security (encryption, decryption, signing, verifying) in the special services of Prospect. It supports UNIX, Windows 95 and NT. For further information about the integration of the SecuDE tool see also 'Prospect Trial 1, Pre Test for Security'.

3.4.3 Passing of Security Information in a Multi-domain Environment

This section represents the recent reflections about passing security related information (for authentication) from the customer domain to the different provider domains.

Some general assumptions:

- Prior to any service usage (regardless whether using the TESP, the WebStore, the HT or the MMC) an access session has to be initiated.
- The access session is different for every service provider, thus returning a different TESAccessSessID for each service provider.
- Authentication information is used to authenticate a user to the service provider. This information depends on the technology used. In case of using the SecuDE software it means the usage of asymmetric keys for the user and the different service providers. The token is passed via the passwd field as specified within the IDL of the ISM and UA and is the only information that is encrypted!
- Every user (person) has only a single user ID.
- The UA of the different service providers is the only one which checks the authentication of the user. If the authentication data is valid, further service access is granted. At least for Trial 1 this

is the only time when this information is used. Therefore, only the UA and the TESUAP are extended using the SecuDE software.

- In order to allow the TESP to integrate other services seamlessly, the user enters the security related information only once when initiating the access session to the TESP. Therefore, the TESUAP stores the security related information locally to pass it to other service providers.
- There are only 4 different functions that are used from the SecuDE software package. These are Encrypt, Decrypt, Sign and Verify.

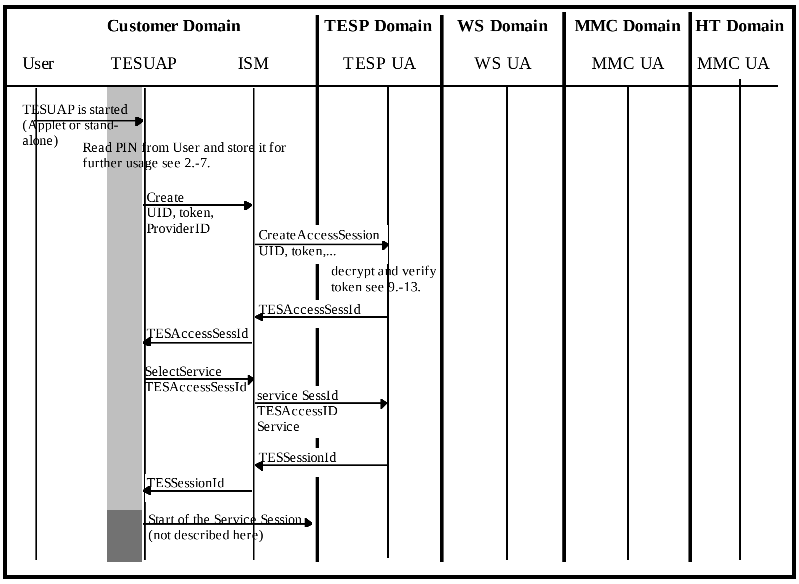


Figure 8: Forwarding of security information to the different service providers

This figure summarises the discussion about passing security related information from the customer domain to the different provider domains.

The user accesses the TESUAP. This may be done via downloading a special applet from the HTTP server of the TESP. Another option is a TESUAP that is installed at the customer side and invoked by the end user[1].

The TESUAP asks the end user for the PIN in order to access the SecuDE software. This PIN is stored locally for further usage during the lifetime of the TESUAP.

To authenticate a user at a UA the token is generated. It consists of different kinds of information.

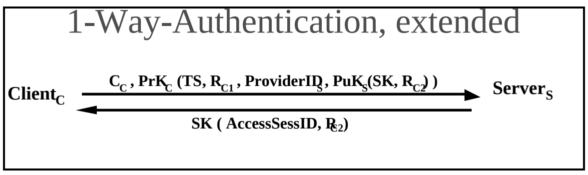


Figure 9: Extended 1 way authentication

The client (UAP) generates two random numbers, RC_1, RC_2 (RC_2 is stored locally and will be used later) and creates a timestamp TS_C for the authentication token. In Trial 2 the client also generates a symmetric key SK and stores it locally. This symmetric key will then be used to protect the TESAccessSessID sent back from the UA to the TESUAP. It could also be used to protect all communication during the service session.

[1] Preferably the applet should be installed locally since it might get forged during downloading. Forging should not be possible if the applet is stored locally since it can then be tested prior to execution.

The client assembles a message, M=(TS_C, RC_1, ProviderID$_S$, d), where TS_C is the client's timestamp, ProviderID$_S$ is the identity of the server and d is some encrypted supplemental information[1].This supplemental data is encrypted with the server's public encryption key for security (d = PuK_S (SK, RC_2)). This message M will then be signed using the secret key of the user and appended to the Client's certificate C_C. The signed message M and the certificate C_C form the token that will then be passed to the UA.

During the transmission nobody is able to forge the timestamp information, the random number or the ProviderID since this information is signed. Decryption of the $RC_2$is not possible as well since this can only be done by the recipient having the valid private decryption key.

The certificate C_C information is optional. It supports the key distribution. If it is used the UA will be informed of the user's public key and userID by certificate. Therefore, the UA only needs the public key of the Certification authority to verify the correctness of the certificate. If all keys are available at the customer side prior to service access, the certificate would not be used. Nevertheless, using certificates is regarded as elegant solution for the key distribution and this data is already available for every single end user.

The TESPUAP invokes the create function of the ISM which forwards it using createAccessSession to the appropriate UA in the provider domain.

The UA verifies C_C (by using the publicly known root key of the certification authority, who had signed the certificate) and obtains the PuK_C (used to verify the clients signature). It also makes sure that these keys have not expired yet. If C_C is not available the UA skis this step.

The UA uses PuK_C to verify the signature either using PuK_C obtained from the certificate C_C or a local copy. This verifies both client's signature and the integrity of the signed information. Furthermore, the UA checks the Provider ID to make sure it is accurate.

The next check performed by the UA is the timestamp TS_C. If the timestamp information is outdated the UA will reject the access session. Then, it checks RC_1contained in the token against a database of already used random numbers (former accesses) to ensure that the message is not an old one being replayed by an attacker. RC_1 will be stored in the database for further checks.

The UA then decrypts the encrypted session key[2] and the random number by using his private decryption key and stores the symmetric session key for further usage[3] at the UA side.

The only information returned right now from the UA to the TESUAP is the TESAccessSessID. In terms of security it would be very interesting to append RC_2 to the TESAccessSessID[4]. This enables the TESUAP to check whether the UA it is talking to is the one it claims to be.

Using this TESAccessSessID the TESUAP either selects automatically a service or prompts the user to select one. Using the service id and the access id the TESPUAP invokes selectService to start a USM using the UA at the provider (this is not shown in the figure above).

The UA returns the interface reference of the USM via the ISM to the TESPUAP. Therefore enabling the user to access the selected service.

The TESPUAP may initiate further access sessions enabling the end-user to access other services (e.g. WebStore, MMC, HT) as well. To do this, the TESPUAP will go through the steps 4 to 8 again for

1 For Trial 1 only the random number will be used. For Trial 2 a symmetric session key SK is added, which is used to encrypt/decrypt the following communication between client and server.

2 Not included for Trial 1.

3 For example to secure the service session as well.

4 This means that the naming convention for the TESAccessSessID has to be extended a little bit to include the random number RC_2 sent by the TESUAP. This extension should cause no trouble since the TESAccessSessID is still unique and generated by the UA.

each service required. No user interaction has to take place since all information needed are already stored locally in the TESPUAP.

Since there is no way to extract the secret key of the user out of his PSE environment this method is assumed to be safe and secure.

3.4.4 List of requirements

The area of security is of particular importance for Prospect Trial 2 and has a broad impact on the Trial 2 system model. The security functionality should be extended in different way, as it will be described below.

It is regarded as a general requirement that all service providers must implement security in a way that a harmonious integration in the overall environment of Trial 2 is possible.

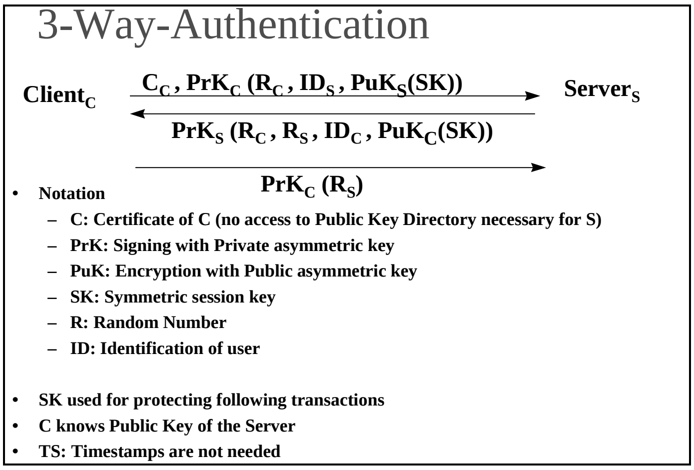
- Authentication, using 3-way authentication protocols:
  - Authentication in the access session.

  In Prospect Trial 1 it was decided to have security only in the access session while getting access to the different Services in Prospect. That means that a user has to authenticate via Personal Security Environment (software and PIN or chipcard based) against the Prospect services.

  As stated previously it is also necessary to integrate encryption mechanisms to encrypt the information (content and data) that will be exchanged in the service session.

  A first step in this direction was made in Prospect Trial 1 by integrating a symmetric session key in the authentication token of the access session. This session key should be considered for further use to encrypt the service session.

  The former used 1-way authentication should be substituted by a 3-way authentication protocol, which is more secure in the way that the UAP authenticates against the UA and vice versa.



  This is realised by using different User ID's and various random numbers that are generated on both sides and that will be signed and transmitted in the 3 steps of the transaction, so that an attacker gets no chance to break into the connection. An additional advantage of 3-way vs. 1-way is that there is no need for timestamps and therefore no need to handle additional synchronised NTP-Servers that are needed to compare the various timestamps in 1-way or 2-way protocols.

  It is to avoid that anybody can attend running courses if he is connected to the Prospect infrastructure and has the appropriate software. This has to be done with the appropriate authentication mechanisms for the whole Prospect environment.

➢ Authentication, support of mobile users and inter-domain security

Especially when we think of the possibility to support mobile users in Prospect Trial 2 it becomes very important, that not only the user authenticates against the system but also the system against the mobile user, so that the user can be secure to communicate with the server that claims to be the right one and uses only authenticated services. This mechanism should be used not only to secure the services used be the end user but also to secure the management layer and the communication between different servers and services.

In principal the same mechanisms can be used for both inter-domain security and intra-domain security.

- Confidentiality and Integrity of content and data in the service session:

Prospect should secure of the TES Customer Management Service at the access level and at the service level (encryption).

Confidentiality and Integrity is very important, especially when taken hand in hand with the suggestion to use the access/service mechanism for all inter-domain interactions, including management ones between providers. This gives a very good security basis for the Prospect infrastructure but with maximum reuse of design and implementation. One point however is that the former said is based very much on a inter-domain vs. intra-domain model of interactions, i.e. Prospect is only concentrating in inter-domain security here, not intra-domain security. Prospect has to consider the needs of intra-domain security since these systems are themselves distributed. This could be done as paper study at first.

Currently the interests for Prospect are seen in the following areas:

➢ Collaboration with TRUMPET.

Trumpet is looking at security of CMIP interactions. The Prospect CMIP interfaces are, in the terms of Prospects model, intra-domain to the ATM VP provider. So from an enterprise model point of view this is one way their output can be useful in Prospect.

➢ Firewall and Intranets:

The use of firewalls is the standard way currently of securing IP between different LAN sites in an administrative domain. Prospect should do some paper study of how such systems could complement it’s intra-domain security needs, including the use of IIOP capable firewalls. It could also spent some effort to explore the extension of this technology to extranets, i.e. inter-domain intranets, and to discuss how this might aid Prospect’s inter-domain security requirements.

➢ CORBA security service:

This may not be something Prospect can use in practise right now, but it would be fine to have an understanding of how it compares to the Trial 2 security model.

