FORM

IST-1999-10357

Engineering a Co-operative Inter-Enterprise Management Framework Supporting Dynamic Federated Organisations Management

Document Number:	IST-1999-10357/BRI/WP5/0230_AnnexA
Title of Deliverable:	D10 Validation of Inter-Enterprise Management Framework – Annex A Operational Requirements
Deliverable Type: (P/R/L/I)*	P
Nature of the Deliverable: (P/R/S/T/O)**	R
Contractual Date of Delivery to the CEC:	2002-01-31
Actual Date of Delivery to the CEC:	2002-03-08

Workpackage responsible for the Deliverable:	WP4
Editor:	Niamh Quinn (NQ)
Contributor(s):	FORM Consortium
Reviewer(s):	Soren Vejgaard-Nielsen (UHC), Jacques Brook (KPN)

ABSTRACT

This Annex to FORM Deliverable 10 contains the test plans and conclusions for each of the four test teams and the list of test cases.

KEYWORDS

Evaluation, Validation, Trial, Test cases, Requirement assessment, Fulfilment, IES, VPN, Assurance

See http://www.uhc.dk/form/index.htm for further details

* Type: P:Public, R-Restricted, L-Limited, I-Internal

** Nature: P-Prototype, R-Report, S-Specification, T-Tool, O-Other

IST-1999-10357

FORM

Deliverable D10

Validation of Inter-Enterprise Management Framework

Annex A, Operational Requirements

Editor :	**Niamh Quinn**
Status – Version :	2
Date :	**2002-03-08**
Distribution :	Public
Code :	IST-1999-10357/BRI/WP5/0230-AnnexA

The FORM Consortium consists of:

Atos Origin Intégration (France) – *Project Coordinator*

Broadcom Eireann Research Ltd. (Ireland)	Trinity College Dublin (Ireland)
DELTA Danish, Electronics, Light & Acoustics (Denmark)	UH Communications A/S (Denmark)
Fraunhofer Fokus (Germany)	University College London (UK)
LM Ericsson A/S (Denmark)	Waterford Institute of Technology (Ireland)
TDC Tele Danmark A/S (Denmark)	KPN Research (The Netherlands)

Table of Contents

1 Introduction

This Annex to Deliverable 10 contains the test plans and specifications which were used to address the operational requirements of the Inter-Enterprise Management Framework. Section 2 of this annex contains the operational requirements and test cases lists from Trial 2.

2 Test Plans and Specifications

This section provides test-plan and associated test-cases for the second and final FORM trial (T2).

The test teams are:

Team	Partner(s)	Functional Area
T2-TT1	GMD, UHC, UCL	Subscription & SLA Negotiation
T2-TT2	ATOS, LMD, DELTA, (BRI)	VPN Service Provisioning
T2-TT3	BRI, TCD, TDC	GQIPS Provisioning, Service Assurance and Customer Reporting
T2-TT4	GMD, WIT	Charging and Billing & Customer Account Management

2.1 Trial Team 1: F-IES

The trial system was intended to test the interoperation of the building blocks comprising the fulfilment part of the overall FORM architecture and is based on one-stop shopping.. The Inter-Enterprise Service Provider (IESP) offers a package of services from various service providers and maintains the relationship with the customer on behalf of these service providers. The trial has shown the ordering of a package of services from the IESP via the relevant contracts, i.e. SLAHandling Service. SlaNegEng, and the SLARepository. The trial showed how a customer may subscribe to a service on-line by negotiating the preferred QoS parameters and cost for the service package requested. The SLA is concluded in real-time and stored so that it may be modified at a later date if required.

2.1.1 Trial Planning

Planning for the trial involved establishing the trial objectives and producing two trial plans. Three building blocks and three trial plans were involved, as described below.