- On-line key management and distribution:

Prospect considers an on-line Certification Authority as a useful feature of the security provider, so that users get on-line support from the Certification Authority (CA), i.e. support to get dynamic authenticated (on-line) access to the CA with the possibility of generation of chipcards at the user side and remote certification of such user prototypes at the Certification Authority side.

IBM has stated that they want to manage the security service in Trial 2, i.e. use functionality of the Certification Authority.

Additionally it is regarded as nice to have to establish the role of a security administrator. Such an administrator could monitor the system. He would get all security relevant information (i.e. unauthorised attempts for login, faults in time, random numbers, etc. during user authentication).

On-line key management and distribution is definitely an interesting requirements. Currently DTB have been performing the CA role manually. As well as investigating doing this in a more automated fashion in Trial 2 as mentioned above, it is regarded as quite useful also to look at co-operating with the TELEMATICs project ICE-TEL. ICE-TEL has set up CA's in several countries and so inputs of this project might be very interesting for Prospect.

- Use of PLASMA

PLASMA (platform for secure multimedia applications) was an R&D project of DTB first and will be developed as a product at DTB at the moment. It becomes a security product of Deutsche Telekom that will be available in August 97. PLASMA offers the possibility to substitution the SecuDE security environment. It will provide all the basic security functions that are needed in Prospect and offers the application/service developer an easy to use API (easier than SecuDE) to integrate security features in their applications without knowledge of basic cryptography.

Additionally PLASMA offers an interface to integrate security hardware in the own system For example: With PLASMA a developer of multimedia applications or services do not need to know how to integrate chipcard readers, PLASMA will do it for him via the API.

By the way with the PLASMA concept Prospect get a mechanism for the management of security via formal security policies with which it is possible to change the desired basic cryptographic functionality that is integrated into the platform and will be used by the service or application while the system is running. With PLASMA it is possible to take arrangements for formal security policies between communication partners (clients and servers) and so to support a security administrator by enforcement of a common security strategy in a whole system.

But this offer needs to be consider together with any implications it has for co-operating with ICE-TEL, mentioned above.

Another point of interest is to consider the impact of integrating Prospect's security with Netscape for the end user, especially considering the Netscape 4.0 security enhancements. Having secure applets could be a definite advantage for Trial 2 and some effort should be invested.

- Legal aspects of security - world wide

This is an interesting point for security in Prospect Trial 2. It is important to consider for example the different export restrictions for cryptography - different in the countries of the EU - and how to find a practicable solution for this fact in Prospect.

As mentioned above the ICE-TEL project has delivered various information on Firewalls and National Security Regulations that might be of great interest for Prospect. Some kind of collaboration with this (or other) projects may be beneficial.

- Integration of E-Cash as electronic payment

All service providers must take the integration of E-Cash in future accounting scenarios into consideration. Prospect could add a facility to pay on-line in a secure way with a bill based on the resources consumed.

This feature is very interesting and some paper work could be done first to have a look at suitable mechanisms and the integration of secure payment (billing / accounting) in Prospect Trial 2.

A first step towards securing inter-domain management interfaces in Prospect is to reuse the same mechanisms used to secure user access and service sessions, i.e. one provider's systems con only access another via secure interactions with user Agents and User Service Session Managers. Figure 10 below indicates how this could be accommodated on the existing Trial 1 system.

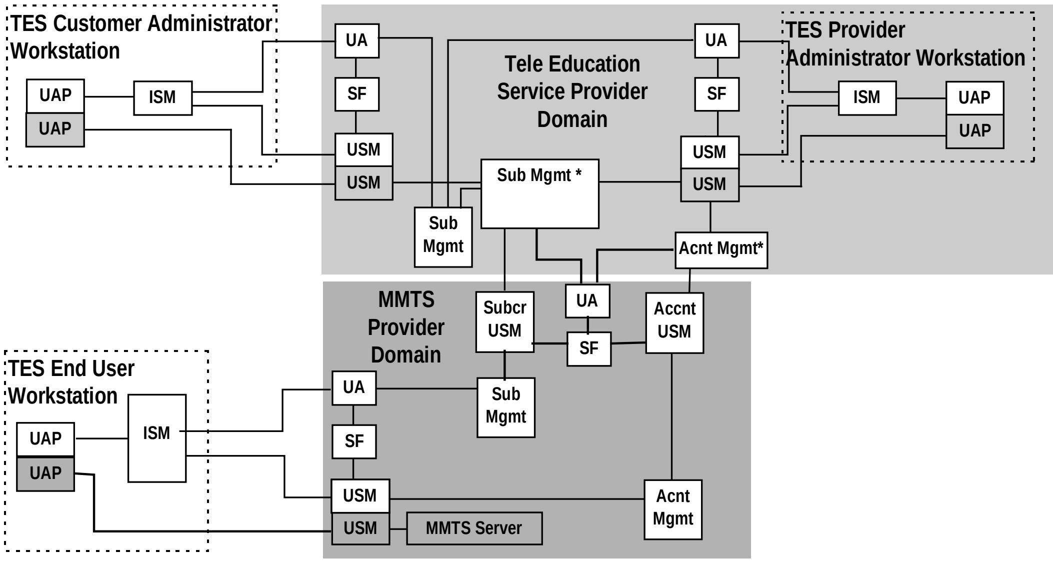


Figure 10. Trial 1 system model augmented to support secure inter-domain management interfaces

3.5 Subscription Management

A user must subscribe to a service before using it and during this subscription process the user interacts with the subscription management system. This section describes how to extend the subscription management system from Trial 1; both requirements and explanatory scenarios are presented.

3.5.1 State of the Art

The subscription management functions in Trial 1 consists of two principle components, the common subscription management component and the subscription management propagation component. The former is based on the TINA subscription management functions described in TINA service architecture version 2.0 [TINASA2], with additional input from the VITAL and TANGRAM projects. The subscription management propagation component is an extension to the former, developed within Prospect, which supports the composition of separately managed service offerings into what appears to the customer to be a single service. Full details of the current model can be found in deliverable D4A [Prospect D4A].

3.5.2 List of Requirements

The process of performing the detailed design of the subscription management and subscription management propagation components and in particular of applying these components to specific service implementations in Trial 1 provided a lot of insight into how the existing design could be enhanced. From this process the following requirements were identified:

- For a single subscription the customer can define multiple subscription assignment groups (SAGs) and multiple service profiles. Profile and SAGs can be assigned to each other so that the users, network access point or terminals defined in a SAG access a service within the restrictions defined in the service profile. Several service profiles can be assigned to a single SAG, so its members can access services subject to any of these service profiles. Currently however multiple SAGs cannot be assigned to the same service profile, thus limiting the flexibility of the system. This functionality should be provided for Trial 2.

- The IDL interface currently supported by the subscription management components only allow modification to SAG via an operation that passes the entire SAG content. This is highly inefficient for SAG with large numbers of members. This interface should be modified so that individual SAG members or sub-groups of SAG members may be added or removed.
- The modelling of a SAG needs to be examined to see how it can support groups of SAGs, both when all the SAGs belong to a single customer and when they belong to different customers. It should then be possible to make a single assignment between such a group of SAGs and a specific service profile, under a specific service contract.
- The current IDL and information model assumes that the services being subscribed to are connection based ones. The Prospect services are, however, TCP/IP based and therefore their management is more based on the capabilities of the end user application and securing access to the service content, than managing connections in the network. The underlying data structures (primarily the service common data structure) of the service template, subscription and service profile need to be remodelled so that they support the IP service model more efficiently. This is closely related to the requirements for performance management. In addition the complexity of the current structures in this area imposed many implementation problems, so a concomitant simplification of this information structure would also be beneficial.
- The addition and removal of subscribers and individual subscription contracts is supported by the current subscription management model but were not imposed as requirements in the Trial 1 scenarios. Their inclusion as requirements for Trial 2 should be considered.
- The current subscription management model includes some support for the management of multiple services (as defined by different service templates) by a single provider. In Trial 1 however this was not used in support of services that required different management behaviour, just for services that required different service client software behaviour. For Trial 2 support should be included for multiple services with different management behaviour, i.e. it should support the management of different service factory and subscription registrar implementations.
- Interactions between the subscription management propagation component in one provider domain, and the subscription management component in other provider’s domains is currently not subject to any security. These interface should be at least subject to authentication and access control restrictions for Trial 2. The encryption of the information passing over these interfaces should also be considered. This is closely related to the requirements for security.
- The information model used in the subscription management propagation component for mapping subscription information in the composite service provider domain to subscription information in the constituent services’ providers’ domains is currently somewhat restrictive. This model should be review to consider different forms of mappings between the composite service offering and the constituent service offerings.
- The interaction between subscription management and accounting management has not been fully explored in Trial 1 and should be modelled more thoroughly in Trial 2.

Since these systems were designed TINA-C has released an updated version of it service architecture in [TINASA4]. This is not therefore reflected in the current design but forms the basis for some of the new requirements. In particular the following should be considered for the Trial 2 system model:

- The new TINA service architecture, unlike the previous one, considers issues of service composition. The Prospect solution to this problem and its effect on subscription management should be compared to that taken in the new service architecture and, if deemed feasible, aligned to it.
- The TINA service architecture considers in some detail the full service life-cycle, including the deployment of new services and their subsequent withdrawal. This has an impact on the subscription management component, in particular concerning the dynamic configuration of objects within this component. The impact of this on the Prospect subscription management

model should be assessed, and this could be considered as a further requirements on subscription management.

In the Trial 1 system model, subscription management was only applied to the TES provider and the MMTS providers. The VPN provider and ATM VP provider also present in the Prospect enterprise model did not support subscription management. A requirement to do so should be considered as an enhancement to the overall system model for Trial 2. Figure 11 shows how such reuse of the subscription management components could impact on the system model (the same is shown for accounting management).

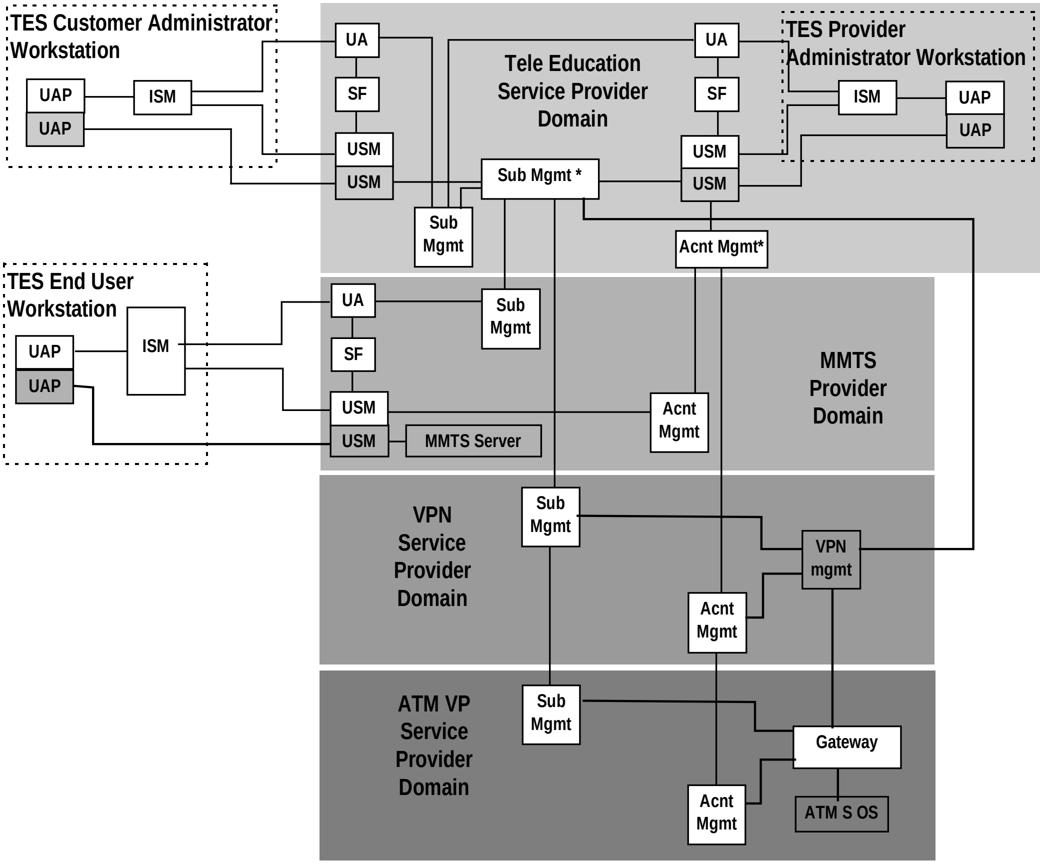


Figure 11: Trial 1 system model augmented to reuse subscription and accounting management in the VPN and ATM VP domains

Subscription management could be used in the VPN and ATM VP domain to specify which end-points of these services were allocated to which customers. The actual service would then just concentrate in providing links between these end points. This would impose the following additional requirements on subscription management:

- Revise subscription model to ensure NAPs and terminals are supported in SAGs in a way that is compatible with existing VPN and ATM VP models.
- Revise subscription propagation model since the exact form of mapping from TES SAGs to MMTS and VPN SAGs may be different (the former more concerned with users, the latter with NAPs and/or terminals).
- The VPN and ATM VP model will need to be modified to get end points from the subscription management rather than directly.

3.5.3 Scenarios

The Trial 1 subscription management components where involved in the following outline use cases that assumed that services were already defined and that customers were already subscribed to these services:

- A customer administrator authorises a user to user a service
- A customer administrator bars a user from using the service
- A customer administrator adds a customer site to the group of network locations from which users may access the service.
- A customer administrator removes a customer site to the group of network locations from which users may access the service.

To illustrate the impact of some of the above requirements, on the subscription management components used in Trial 2 the following outline use cases are presented:

- A provider administrator deploys a new service by including its service template details and configuring new subscription management and service management components.
- A service provider administrator configures mappings of a composite service configuration onto those of constituent services.
- A service provider administrator removes mappings of a composite service configuration from those of its constituent services.
- A provider administrator withdraws an existing service by removing service template details and deconfiguring the relevant subscription management and service management components.
- A provider administrator opens an account for a new customer by creating the appropriate subscription contract information.
- A provider administrator closes an account for an existing customer by modifying the appropriate subscription information.
- A provider administrator subscribes an existing customer to a new service by creating appropriate subscription information.
- A provider administrator removes the subscription of an existing customer from a service.
- A customer administrator creates specific service profiles within the bounds of an existing service subscription.
- A customer administrator modifies specific service profiles within the bounds of an existing service subscription.
- A customer administrator removes specific service profiles for an existing service subscription.
- A customer administrator creates a SAG for its users.
- A customer administrator is able to add and remove subgroups of users from a SAG.
- A customer administrator deactivates a service profile associate with a SAG of its own users.

3.6 Accounting & usage information

Accounting in Trial 1 was relatively simple since users had to pay in advance. But payment-in-advance is a rather simple-minded and inflexibility principle. In Trial 2 it is the aim to implement more sophisticated management functions - in particular functions that take actual usage into account and which allows individual users to be treated differently. This section contrasts the Trial 1 system with the expected Trial 2 system.

3.6.1 State of the Art

Accounting management for Trial 1 consisted of components in two subsystems. The components in each MMTS's accounting subsystem monitored and logged service usage (UMDataCO & UMLogCO), controlled tariffs (TariffControlCO) and allowed charging and billing (ChargeControlCO & BillControlCO), while a component in the TES subsystem (BillConrolPropogatorCO) collected bills from the individual MMTSs and combined them to provide an overall TES bill. The accounting subsystem components are based on those in the TINA service architecture, version 2 [TINASA2], with input from the TANGRAM project. The component in the TES subsystem was developed within Prospect to support an overall service bill for the TES customer. Details of these two subsystems are available in deliverable D4A [Prospect D4A].

3.6.2 List of Requirements

The design, implementation and use of the accounting management components highlighted some areas where the present design might be enhanced. The requirements below identify some areas for enhancement:

- *Usage sensitive accounting for the TES customer.* At present a flat-fee based bill, rather than a usage sensitive one, is passed to the TES Customer by the TES provider. (Although the TES provider receives a usage based bill from each MMTS). In Trial 2 it is hoped that the TES Customer bill will be usage based.
- *Individual End-User usage reports.* It is hoped that Individual End-User usage reports can be made available to the TES Customer to help with End-User evaluation and evaluating the effectiveness of the course materials. These usage reports may be made available to the End-User at the discretion of the TES Customer. The TES Provider may require per user usage reports from each MMTS provider to allow it to pass these reports to its customers.
- *Individual End-User billing.* At the moment only account based billing is supported. At the usage metering and logging level there is support for per-user usage data; this is lost in the (necessarily) simplified charging and billing scheme that uses this data in Trial 1. The Trial 2 model should allow more flexible charging and billing based on this usage data, and in particular should support individual End-User billing if the TES Customer requests this service.
- *Improved definition of the relationship between the Charging and Tariffing information objects.* The relationship between tariff information objects and charging needs improvement; at the moment there is a loose relationship that allows a per session charge, and a charge for requests in that session context, with allowances made for multiple user sessions that will be present in the Trial 2 system. The MMTS may support a flexible charging model in the future, for example to allow an alteration of the charge to account for the fact that the same user requested the same document a number of times in a short time period. This would mean, for example, that the tariff that is applied to usage data to compute a charge would have to support additional parameters to allow for document dynamism (how frequently its content is altered), size, frequency of request and the user making the request.
- *Improved Usage Information security.* The MMTS Providers, TES Providers, Customers and ultimately End-Users, require security support for data confidentiality for the usage data collected. For the MMTS Provider in particular, some sort of access control to the collected data in the UMLog Computational Object is needed; at the moment this is difficult, mainly because of poor middleware support for security that necessitates application level security mechanisms. An access controlled version of the naming service could help alleviate this problem by ensuring only entitled clients entitled get the necessary object references. The MMTS Provider in an Open

Market must ensure that competitors cannot see the charges on which their bills are based; there is a need for access control to each ChargeControlCO too. TES Providers that invoke each MMTS BillControlCO must ensure that its Customers cannot see the bills produced in this way, and must also insist that its Customers cannot invoke these billing operations directly, again, there must be an access control mechanism for each MMTS BillControlCO.

4 Project requirements - individual services and components

The previous chapter contains a description of the new management functionality that will be introduced in Trial 2. Early in the preparation of the present document it was realised that some requirements do not fit well into the standard categories of management disciplines, they rather have to do with certain aspects of one or more services in the system. Moreover it became clear that quite a few requirements arose in the process of constructing the individual components that comprise the Trial 1 system. The present chapter is devoted to the presentation of all such requirements.

4.1 TES User Interfaces to Management Services

It is important to have good user interfaces to management service. Good interfaces enable administrators to get a quick overview of managed components and allow them to properly take advantage of the supporting management systems. This section sketches the extra functionality that should be added to the user interfaces in the transition from Trial 1 to Trial 2. Experimentation is needed, though, to arrive at the final design of Trial 2 user interfaces, in particular to find the best graphical representation of the management information.

4.1.1 Current State

The TES Management User Interfaces, in Trial 1, correspond to the Management interface provided to the TES-CA (Customer Administrator) and the one provided to the TES-PA (Provider Administrator). The former corresponding, in term of functionality, to a subset of the latter.

These interfaces are based on the management functions provided externally by the TES Management System. These functions allow to access and maintain subscription and accounting management information stored by the TES Management System.

The functions provided to the TES-PA are:

- Subscription management:
  - Service Templates Management (Create, Modify, Display, Delete)
  - Subscribers Management (Create, Modify, Display, Delete)
  - Subscription Contracts Management (Subscribe, Modify, Display, Unsubscribe)
  - Customer Sites Management:
    - Subscription Assignment Group (SAG) Management (Create, Modify, Display, Delete)
    - Service specific setting for a group (Set Service Profile, Delete Service Profile)
    - Activate/Deactivate a Group for a service
- Accounting Management
  - Get the charges per user
  - Get the bill

The functions provided to the TES-CA are:

- User access control management, which allows to authorise or bar the access to a service for a specific user
- In-Service customer site management, which allows to add or remove a NAP from a SAG

- Display Subscription information, which allows to display all the information relative to a subscriber (or Customer): subscriber information, subscription contracts, SAGs, service profiles
- Display accounting information, which allows to display the bill

TES Management User Interfaces design is based on an integration in the general models defined by Prospect and influenced by TINA SA.

TES Management User Interfaces implementation is based on integration of new technologies as Java, CORBA and Web.

4.1.2 Evolution of the Interfaces

Main issue, concerning the evolution of the user interfaces, will be the support of the new IDL provided by the TES Management System.

This will provide new functionality to be offered to the TES -PA and the TES-CA. New functionality will be based on evolution of Service Management areas already considered: subscription and accounting, and, moreover, the new Service Management areas considered for Trial 2.

Other evolution issues of the management user interfaces are:

- Integration in the DSI model, that will mainly provide security features (authentication).
- More possibilities provided to the TES-CA regarding the subscription: online subscription, creation/deletion of the SAGs.
- Provision of a Log Control functionality to the TES-PA, allowing to visualise all the access and modification to the management information maintained by the TES Management System.
- Enhancement of the current user interfaces: help text, check of field formats, etc. This should be based on the feedback that was obtained from system administrators during Trial 1.
- Evaluation for use of new technologies as Java Beans, JMAPI and others.

4.2 CPN

Within the context of customer premises network management the focus is on distributed object-oriented frameworks for managing intranets and customer premises networks. As such, the framework itself will have a number of clients. In keeping with the Prospect desire to promote or project the visibility of the underlying network management systems, it is proposed to develop a Web based management administration tool for CPNs. This tool will support the FCAPS functional selection of the project within the context of the CPN. Additionally the CPN_OS module within the VPN service will be evolved.

4.2.1 A three-tier approach to CPN management and an object-oriented intranet management framework

A three-tier architecture has been adopted for the CPN management systems. This is based on an adaptation of the NMF’s omnipoint integration architecture [NMF94], as shown in Figure 12. This was adapted to produce the CPN management architecture shown in Figure 13.

The essence of the NMF’s system management framework, as shown in Figure 12, is that there needs to be some form of independent interface definition notation (IDN) that can capture the semantics of the underlying management domains and their corresponding management information models. This - together with a number of abstract components, that is, adapter objects, composite objects, and intelligent objects - provide the basis for an integration framework, in which a coherent approach to handling multiple management systems and protocols can be developed. The architecture shows that underpinning this framework are the access facilities, which provide the basic mechanisms which provide the communication capabilities for the exchange of management information. SNMP, CMIP, and distributed computing platforms, such as CORBA are identified at the access facilities level. Proxies are also specified as a fundamental mechanism for achieving interworking, at the access facilities level.

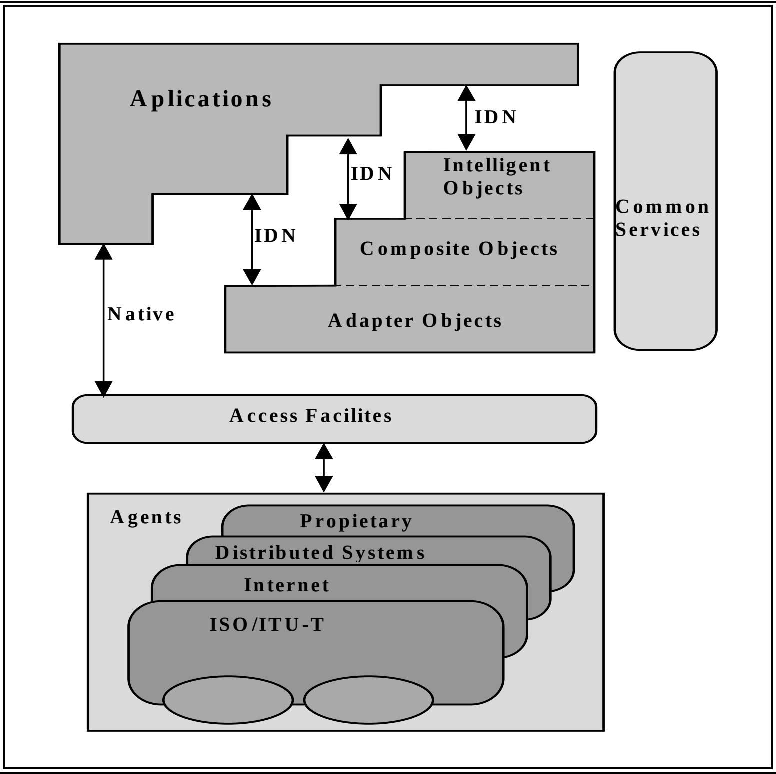


Figure 12: NMF's Omnipoint Integration Architecture

Within the framework a management application can be constructed having various levels of abstraction and sophistication. At a basic level the management application interacts with the access facilities, and as such it must have in-built knowledge of the underlying management technologies, that is their models and protocols.