2.1.1.1 Trial Objective

Evaluation of:

- The use of schema/DTD for SLA negotiation.
- Applicability of SLA negotiation sequence diagrams
- The scalability/usability of technology mediation in the SLA repository (Script based technology gateway)
- Platform support for SLA negotiation and order handling components
- Integration between SLA negotiation and SLA Handling

2.1.1.2 Trial Plan

Test Case ID	Name	Partner(s)	Planned
T2-TT1-1.1	SLA/SLAR interaction	UHC, UCL	04/12/2001
T2-TT1-1.2	F-IES integration	UHC, UCL, FOKUS	04/12/2001

2.1.1.3 What is Tried/Tested

The purpose of this trial is to test all the implemented F-IES building blocks and their associated contracts.

Building Block(s) (BBs):

BB	Version	Provider	Comments
SNE	v.1.5	UCL	
SLAR	v.0.9	UHC	
SHS	v.0.9	FOKUS	

Contract(s):

Contract	Ver.	Specification URI	RP	Description
SLAHandlingService	1.0	http://www.cs.ucl.ac.uk/research/form/models/ContractCatalogue/fokus.fhg.de/FORM/SLAHandlingService/Contract.xml	IES-CM / Internal	The SLA Handling Service contract is a service management contract and it is provided by the SLA Handling Service building block. This contract is offered at the boundary between the SLA Handling Service and the SLA Negotiation Engine. It allows customers to order services from a service provider and enables SLA negotiation to take place as part of the ordering process.
SlaNegReq	4.1	http://www.cs.ucl.ac.uk/research/form/models/ContractCatalogue/cs.ucl.ac.uk/FORM/SlaNegReq/Contract.xml	Internal	This contract enables a party to enter and complete a SLA negotiation process with a SLA Negotiation Engine. The party entering the negotiation process is a prospective service customer. The SLA negotiation engine is able to control the negotiation process on behalf of a service provider.
SLARepository	1.1	http://www.cs.ucl.ac.uk/research/form/models/ContractCatalogue/uhc.dk/FORM/SLARepository/Contract.xml	Internal	This contract provides functionality to create, modify and delete SLA's and SLA templates in the SLA repository.

2.1.1.4 Test Environment

The tests were run on 3 separate laptops all connected to a shared TCP/IP network.

Hardware Environment:

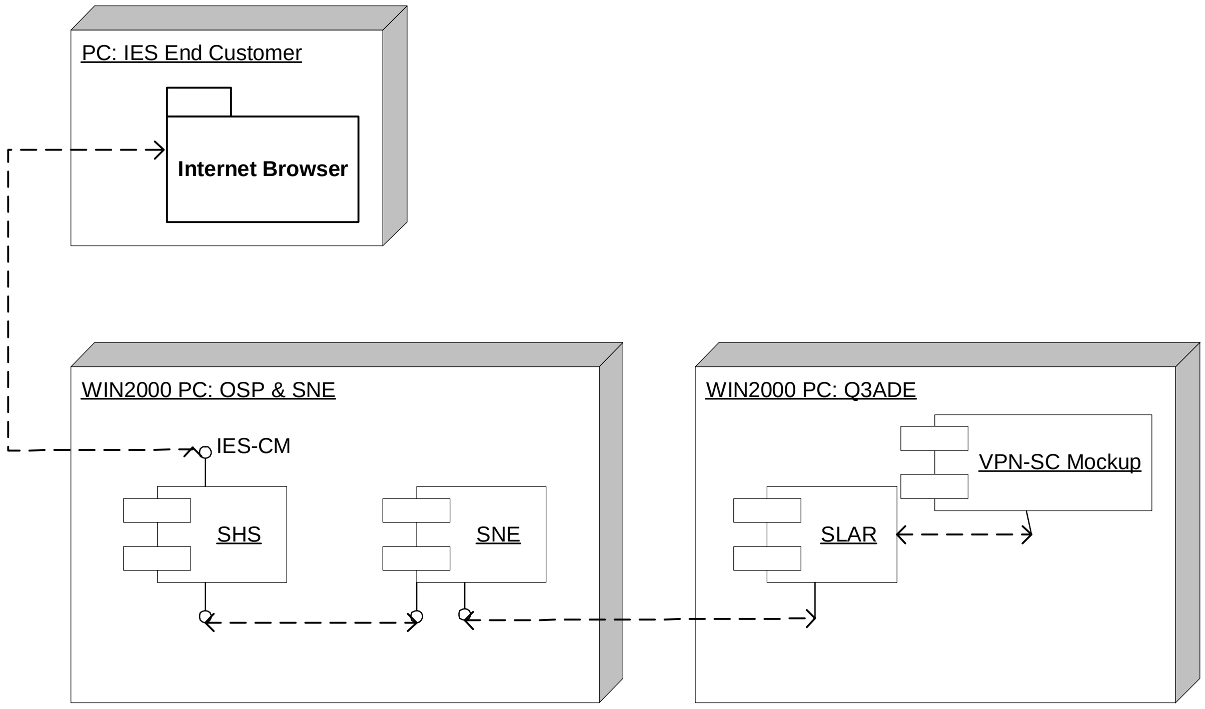
Product	Version	Used By	Provider	Comments
Windows2000 PC		UHC		(SLAR on Q3ADE)
Windows2000 PC / Windows 98		FOKUS/UCL		(OSP & SNE)
PC (IES End Customer)		FOKUS		(Customer applet)