By using a set of object adapters, a set of object abstractions are defined. These abstract the underlying resources and encapsulate the management model/protocol, performing the relevant translations and mappings. The management application is relieved of having to know all the details of the underlying management technologies, and only interacts with the appropriate object abstraction.

With the composite object approach the trend is towards a single uniform object model that encapsulates all the underlying objects models, which are then accessed through a coherent service interface. This is similar in approach to that of TINA-C's DMF; it is also at the same level of abstraction as the GOM [BAN96a] approach; and has strong relationship to the 'facade' design pattern [GAMM95]. The structure of a composite object may be recursive. This approach builds upon those of the object adapter and access facilities.

The intelligent object approach captures the behaviour and semantics of the underlying resources in a set of abstract views, together with a set of rules that specify the behaviour of the system. They embody the processes which govern a collection of resources. Intelligent objects provide for dynamic, adaptive management solutions.

4.2.2 CPN Management Architecture

For the CPN management system the omnipoint architecture has been adapted to that of a three-tier architecture, as shown in Figure 13. At the upper level is the management application with the corresponding object model derived from an FCAPS functionality perspective. This is under pinned by the CPN framework and its corresponding object model. This is equivalent to the adapter object layer in the omnipoint architecture.

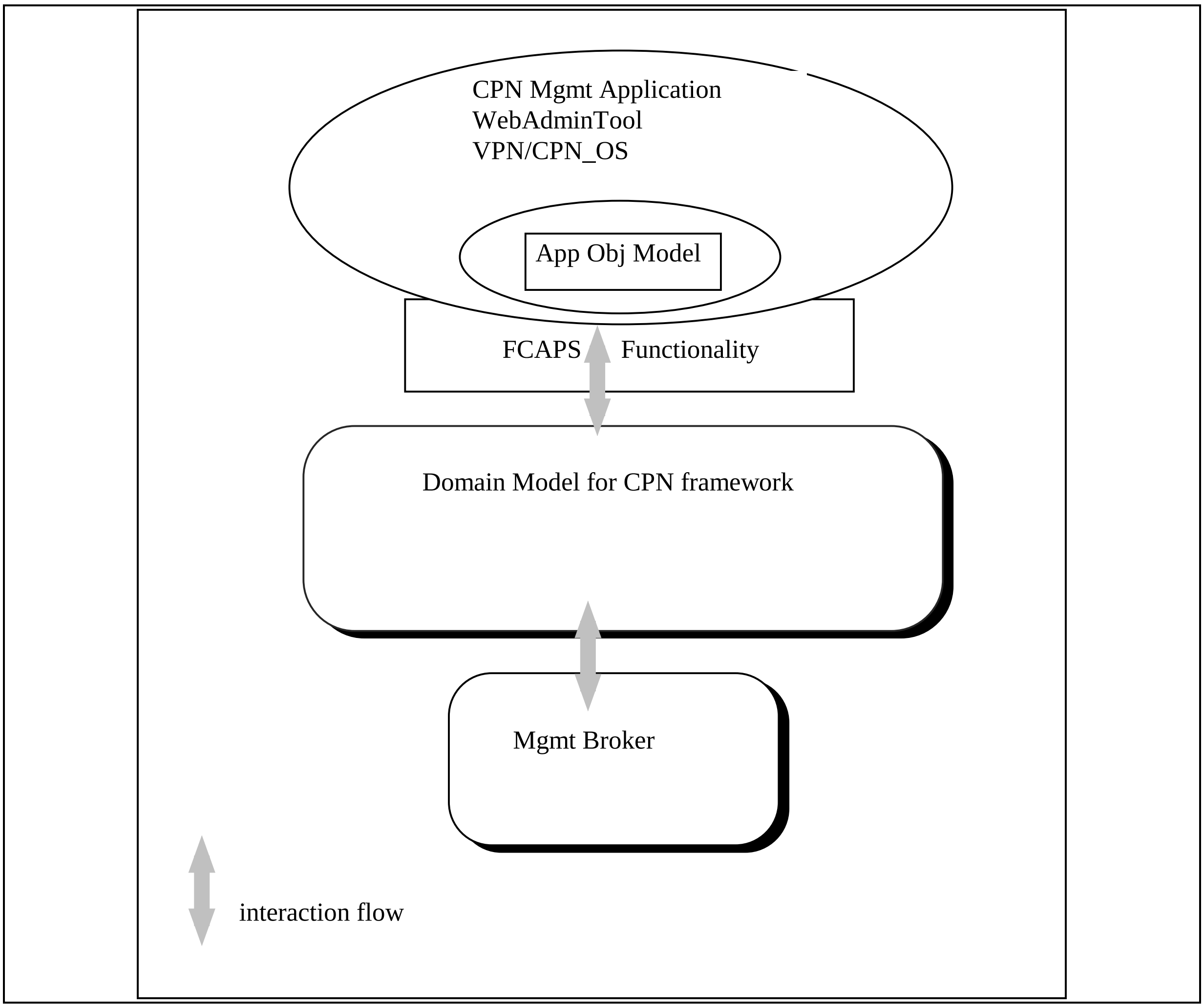


Figure 13: CPN Management Architecture

At the lowest level is a management broker (or brokers). The brokers act as intermediaries for the interacting with the target technological domain, for example SNMP or CMIP or some other network management protocol.

The principle objective of the lowest layer is to provide generalised access to the underlying target management facilities, for example to provide SNMP support and interact with the relevant SNMP agents. The management broker is a generalisation of the protocol adapter concept. The explicit design for the management broker has not yet been finalised. Some possibilities are shown in Figure 14.

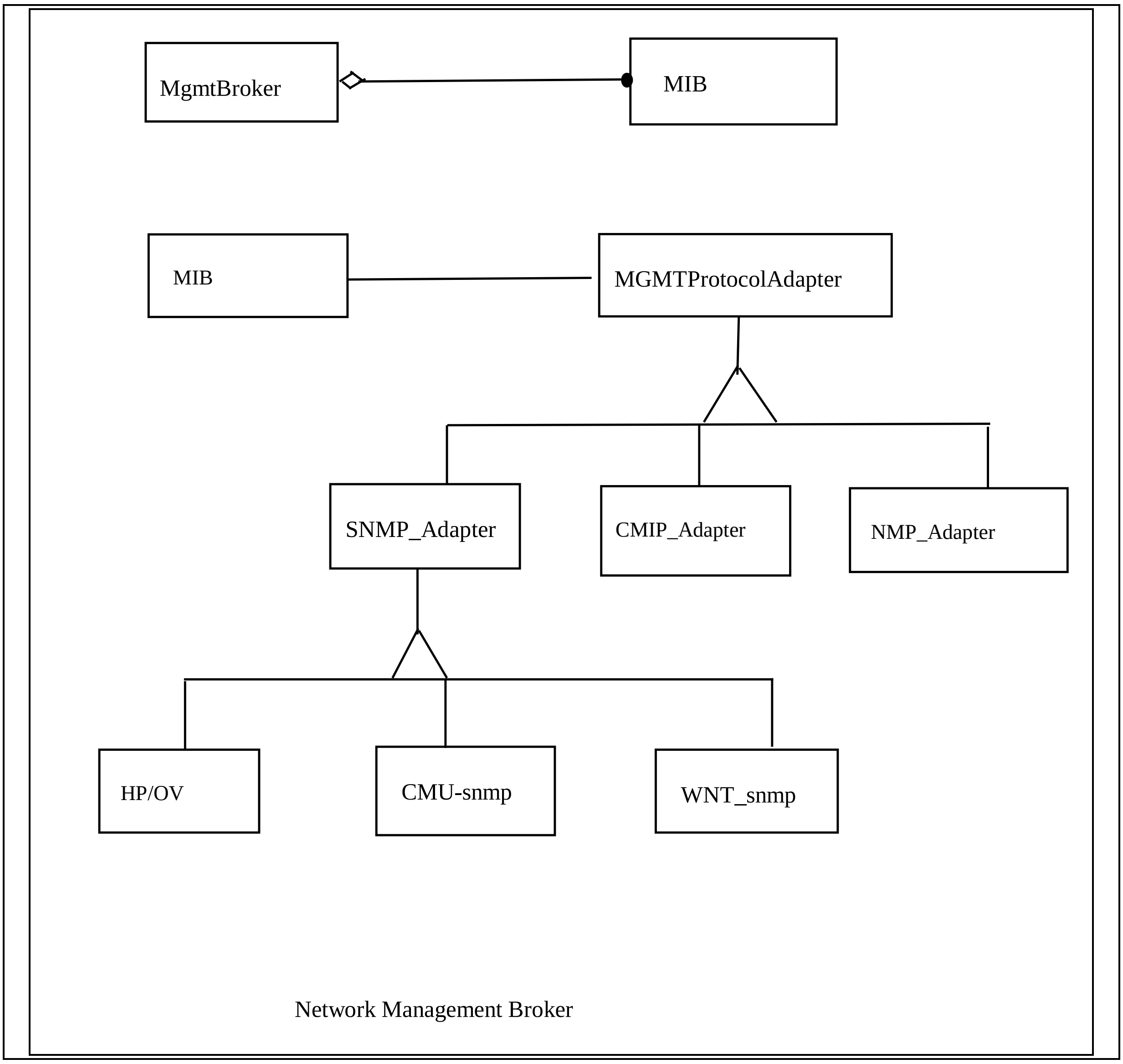


Figure 14: Network Management Broker's Object Model

At the application level object model use is made of a composite object approach to provide a set of functional interfaces encapsulating the FCAPS functionality**.**

4.2.3 Intranet/Customer Premises Network management - Distributed Object-oriented Framework

The role of the CPN management framework is to provide some fundamental abstraction and mechanism, upon which management tools and applications can be built, which will handle all the local network management issues at a customer premises. The main goal is to provide general management components which will handle local network resources, at the customers premises, to support the operations of the 'higher level' management services, for example a CPN_OS in a VPN service, or a Web based administration and monitoring tool, or to provide low level network management services to higher level multi-media tele-services and their corresponding management systems as shown in Figure 15. Additionally, the framework can be used as a basis for the construction of corporate intranet management systems.

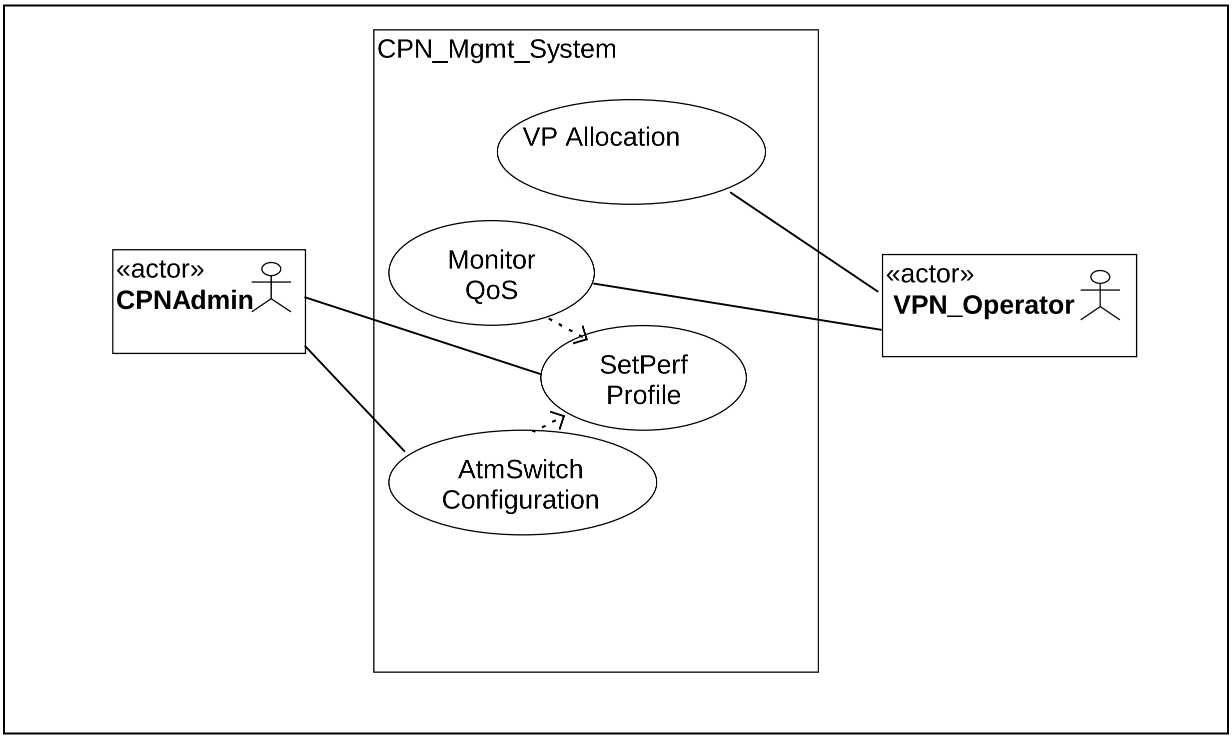


Figure 15: Use Case diagram for CPN performance monitoring.

The framework's focus is the management of local network resources, which include ATM switches, routers, routes, workstations, network interface cards, network addresses, permanent virtual circuits and so on. Because of the diverse range of resources to be managed and the potential for a corresponding diversity in range of management protocols and mechanisms, it is desired to construct such a framework using a flexible and extensible architecture. A common approach in achieving this goal is to use an object model, often the CORBA object model, and to provide a mapping to/from the underlying management 'information model'. Such an approach is adopted for the CPN management framework using the CORBA object model. The work of [Ban96], which presents a generic object oriented model for multi-domain management, uses this approach. This is of particular relevance to the current CPN work. It is a more comprehensive solution in terms of handling multiple management technologies, and would provide a technology integration framework upon which to build CPN management framework.

Within the CPN framework it is intended to provide support for FCAPS management functions, in line with the rest of the Prospect project. Configuration will be the core management service, offering the client the ability to configure the resources, such as routers, VP and so on, contained in the domain. The main requirements on the framework will be dictated by its clients, and in particular the VPN's CPN_OS. Additionally, investigation of Fault, Performance and Security management issues will be undertaken. Various aspects of performance and QoS management are of interest, in particular it should be useful to examine IP over ATM performance and to correlate the two perspectives.

The framework will be instrumented with relevant sensors and actuators to support the appropriate fault management, detection, reporting and recovery.

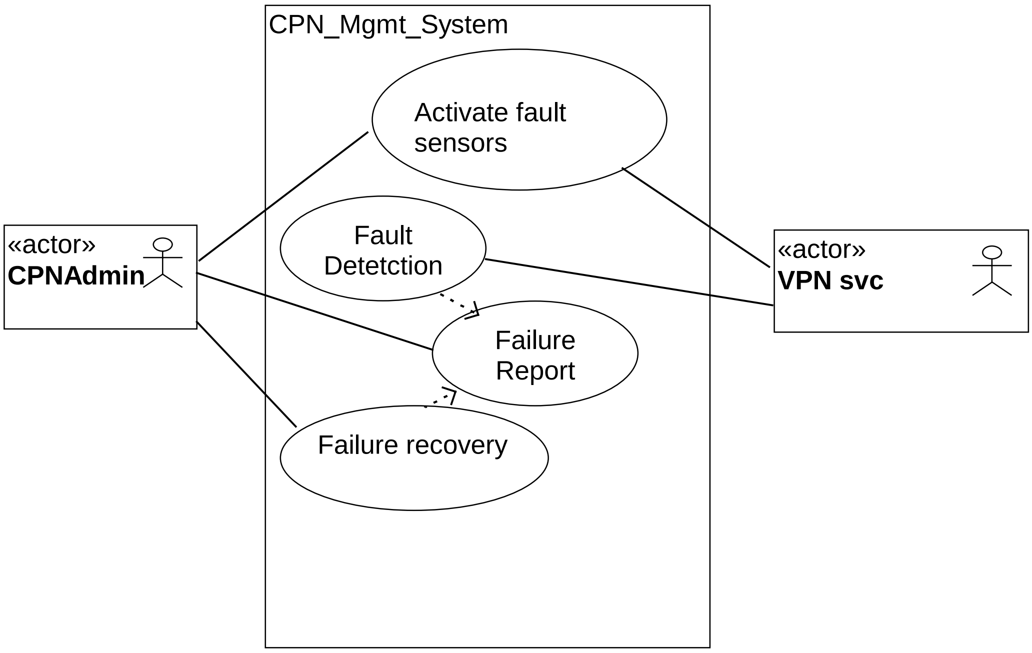


Figure 16: Use Case diagram for CPN fault management

4.2.4 List of requirements

The main requirements on the CPN management system are seen to be as follows:

- Configuration management for routers, local ATM switch VPs, network interfaces, in a LAN based management scenario, and in a ATM LAN based management.
- The CPN management framework, representing the domain CPN model, should exhibit flexibility, extensibility and adaptability.
- Provide transparent access to SNMP functionality.
- Support the selected FCAPS functionality of the VPN service.
- Provide an end-user management interface tool (Webbin' CPN), which is easy to use, is extensible and adaptable.
- Provide support for mapping SNMP traps to relevant CPN domain events.
- Provide 'localised' performance management via TCP/IP throughput monitoring, ATM VP monitoring, and a correlation service between the two.
- Support the relevant functionality for using a public IP service (JAMES IP service).
- RSVP support.

4.3 Public Network, Network Element

At the lowest level of the Prospect system the management of network elements and network layers are found. The present and next section describes the requirements on how to evolve these systems from Trial 1 to Trial 2. The present section deals with the network elements.

4.3.1 State of the art

The implementation of network element management in Trial 1 includes the capability to connect and disconnect at the ATM Virtual Path level according to the ITU-T standard I.751 for management of the of ATM network elements. In Trial 1 VC switching is not supported.

Performance management is supported through Current Data objects, who can be configured to report a number of ATM Cell level statistics collected in the ATM CrossConnect equipment.

A graphical interface - built in Java - displays the connections on an ATM CrossConnect and allows the management user to establish and delete connections and to modify their associated bandwidth.

4.3.2 List of requirements

There are requirements for adding simulation capabilities to the ATM Network Element Level management for Trial 2. The Network Layer management in Trial 2 requires behaviour to generate faults and performance data.

4.4 Public Network, Network Layer

This section complements the previous section with a discussion of how to evolve management of network layers from Trial 1 to Trial 2.

4.4.1 State of the art

In Prospect a distinction is made between the Network Layer and the PN Service Layer. The description of the Trial 1 status is split accordingly.

4.4.1.1 Network Layer

The Network Layer management OS in Trial 1 implements the functionality for ATM virtual path set-up at the Network Level.

The Network Model is based on the work from Prepare, and hence is an ATM profiled specialisation of the ETSI GOM model. The concepts of recursive breakdown of sub-networks into links and sub-networks is implemented. The implementation also supports automatic routing of new connections and the routing information tables can be updated dynamically during the operation on the Network Level Manager OS. The state of the network is visualised through a graphical interface based on a Java applet fetching the Network Level management MIB through a CMIP/Q3 interface.

The Java graphical interface provides the management user with easy access to setting up and taking down ATM connections from a certain level of sub-networks in the GOM hierarchy by just drag-and-drop between the topological points.

The values of bandwidth attributes specified in the connect and disconnect actions to the Network Level OS has currently no effect on the network resources.

Handling of QoS requirements/measurements is not supported by the current information model.

4.4.1.2 PN Service Layer

The PN Service Layer receives from the CORBA/CMIP Gateway the requests for creation and deletion of VPLine objects. It then sends an createAtmSubnetworkConnection/ deleteAtmSubnetworkConnection action to the Network Layer Management OS.

It is the PN Service OS who holds the knowledge of the relation between the E.164 address specified in the create operation and the reference to the Managed Object representing the A and Z end object instances.

There is a textual User Interface to the PN Service OS.

4.4.2 List of requirements

As with the description of the Trial 1 state of the art, the list of requirements is split into two - one for the network layer and one for the PN Service Layer.

4.4.2.1 Network Layer

For Trial 2 the network layer management will be extended with fault management and performance management.

4.4.2.1.1 Fault Management

The Network level manager will correlate and aggregate alarms and state change notifications emitted from the underlying network elements and provide to the management user a view of which connections are affected by the fault conditions in the network elements.

The different severity levels of received and cleared will alarms will be co-ordinated.

The fault conditions can be provoked by either manipulating the hardware (pulling a fibre, resetting a CrossConnect, etc.) or by including a simulated faulty behaviour in the Network Element Management OS. The last option is seen as the most feasible during the period of development of the Fault management system, and the first is maybe appropriate for the final demonstration in a trial situation.

4.4.2.1.2 Performance Management

The Network Level manager will collect performance measurements from the underlying Network Elements. It will use advanced statistical calculation schemes to deduct measures for the perceived QoS values on each connection, for the purpose of keeping the agreed level of QoS with the end user.

In cases where no CurrentData objects are available, the ITU-T X.738/X.739 [ITUT738,ITUT739] generic objects for performance management will be used for the collection of performance measurements.

The validity of the statistical calculations depends on the presence of realistic ATM level traffic patterns. That is difficult to achieve in the Prospect trial environment as long as the available bandwidth is limited to unrealistic low values by the James network. It is therefore planned to extend the Network Level management OS with the capability to generate statistical measurement values by simulation.

4.4.2.2 PN Service Layer

The PN service Layer management OS will either be extended to support the new fault and performance management features, or it will be removed as an individual component from the Prospect configuration.

4.5 VPN

This section describes the requirements on a VPN GUI. This document makes a distinction between two kinds of GUIs:

- Operator/UserInterface
  This interface provides access to the functionality in the VPN application, for the purpose of operating the VPN service.
- Visualisation Interface
  This interface gives a visual representation of functionality/topology etc. in the VPN application, for the purpose of demonstrating the principles behind the VPN service.

The requirements for these GUIs are very different by nature. We have decided to focus on the visualisation GUI.

4.5.1 Requirement

The VPN has many aspects which could be interesting to visualise.

- Distribution - the VPN application is a distributed application capable of running on several host machine, on different hardware and software platforms.
- Autonomous - the components of the VPN application are autonomous, with no central authority.
- Technology heterogeneity in the VPN.

4.5.2 Visualisation Interface

The visualisation GUI could present the following:

- The topological structure of the VPN application (different domains, end users and connections between domains).
- End to end connections (existing connections or connection under establishment).
- Technology (LAN, ATM technology could be visualised in some way).

These kinds of requirement indicates that the visualisation GUI should be highly graphical, and not just list/data based.

A representation of the topology and structure of the VPN, could look like Figure 17.

The VPN application consist of a number of domains (2). A number of end users can be connected to a domain (1). A connection can exists between two domains, which is presented by (3 and 5). If a domain provides a connection through the domain, it can be represented as (4).