Software Environment:

Product	Version	Used By	Provider	Comments
Q3ADE	504b3[8]	UHC	UHC	
Apache-xerces	1.3.12	FOKUS, UCL	Apache	
Jakarta-tomcat	3.2.1	FOKUS;UCL	Apache Group	
enago OSP[1]	0.9.2	FOKUS	IKV++	

Deployment Diagram

[1] enago OSP is the commercial version of the PLATIN Platform



2.1.2 Test Cases

The tests were broken into two parts. One test case was used to test the interaction and functionality of the SLA and SLAR. The second test case tested the integration of the full F-IES system.

2.1.2.1 Test Case 1.1: "SLA/SLAR interaction"

Test ID:	T2-TT1- 1.1
Event Type:	Common
Location(s):	D/FOKUS
Partners involved:	UCL, UHC
Planned Date:	[start] 11
Trial Planner(s):	AO/UHC
Trial Evaluator(s):	AO/UHC, TT/UCL
Developer(s):	AO/UHC, SVN/UHC, TT/UCL

Purpose

The purpose of this test case is to evaluate the functionality of and interaction between the SNE and the SLAR.

1) SLA negotiation
2) Creation of SLA managed object in SLAR
3) Notification activated translation/propagation of SLA information

Pre-conditions

The SNE and the SLAR is running and the TCP/IP network between are working.

Post-conditions

A trace shows the progress of the SNE and the SLAR

A SLA managed object is created in the SLAR.

A XML document is presented as a trace on the SLAR. This document is an example of a translated SLA to be sent to VPN-SC.

The SNE and the SLAR are in their initial state

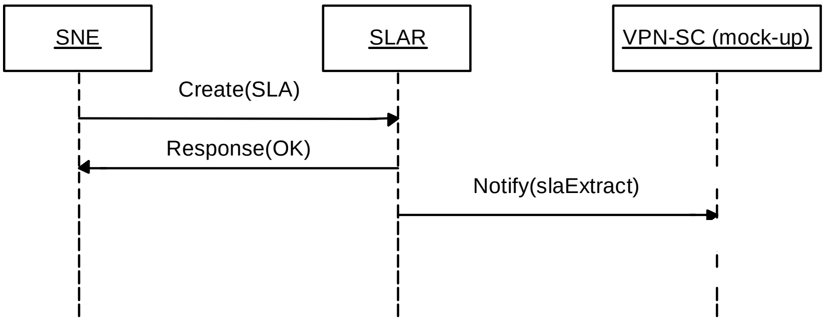
Test Case Success Criteria

1) A SLA managed object is created in the SLAR.
2) The SNE receives an ok response from the SLAR
3) A trace of the translated SLA on the SLAR

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system http://skinfaxe.delta.dk/reqsys_public.

Test Scenario



2.1.2.2 Test Case 1.2: "F-IES integration"

Test ID:	T2-TT1- 1.2
Event Type:	Common
Location(s):	D/FOKUS
Partners involved:	UCL, FOKUS, UHC
Planned Date:	[start] 11
Trial Planner(s):	AO/UHC, TT/UCL, TG/FOKUS
Trial Evaluator(s):	AO/UHC, TT/UCL, TG/FOKUS
Developer(s):	AO/UHC, SVN/UHC, TT/UCL, TG/FOKUS

Purpose

The purpose of this test case is to evaluate the interaction between all the F-IES building blocks, SHS, SNE and SLAR

Pre-conditions

The SHS, SNE and SLAR are running

Post-conditions

1) A service has been agreed on the IES Customer applet
2) SNE traces shows the SLA negotiation progress
3) A SLA managed object is created in the SLAR
4) All the BBs are back to their initial state

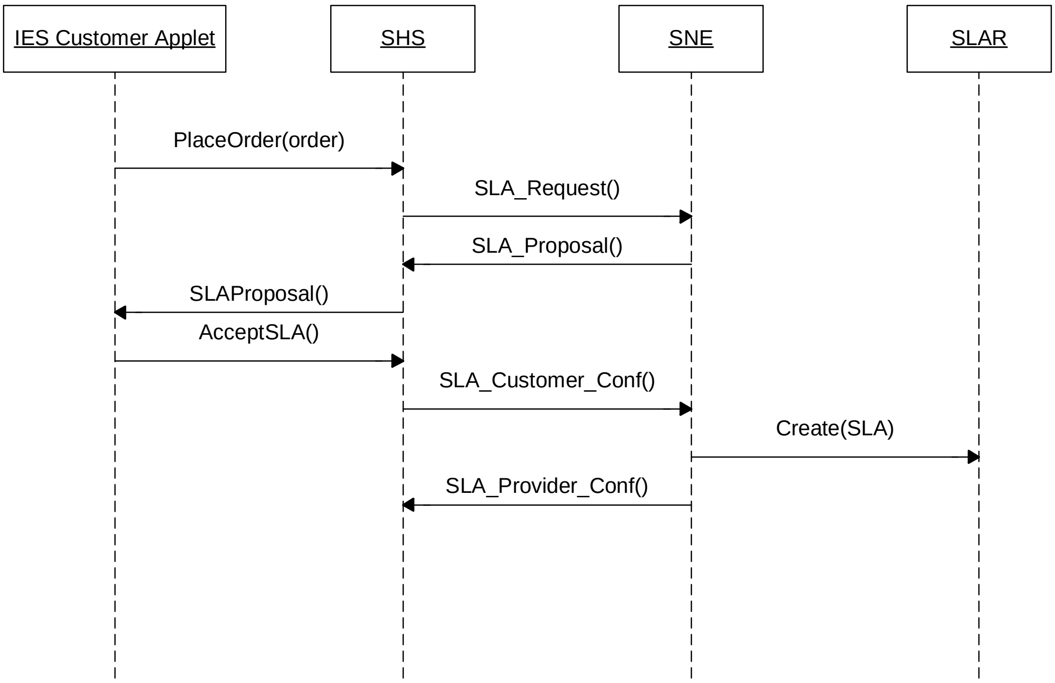
Test Case Success Criteria

See above

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system http://skinfaxe.delta.dk/reqsys_public.

Test Scenario



2.1.3 TT-1 Conclusions

The trial was able to validate the interoperability of the building blocks and their contracts and the objectives listed in 2.1 were fulfilled.

The trial showed that dynamic on-line subscription, including SLA negotiation, for a service that is provided by a third-party provider (MediaShop) was possible. Different bandwidths could be selected by the customer, which resulted in different performance when using the service according to the bandwidth negotiated. The contracts involved in this part of the trial were the SLAHandlingService, the SlaNegReq and the SLARepository.

Further investigations can be undertaken in the following areas:

- Enhancement of the functionality of the SLA Negotiation Engine so that several parameters can be negotiated flexibly.
- Administrative GUIs are needed to configure the building blocks on-line. In the trial this was done manually.
- The different components for subscription, SLA negotiation and accounting were not harmonised, for example, in their tariff usage. This needs to be made consistent across the whole functionality of the underlying information models inside the databases used.
- Integration with VPN-SC

Match Findings/Results with Purpose

The main purpose of the Trial 2, Test Team 1 (TT1) was to validate the functionality of and interoperability of the F-IES building blocks and their contracts.