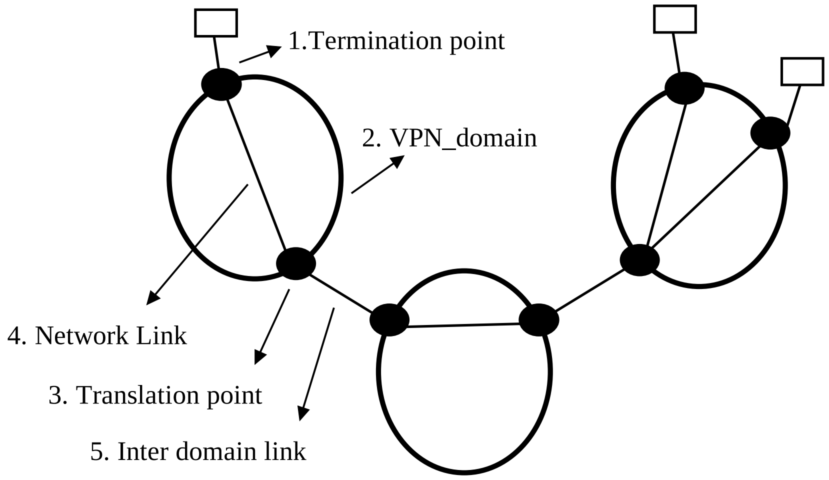


Figure 17: Basic visual parts of the VPN.

The different objects presented in Figure 17 are:

1. TP (termination point). This is a graphical representation of the point of attachment of a terminal.
2. VPN domain. This is a graphical representation of a VPN domain. Here, a domain is a system containing an ‘End-to-end VPN management component, and the underlying network managed by it.
3. NetworkLink. This is a graphical representation of a link between a number of end points (TP or TRP), within one domain.
4. TRP (translation point). This is a graphical representation of the end point where a domain is connected to another domain.
5. Inter domain link. This is a graphical representation of link between two domains.
6. GlobalNetworkLink is an object which model a logical connection between endpoints, residing in different domain.

(1-4 and 6 maps to objects in VPN information model, while 5 is a GUI object, which maps to the pointer which exists between two translation points.)

With Figure 17 in mind, the following requirements can be listed. After each requirement it is stated whether it is actually a requirement (req.), or an idea for future improvement (optional):

4.5.3 Visualising VPN information

- Show all domains (required).
- Show a subset of all domain (optional).
- Show inter domain connection, related to a currently shown end to end connection (required).
- Show all inter domain links (optional).
- Show a specific end to end connection(required).
- Show all end to end connections (optional).
- Show an end to end connection under establishment (optional).
- Show the usage state for all networkLinks (reserved or allocated) (required).
- Show TP related to a currently shown end to end connection (required).

- Show all TPs (optional).
- Show a selected subset of all TPs (optional).
- Show additional object information; other information related to the objects (reservation time, host machine etc.) (optional).

4.5.4 Customisation of screen layout

- Change the position of domains (optional).
- Change position of TP/TRP (optional).
- Change the graphical representation of domains, and TPs (optional).
- Different graphical images for domains, indicating the technology in a domain (ATM, LAN, Q3, SNMP etc.) (optional).
- Different graphical images indicating the type of user/service (optional).
- Show geographical back ground map covering the VPN domains (The area of Copenhagen, Berlin, London and Dublin); the map will be static. (required).

4.5.5 Technical Requirements

- The GUI should be implemented as a Java applet, which can be viewed in a standard WWW browser (required).
- The GUI can be updated by event notifications from the VPN application (required).
- The first GUI will not support queries into the VPN application, but it must be designed for supporting it later on.
- The GUI must be tolerant to missing event information from the VPN application; the missing information can result in incomplete graphical representation of the VPN.
- The GUI must report errors, missing information etc. to the user.

4.6 CORBA/CMIP Gateway

In Prospect there are two conceptual frameworks within which management components have been built. At lower layers components conform with TMN concepts whereas upper layer components draw on CORBA concepts. It is crucial to provide an interworking between these two worlds and within Prospect this is done by means of a gateway that can translate between CORBA primitives and CMIP primitives which are used within the TMN world.

4.6.1 State of the art

The CORBA/CMIP gateway in Trial 1 is hardwired and static, specially build to match exactly the very limited information model of the VP Service component in Trial 1. It is described in detail in Deliverable D33A, chapter 6 [Prospect D33A].

4.6.2 List of requirements

The second version of the gateway (for Trial 2) will provide a generic and flexible approach to CORBA/CMIP interworking which will allow for run-time (re)-configuration of the gateway to facilitate the addition of new agents, object classes, notifications etc., without the need for service interruption.

The Trial 2 CORBA/CMIP interworking solution will be divided into the basic gateway service represented via an number of adapter objects, providing the connection to the CMIP domain, and the value added management services represented via composite objects.

The second version is described in detail in Deliverable D33A, chapter 7.

4.7 WebStore

The tele-education environment within Prospect consists of several end-user services. The first of these, the WebStore, enables course participants to store and retrieve interactive multi-media contents on a dedicated high-performance server. For Trial 2 this service will be enhanced so as to provide improved facilities for manipulating documents and monitoring document access.

4.7.1 Current State

The following list describes the facilities that the WebStore service has provided for Trial 1 sorted by the functional areas they belong to. All of those functions are accessible in two ways: via the role-specific graphical user interfaces which are provided at the WWW (one for each role, i.e. end user, customer administrator and service provider administrator) or via specific IDL interfaces.

Core functionality

- store new documents
- retrieve stored documents
- delete stored documents
- get information about stored documents (e. g. size, creation date, owner, etc.)

Subscription management functionality

- create a new subscription (i. e. add a new customer)
- cancel an existing subscription (i. e. delete an existing customer)
- modify customer data
- add a new user
- delete an existing user
- modify user data

Accounting management functionality

- initialise the billing process
- terminate the billing process
- collect usage information
- calculate a bill
- send a bill
- get accounting information per user (MB per time unit for an end user)
- get accounting information per customer (MB per time unit for all end users of a customer)

Security management functionality

- authorise user
- change password

4.7.2 Evolution of Service

This subsection describes the planned evolution of the WebStore service for Trial 2. This is partly based on original plans for the enhancement and extensions of the WebStore service that already existed before Trial 1 and partly on other service provider requests that occurred during Trial 1.

4.7.2.1 Planned Enhancements and Extensions

Core functionality

- Replacement of the underlying, currently file based, document storage facilities by a commercially available distributed database architecture (e.g. Oracle NCA)
- Manually or automatically initiated notifications of new documents via e-mail to selected addresses containing the URL of the newly stored document
- Customisable user interfaces for specific end users

Accounting management functionality

- provision of additional information for statistical purposes (e.g. number of storages, retrievals and deletions per end user or per customer; number of read accesses per document; duration of an access session per end user, average transfer rate per document)

Security management functionality

- access control editor for the manipulation of document access rights

4.8 HM

The HM service supports the general accounting and subscription systems. For Trial 2 the HM service could supply the parameter values needed by the dynamic charging system - as outlined in section 3.6 on accounting and usage information - if the tariffs selected indicate such a policy.

A dynamic tariffing capability is particularly useful for the HM service; it may even be possible to allow the End-User to change the tariffing parameters (within bounds set by the TES) to reflect their (perceived) usage patterns. For example; a frequent user of information might be charged on a sliding scale, while a once off user maybe charged a larger fixed amount for information usage. (For the infrequent, or once-off, user, copying could be discouraged by reducing subsequent referrals to a lower cost that returns to the full cost over a set time period.) This facility could be used to help counteract the reluctance of users to subscribe to information based services (in the case of the Internet, as stated in [Pitkow]), where both cost of access and quality of information can influence their decision.

The HM service should behave well under heavy load; at the moment the implementation is based on native code (compiled C++) rather than an interpreted language (Java bytecodes) because some basic server testing (using ptester [Signum]) showed the Java based daemon used eight times more processing power than a native code equivalent that supported a higher request rate. This could change with time, however, as compiler technology improves and the Java interpreter implementation is streamlined.

The HM service should also allow easy reporting of errors in service & supported content; currently support is E-mail based, but a form that is served as part of the error document might provide better feedback and more relevant information automatically, enabling faster response from the service provider.

4.9 MMC

Course participants in the Prospect end-user trials communicate by means of the audio/video conferencing tools. These tools put high demands on the bandwidth and quality of service provided by lower layers. In Trial 2 the management of the MMC services will be enhanced with performance monitoring and control and using performance information for accounting will be tested. The services themselves will also evolve, in particular the PC implementation will be improved and facilities for externally controlling video and audio tools will be added.

4.9.1 Current State

The Trial 1 MMC service model consists of the common subscription and accounting management components, the common desktop/service integration model and MMC service specific components. These latter components are a MMC specific USM component, a multimedia conference server (for storing and retrieving conference announcements [Handley2]) and the MMC UAP component. This model is summarised in Figure 18 below.

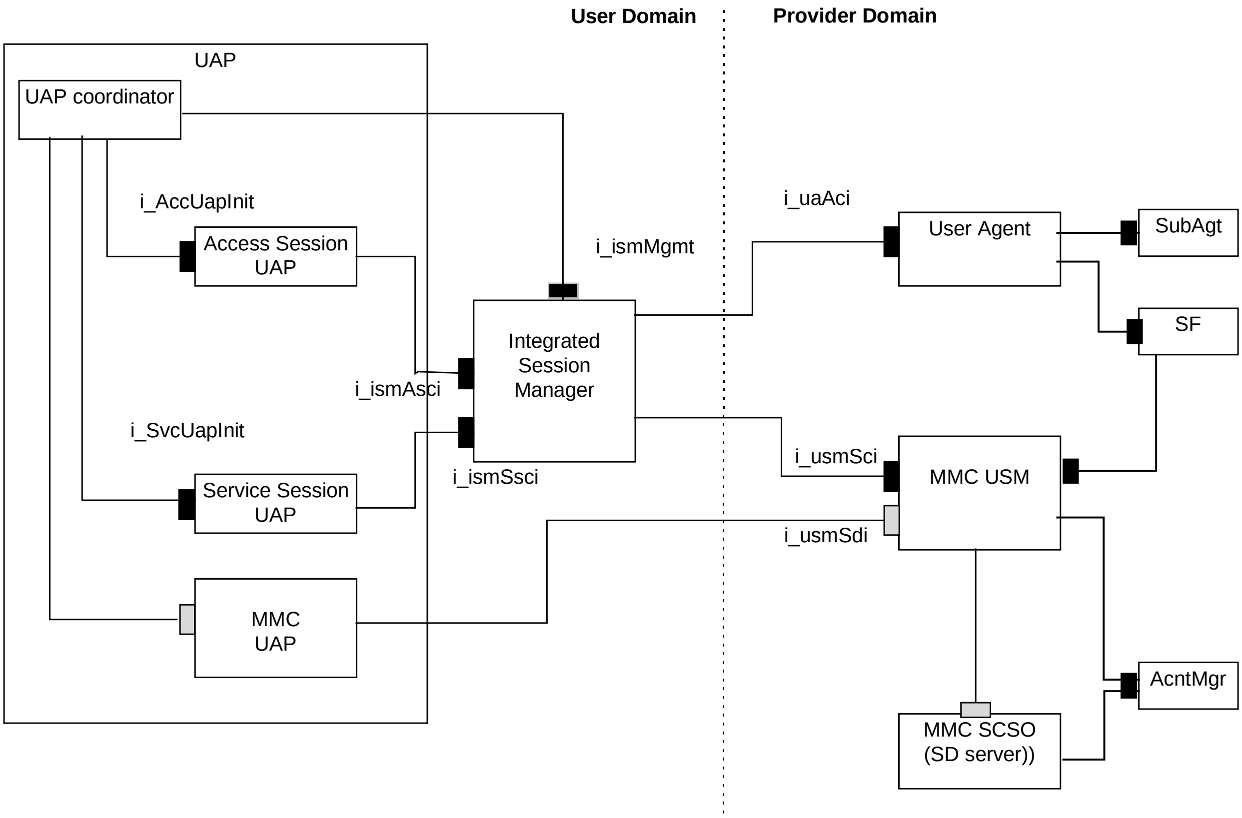


Figure 18: Trial 1 Model for MMC Service

In addition the MMC service uses the stand-alone desktop audio and video conferencing applications RAT and VIC [Bennett, Handley1], with support of the MERCI project. The tools communicate using IP multicast [Deering] operating on an overlay network called the multicast backbone or MBONE. Some control over these tools are possible from the UAP by passing Tcl/Tk commands to the user interfaces of these tools via a TCP/IP port. Further details of the current model can be found in deliverable D4A [Prospect D4A].