This included evaluation of:

- The use of schema/DTD for SLA negotiation.
- Applicability of SLA negotiation sequence diagrams
- The scalability/usability of technology mediation in the SLA repository (Script based technology gateway)
- Platform support for SLA negotiation and order handling components
- Integration between SLA negotiation and SLA Handling

The use of schema/DTD for SLA negotiation.

As part of the F-IES trial system three DTDs were created representing each of the BB contracts (SLAHandling Service, SlaNegEng, and the SLARepository). These DTDs proved very useful as part of the individual pre-trial tests conducted by each partner. Test XML documents were exchanged between the partners and validated against the agreed DTD. Therefore most of the building block functionality testing was completed before the trial.

Applicability of SLA negotiation sequence diagrams

A prototype SLA Negotiation Engine was developed as part of the trial system to test the use of policies as part of the SLA Negotiation process. The SLA Negotiation Engine proved capable of validating the SLA requests send by the IES Customer using predefined policies.

The scalability/usability of technology mediation in the SLArepository

The SLA repository was implemented by using the Q3Ade Technology Gateway. XML DOM parser like functionality was implemented and scripts were written to converter the XML encoded SLAs. The script approach proved very useful during the implementation, as changes to the DTDs were easily adapted. Also during integration some handshake problems were quickly solved by minor changes to the scripts. As expected some functionality proved to be too performance critical for the use of scripts and would therefore have to be replaced by compiled code for a real-time environment. The Technology Gateway therefore now implements support for transparent migration of scripts to C++ code. In other words function calls can now be made to C++ code or scripts seamlessly.

Platform support for SLA negotiation and SLA handling components

SLA negotiation was a standalone component and therefore required no platform support. The SLA handling component is a service running on the platform. It needs to be registered in subscription and needs to be started by the user within an access session of the platform. Entries in the subscription database are required before the service can be used.

Integration between SLA negotiation and SLA Handling

The communication between SLA negotiation and SLA Handling Service is done via TCP/IP by transmitting XML documents which need to be parsed at both ends. To support this, valid schema definitions are necessary to ensure a common information model on both sides. XML DOM parser like functionality was implemented and scripts were written to convert the XML encoded SLAs.

Further investigations can be undertaken in the following areas:

- Enhancement of the functionality of the SLA Negotiation Engine so that several parameters can be negotiated flexibly.
- Administrative GUIs are needed to configure the building blocks on-line. In the trial this was done manually.
- The different components for subscription, SLA negotiation and accounting were not harmonised, for example, in their tariff usage. This needs to be made consistent across the whole functionality of the underlying information models inside the databases used.
- Integration with VPN-SC

Requirements Impact

SLAs are becoming increasingly significant in selling services and so flexible on-line negotiation was an important requirement for the trial. The functionality required led to the generation of the trial test cases so that on-line dynamic negotiation of SLAs could be tested and validated in the trial test cases. The ability to offer service subscriptions via on-line SLA negotiation is a critical element in today’s competitive market and the trial showed that it is possible to build individual building blocks that can operate together to meet this requirement. This addresses requirements EC-II.02, EC-II.03, SA.II.04, SA-II.o5, etc..

In an ebusiness environment, such as that represented by FORM, it is important that services can be rapidly and flexibly subscribed to on-line. It is also important that customers can select the QoS parameters they desire for the service. The trial showed that the QoS of the service being ordered could be selected by the customer. In this case bandwidth, and thus the usage performance, could be determined by the customer. This addresses requirements EC-II.08 and QA-I.01.

The trial showed also that SLA negotiation and conclusion can be undertaken in a one-stop-shopping environment and that various services can be ordered via negotiation of one SLA. This addresses requirements EC-II.07 and SA-IV.08.