4.9.2 Evolution of Service

It is intended that the MMC service reflects changes and enhancements to the common areas of functionality such as subscription management, accounting management and security, as well as incorporating aspect of new common functional areas such as PCS, fault management and performance management. This will be performed largely by the reuse of common implementations that perform these functions, however some MMC service specific functions may need to be considered when integrating with these new or enhanced components. Such considerations include:

- The VIC and RAT tools perform measurements of end to end quality of service they experience using the RTP protocol [Schulzrinne]. If this information could be logged and retrieved in a convenient way from the desktop, it might provide useful information for performance management applications trying to correlate this with network usage and packet or cell loss.
- Similarly performance tools for monitoring the MBONE are becoming available and could also be modified to make the information they collect available to some performance management application.
- Currently the mrouted processes are managed by hand, however they do contain SNMP MIBs. These MIBs could be accessed from configuration management applications, in response to subscription management activities, e.g. setting up multicast tunnels to other mrouted in other parts of the network, or performance management activities, e.g. monitoring cell loss and other performance metrics collected by the mrouteds’ MIB.
- Currently accounting management is not fully integrated with the MMC service. This needs to be included in Trial 2 to enable accounting on the following items:
    - Initiation and termination of an MMC service session for a user
    - Announcement of a conference: detailing conference ID, type (open or invite only), invitees list (if any), media type including quality of service and expected duration.
    - Removing an announcement: detailing conference ID and the time.
    - Joining of a conference: detailing the time he/she joined, the conference ID, the media used, the media quality of service used)
    - Leaving of a conference: detailing the conference ID and the time.

No other enhancements to the management of the MMC service are planned.

The MMC service itself has been assessed thoroughly though the evaluation of Trial 1. Several suggestions have been made concerning the improvement to this services and will be considered for implementation in Trial 2. These enhancements include the following:

- Better non-manual control of VIC and RAT via a programmatic interface. This should allow full control over muting and unmuting of users transmission, control over transmission rates and compression techniques. Such an interface would preferably be provided via a Java class, ideally a down-loadable applet.
- The current MMC UAP implementation only allows the joining of a conference by the user, creating it on the fly with default parameter if the named conference does not already exist. An enhancement to the MMC UAP implementation to allow for the explicit creation of conferences, separate to actually join them would be required. This functionality is already supported by the IDL for the MMC server.
- The version of VIC and RAT running on PCs both experience performance problems. Though this is not something that can be addressed directly by Prospect, any improvement in these tools will be tracked and incorporated in the MMC system.

4.10 Tele-education services

Ideally users of a tele-education service should have the feeling of being an integrated course environment that is mediated by computers; underlying services and management systems should be fully transparent to the end-user. A lot of projects are working on realising this vision. This section first surveys state-of-the-art within tele-education. This survey together with experience from Trial 1 (see section 2.1) forms the basis for the requirements that are presented afterwards.

4.10.1 State-of-the-Art in Tele-education

The present examination of the state of the art in tele-education should be seen as a follow-up to a similar exercise conducted for D21A. In particular this time effort has been concentrated on modifications to the existing Trial 1 system, therefore this should not be seen as an exhaustive state-of-the-art review but rather as a description of some of the influences on our work for Trial 2.

Having completed extensive trials of both tele-educational courses, it became apparent from student responses to evaluation questions, the importance of providing interactive environments in which the students can experiment with the concepts that they are learning. New technologies such as QuickTimeVR, VRML, Java, Shockwave and ActiveX provide a means where this is now possible. Graphics and associated text that was previously presented in a flat two dimensional form can now be presented as live interactive simulation environments which the users can dynamically participate in. The physics department in the university of Toronto use a Java applet to explain the concepts of projectile motion where the user can set the launch angle and coefficient of linear resistance [Sutherland]. The applet animates the trajectory and calculates the properties of the body dynamically. As part of their web-based dynamics course the physics department use this simulation and others to teach the fundamentals of dynamics. Their research indicates that students using multimedia supplements such as video and animation integrated with lecture style audio as supplements to regular course materials did significantly better on tests than students who did not use them [Sutherland].

The potential these technologies provide for performing simulations combined with the flexibility of access to the WWW provides a very potent force for users in an educational environment [Kaplan].

[Abowd] has pointed out that not only should different modes of teaching be supported in a tele-educational environment but also the different styles of learning adopted by students need to be supported. So for instance students who like to annotate their work or the course material should be facilitated in doing so. This is very much in the spirit of the hypertext origins of the WWW. Another point raised by [Abowd] is that all multimedia activity in the virtual classroom should be captured and associated with the relevant course material. For instance, the teachers comments on a particular slide could be captured and stored with the slide in question. Also the conversations of students working on group work could also be recorded and stored with the exercise.

Students require a mix of both synchronous and asynchronous communication. Synchronous communication, such as the student and instructor interacting through audio/video conferencing while working on a collaborative software package has the desired effect of student motivation and retention [Wilson]. Asynchronous activity is just as important. The mix must be adjusted to suit the course and audience. The more asynchronous the material the more flexible the course will become. Self study modules provide the student with asynchronous material which the student can follow at their own pace. Asynchronous activity must be combined with a need to incorporate a structure of continuous feedback and interaction that retains the students attention and insures a satisfactory success rate [Wilson]. An objective of an educational system developed on the WWW by the ELM Group, a part of the cognition and communication group of the department of psychology at the University of Trier, Germany was to reduce the users requirements in hardware and software and let them chose the time and place more freely [ELM]. Tele-educational systems must be adaptable to a users preferences and should support the mobility of students at different locations. In [ELM] the system can be returned to after a previous session with the users former interactions intact.

One successful educational environment was developed at the Renselaar Polytechnic Institute in New York. Here they have developed an environment where the focus is on the student activities rather than the instructors and where emphasis is placed on small group collaborative work and sessions. The instructor plays a supporting role in the learning process rather than an education provider role. From experiences gained in this research, a number of characteristics have been identified as necessary in an effective interactive multimedia distance learning environment [Wilson]. These characteristics are:

1. The use by users of standards based multimedia PCs, equipped with live audio/video and connected to a multicast network
2. The support of synchronous and asynchronous communication
3. Course content authoring to be compatible with industry standard authoring tools
4. Professional quality software tools to be used in the development of the tools, graphics, audio
5. Facility for small group discussions
6. Question and answer for evaluation of student performance
7. Collaborative software for application sharing
8. Floor control to allow classroom co-ordination for both instructor led and student centred learning
9. Administration tools for scheduling of classes, registration of students and resource management

As has been pointed out by [Racsko], it is necessary to note that the overhead of learning authoring tools may be high and in that case only the most motivated of teachers will expend the necessary effort to learn them. However, results of the Interactive Multimedia Distance Learning project at AT&T in conjunction with the experience gained at Renselaar, LearnLinc - a PC-based distance learning environment - was developed, which show the benefits of implementing such an environment. LearnLinc incorporates desktop video conferencing, application sharing, scaleable class sizes, enhanced multimedia authoring tools, and multimedia resource management tools. Studies carried out have shown that participants using LearnLinc have achieved both higher verifiable levels of content retention and higher satisfaction with the distance learning process [Wilson].

WEST, a commercial product discussed in D21A has had many significant changes and developments. It is now known as TopClass and is produced by WBT Systems [WBT]. TopClass is a set of integrated multimedia training tools designed to support the creation and delivery of course materials over networks such as the Internet or a corporate LAN using WWW technology. A particularly interesting aspect of systems built using TopClass is that students conduct all their interactions in an integrated environment which for them will be their classroom. Enhancements it provides are a plug 'n' play capability to easily distribute and transfer courses to other servers, an auto testing capability to evaluate students and customise their course material based on performance and extensive user management providing security and progress tracking. TopClass reduces the administration overhead and changes the paradigm from a situation where the instructor manages and teaches the class to one where the instructor is free to concentrate on teaching and facilitating students.

4.10.2 Requirements

Prospect’s own experience from Trial 1 (and a number of pre-trials) agrees with the conclusions discussed above, but the necessity for appealing and quick-to-learn authoring tools was perhaps even more clear in the trials, than documented elsewhere. The production of tele-educational material is not easy since almost all of it has to be prepared in advance - taking different levels of students’ knowledge into account - and since much of it exploits new techniques such as interactive animations and scripting of multiple-choices. This cannot really be said to come as a surprise - constructing programmed education material has for long been known to be very time consuming. The advent of new communication technologies, however, enables synchronous teaching not much different from traditional tutoring where the teacher can be called whenever a problem arises; moreover the technologies enable new features such as video clips and hyperlinks; it is therefore reasonable to expect that preparation of tele-education material can be done much faster than today. Tools already exist for making animations and for preparing scripts, but these are general tools and have not yet been integrated with the rest of the tele-educational course environment. The Trial 2 service should be enhanced to cope with these problems.

The virtual course facilities also need to be enhanced in other ways for Trial 2. Most of these enhancements follow directly from the end-users' feedback (see section 2.1). Additionally it should be mentioned that in Trial 1 all tools were not fully integrated; e.g. it was apparent for most users that audio and video handling was devoted to two special applications. In Trial 2 all tools will be fully integrated.

To sum up, in addition to the requirements already discussed in section 2.1, at least the following concrete enhancements should be introduced in Trial 2:

- **Definition of templates**: Often one type of educational material will be used several times in a course. E.g. multiple choices can be used repeatedly to check that students have understood previous material; similar it will probably be wise to put animations into a common framework where students can, say, run the entire animation, single-step it forwards and backwards and copy individual pictures to a white board. The course facilities should comprise tools that aid the teacher in defining a few templates for such recurring patterns and let him instantiate them as needed. No knowledge should be required from the teacher about how templates and their instantiations should be required.

- **Authoring tools**: Currently teachers will have to find an ad hoc way to construct course material for the Prospect's course environment; numerous different tools were used in Trial 1, in spite of the fact that all prepared material have a number of similar characteristics and all fit into the same context. To take advantage of the similarities authoring tools should be developed. These tools should support traditional elements such as header/footer, page numbers, preferred way of displaying lists as well as a set of new multimedia features such as pointer and focusing widgets, magnification, animation, hyperlinking. These tools should be fully integrated with the course environment such that tutors automatically get the e.g. the right window size for slides that they prepare.

- **Administration tools - course material**: As a rule, all educational material will be organised into some linear sequence - the default route a student should follow in order to get done with the course. The teacher should have tools at his disposal for organising all this material into different structures. One structure should probably be nothing but the file system into which the material is placed; another should be the logical linear sequence through the material; yet another structure could be used for organising cross references/hyperlinks within the material; and a final structure could reflect structure as it should be perceived by students - i.e. this structure should reflect in which rooms the students will find what.

- **Administration tools - audio/video**: The teacher or some assisting technical manager could be given a “mixing console” from which he can control all participants' attenuation, transmission rates, state (muted/unmuted), coding formats etc. In the pre-trials such a tool could have saved much time initially in lectures that had to be spent on fine-tuning settings of the audio and video tools. Ideally, though, most of this fine-tuning should be done automatically - which would render a mixing console superfluous.

- **Conversion tools**: Teachers are not expected to be willing to start from scratch when they move to the tele-educational setting - they probably rather want to take large parts of their existing course material and port it. The course environment should support and facilitate such conversions. Candidates for conversion are: PowerPoint slides, Word documents, HTML pages, pictures in various formats etc.

- **Better integration**: In Trial 1 audio and video was integrated into the virtual course facilities in the sense that these applications could be launched from applets in the course pages and the audio/video sources could subsequently be muted/unmuted. But there was no integration between the GUI's of the different components. This had various consequences. For instance information about other people in a room could occasionally be found in at least three different places: At the RAT panel, at the VIC panel (accompanied with a picture) and at a panel inside the course facilities. Such duplicated information should be avoided in Trial 2, the video pictures should be integrated with the rest of the course environment and superfluous information should be removed from the GUI.
- **Experimentation**: Technical problems have blocked a thorough assessment of the concepts around which the TES environment has been build. Experimentation is needed before Trial 2 to find additional enhancements.

5 References

[Abowd] G.A. Abowd et al. *Teaching and Learning as Multimedia Authoring: The Classroom 2000 Project*. In the proceedings of ACM Multimedia '96, Boston.

[APACHE] Apache Project. *Apache HTTP Server Project*. http://www.apache.org/

[Bennett] R. Bennett, A. Sasse. *Multimedia Conferencing over the Internet: The MICE project and tools*. Proc. of Networkshop 23, 1995.

[Berson] S. Berson, L. Berger. *IP Integrated Services with RSVP over ATM*. Internet Draft, March 26, 1997.

[Deering] S. Deering. *Host Extensions for IP Multicasting*. RFC 1112, January 1989.

[ELM] ELM Research Group. *Episodic Learner Model - The Adaptive Remote Tutor*. http://www.psychologie.uni-trier.de:8000/projects/ELM/elmart.html.

[Garrett] M. Garrett, M. Borden. *Interoperation of Controlled-Load and Guaranteed Services with ATM*. Internet Draft, March 26, 1997.

[Handley1] M. Handley, J. Crowcroft, C. Bormann. *The Internet Multimedia Conferencing Architecture*. Internet Draft draft-ietf-mmusic-confarch-00.ps, Work in progress, February 1996.

[Handley2] M. Handley, V. Jacobson. *SDP: Session Description Protocol*. Internet Draft draft-ietf-mmusic-sdp.01.txt, Work in progress, November 1995.

[IBM] IBM. *TMN - Extended Fault Management Features*. User's and Programmer's Guide, 1996.

[ITUT509] ITU-T. *OSI – the Directory: Authentication Framework*. ITU-T Recommendation X.509, International Telecommunication Union, Geneva 1993.

[ITUT733] ITU-T. *OSI Systems Management: Alarm Reporting Function*. ITU-T Recommendation X.733, International Telecommunication Union, Geneva 1992.

[ITUT738] ITU-T. *OSI Systems Management: Summarization Function*. ITU-T Recommendation X.738, International Telecommunication Union, Geneva 1993.

[ITUT739] ITU-T. *OSI Systems Management: Metric Objects and Attributes*. ITU-T Recommendation X.739, International Telecommunication Union, Geneva 1993.

[ITUT790] ITU-T. *Trouble Management Function for ITU-T Applications*. ITU-T Recommendation X.790, International Telecommunication Union, Geneva 1996.

[Kaplan] H. Kaplan. *Interactive MultiMedia and The WWW*. Educom Review, Vol. 32, No. 1, January/February 1997.

[Mills] C. Mills, D. Hirsh, G. Ruth. *Internet Accounting: Background (Memo)*. Network Working Group, RFC 1272, November 1991.

[Nahrstedt] K. Nahrstedt, J. Smith. *The QoS Broker*. IEEE MultiMedia, Spring 1995.

[NMF501] Network Management Forum. *Customer to Service Provider Trouble Administration Requirements Specification*. Spec. NMF501 Issue 1.0, 1996, http://www.nmf.org/books.htm#nmf501.

[Pitkow] J.E. Pitkow, C. M. Kehoe. *Emerging Trends in the WWW User Population*. Communications of the ACM, June 1996.

[Prospect D21A] The Prospect Consortium. *D21A - The Initial Requirements analysis*. Public Project Report, CEC id. AC052/DLT/WP2/DS/P/002/b1, The Prospect Consortium, 1995.

[Prospect D33A] The Prospect Consortium. D33A: *Concepts for CORBA/TMN interworking*. Public Project Report, CEC id. AC052/GMD/WP3/DS/S/003/b1.The Prospect Consortium, 1997.

[Prospect D4A] The Prospect Consortium. *D4A: Specification of Existing Management Services for First Trial Phase*. Internal Project Report, CEC id. AC052/LMD/WP4/DS/S/004/b1, The Prospect Consortium, 1996.

[Prospect D53A] The Prospect Consortium. *D53A: Evaluation of the First Trial Phase.* Internal Project Report, CEC id. AC052/TDK/WP5/DS/S/002/a1, The Prospect Consortium, 1997.

[Prospect World] The Prospect Consortium. *The 'Prospect World' Document - End-to-End Inter-Domain Service Management in an Open Service Market*. Public Project Report, CEC id. AC052/TCD/WP2/030/a2, The Prospect Consortium, 1997.

[Racsko] P. Racsko. *Multimedia Courseware Development Strategies in Higher Education*. In the proceedings of Ed-Media/Ed-Telecom '96, Boston.

[Remedy] Remedy Corporation. *Remedy Action Request System*. http://www.remedy.com/ars.htm.

[Sloman] M. Sloman. *Network and Distributed Systems Management*. Addison-Wesley, 1994.

[Schulzrinne] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobsen, *RTP: A Transport Protocol for Real-Time Applications*. RFC 1889, January 1996.

[Signum] Signum support AB. *Phttpd - a multithreaded web server*. http://phttpd.signum.se/phttpd/.

[Sutherland] M. Sutherland. *FUN@LEARNING.PHYSICS*. http://medb.physics.utoronto.ca/Web/website/appletgallery.html.

[Talarian] Talarian Corporation. *RTie 3.5 - Expert System and Inference Engine*. RTworks, http://www.talarian.com/index.shtml.

[TINASA2] *Service Architecture 2.0*. TINA Baseline Doc. No. TB_MDC.012_2.0-94, TINA-C, March 1994

[TINASA4] *Service Architecture 4.0*. TINA Baseline Doc. No. TB_RM.001_4.0_96, TINA-C, December 1996

[WBT] WBT Systems. *Quick Overview of TopClass*. http://www.wbtsystems.com/

[Wilson] J. M. Wilson. *Distance Learning for Continuing Education*. Educom Review, March/April 1997. Volume 32, Number 2.

[X/Open] X/Open. *Common Management Facilities*. Preliminary Specification, Version 2, 1995.

Annex A
Questionnaires for TES Customer/Provider Administrators

Before Trial 1 a questionnaire for administrators at TES customers and providers was prepared. The questionnaire was used later than Trial 1 and results appeared too late to be included in Deliverable D53A. Results are included here instead. The results are presented as a questionnaire filled with figures that represent all responses. For verbal responses only selected answers are displayed.

TES Customer Administration Application:

1. Please give your first impression of the TES customer management service.

useful	*100%*	useless	*0%*
sufficient functionality	*25%*	insufficient functionality	*75%*
fast	*0%*	slow	*100%*
easy-to-use	*25%*	hard-to-use	*75%*

2. What functions the TES management system provides you with do you need most ? Please rate them on a scale from 0 (not important) to 9 (very important).

user management	*9*
site management	*8*
display subscriber information	*6*
display services information	*5*
display accounting information	*8*

3. We believe, that on-line user authorisation and site management are essential features of the management system. What is your opinion ? Do you prefer:

to authorise users and configure sites on-line, or	*100%*
to specify users and sites by filling out paper forms	*0%*

4. The current version of the management system allows you to display subscriber information only. Can you image a scenario where additionally editing functionality is necessary? If yes, please give a brief description of the scenario.

Yes *25%*

the customer should be able to change contact person information.

No *75%*

5. Information about subscribed services is presented at several levels of detail. Which information did you find useful ? Please rate it on a scale from 0 (not useful) to 9 (very useful).

service administrative information	*5.5*
service specific information	*6*
information about subscription assignment groups	*7.5*

6. In the current version of the management system total charges per service per user can be displayed. In addition, access to accounting data, e.g. usage statistics per service per user, may be provided. Would this feature be:

very important *100%* quite important *0%* not important *0%*

7. If problems have occurred during interactions with the service management system, please note them in the following. Examples are service breakdowns and bugs or defects of the application.

a number of actions failed; exceptions were received; sometimes the server crashed.

8. Please feel free to add remarks and suggestions for improvements or enhancements here:

provide on-line help, road map; improve performance; indicate, e.g. through change of cursor shape, that the application is busy

TES Provider Administration Application:

1. Please give your first impression of the TES provider management service.

useful	*100%*	useless	*0%*
sufficient functionality	*25%*	insufficient functionality	*75%*
fast	*0%*	slow	*100%*
easy-to-use	*50%*	hard-to-use	*50%*

2. What functions the TES management system provides you with do you need most ? Please rate them on a scale from 0 (not important) to 9 (very important).

service template management	*8*
subscriber management	*9*
subscription contract management	*8*
customer site management	*7.5*
accounting management	*9*

3. Did you encounter problems to understand the meaning of the fields in the panels ? If yes, please give examples.

Yes *100%*

display service template mapping; assign service profile to a SAG.

No *0%*

4. Do you think access to logging facility reporting all actions carried out by administrators, can be useful ?

Yes *75%*

No *25%*

5. If problems have occurred during interactions with the service management system, please note them in the following. Examples are service breakdowns and bugs or defects of the application.

see TES Customer application.

6. Please feel free to add remarks and suggestions for improvements or enhancements here:

see TES Customer application.

General Questions:

1. In the following management functions are presented which might be necessary or useful. Please indicate the importance of the functionality by rating it on scale from 0 (not important) to 9 (very important).

on line subscription and de-subscription to the service	*8*
automatic installation and configuration of the service	*6.5*
changing subscription details, e.g. adding new users and sites	*9*
on line payment of the course	*8*
receiving charging information, e.g. rates and bills	*6*
receiving accounting information, e.g. service usage per user	*9*
receiving performance information, e.g. network load	*4.5*
receiving notifications about violations of service level agreements	*7*
receiving security related notifications, e.g. failed authentication	*7*

2. So far, your company has to order the service by sending a signed form to the service provider using postal mail. Do you prefer:

on-line ordering, e.g. by filling out a WWW page, or	*100%*
subscription by signed forms via postal mail	*0%*

3. Payment of services delivered over the Internet has become more and more popular. Please mark the one of the following statements you agree with at most.

(a) Payment over the Internet is already secure and I use it whenever it’s possible. *0%*

(b) The software which is currently used for payment over the Internet is not secure enough. But as soon as secure procedures are available I will use them. *75%*

(c) I will definitely not employ on-line payment functions for Internet services. *25%*

4. In future versions of the management system fault management, e.g. trouble ticketing, may be included. Which functionality is important ? Please rate the following functions on a scale from 0 (not important) to 9 (very important).

customer notifies service provider of service breakdown or malfunction	*6.5*
customer requires immediate support, contact to help desk personnel is needed	*9*
customer requires detailed problem report	*3*
customer requires possible fixes or alternatives	*4*
customer requires estimated down-time of service	*8.5*
service provider notifies customer of scheduled down-time	*8.5*

5. In future versions mobility and personalisation of services could be added. Which of the mobility aspects listed below look interesting to you ? Please rate the scenarios on a scale from 0 (not important) to 9 (very important).

role mobility : end-users may act in different roles or a certain role may be assigned to different people; examples for roles are teacher, student, administrator	*8*
personal mobility : end-users may access the service from different locations, e.g. from their office and from home	*8.5*

terminal mobility : end-users may access the service using one terminal attached to different locations, e.g. a laptop *3.5*

application mobility : applications run on different types of terminals and suspended sessions can be resumed on any type of terminal *3*

6. In future versions of the management system Quality of Service (QoS) and performance management may be included. Which functionality is important ? Please rate the following functions on a scale from 0 (not important) to 9 (very important).

definition of a Service Level Agreement *7*

dynamically change the QoS level during a course *5*

provision of performance reports to the customer administrator *6*

payment of the course based on the QoS requested *8.5*

7. Have you already acted as administrator in your company, e.g. network administrator, system administrator or other ? If yes, please describe your job.

Yes *25%*

administrator of a mail system.

No *75%*