2.2 Test Team 2 – F-VPN

2.2.1 Trial Planning

2.2.1.1 Trial Objective

Trial 2 should at least demonstrate two scenarios: (1) Create VPN service and Create VPN Connections. The demonstration will be based on full integration of the VPN-WG BBs: VPN-SC (LMD), VPN-P (ATOS) and IPSec-P (DLT) as well as GQIPS BB (BRI).

Each of the scenarios will present interactions between BBs based on a graphical presentation using FLASH and the VPN-P administrative console.

The focus of T2 is a proof-of-concept functionality test with focus on integration of different BBs.

2.2.1.2 Trial Plan

Test Case ID	Name	Partner(s)	Planned
T2-TT2-1	Request VPN Service	LMD, ATOS, DLT, BRI	T2 trial at Copenhagen, early December 2001
T2-TT2-2	Initiate IPSec-P	DLT, ATOS	T2 trial at Copenhagen, early December 2001
T2-TT2-3	Create VPN Connection	LMD, ATOS, DLT, BRI	T2 trial at Copenhagen, early December 2001

2.2.1.3 What is Tried/Tested

T2-TT2 test cases do not address performance testing.

2.2.1.4 Building Block(s) (BBs)

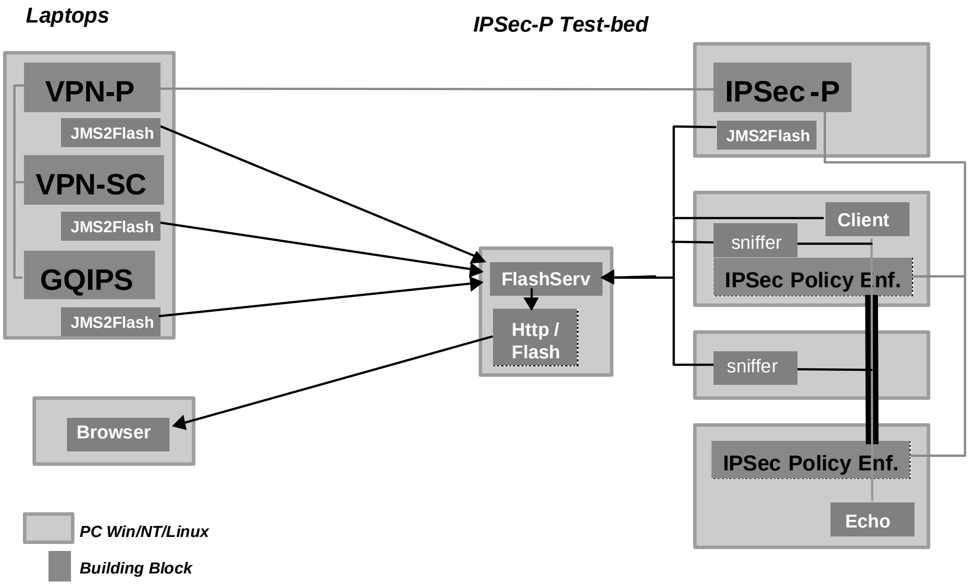
BB	Version	Provider	Comments
VPNServiceConfiguration	v1.0	LMD	
VPNProvisioning	V1.1	ATOS	
IPSec-P		DLT	
IPSecp COPSPR		DLT	Not implemented.
ResourceAllocationManager		BRI	

2.2.1.5 Contract(s)

Contract	Ver.	Specification URI	RP	Description
lmd.ericsson.se/FORM/VPNServiceConfiguration	1.0	http://www.cs.ucl.ac.uk/research/form/models/ContractCatalogue/se.ericsson.lmd/FORM/VP	VPNS-PM	The interface to the VPN Service Provider domain. Contains all the functionality for creating, modifying and deleting VPN topology and

		NServiceConfiguration/Contract.xml		connections.
VPNProvisioning	1.0	http://www.cs.ucl.ac.uk/research/form/models/ContractCatalogue/atos.fr/FORM/VPNProvisioning/Contract.xml		The VPN-Provisioning contract provides separated services for managing the virtual topology of a VPN and then provisioning VPN links (tunnels)
delta.dk/form/ipsec-pContract	1.2	http://www.annecto.dk/annecto/delta.dk/form/ipsec-Contract/contract.xml		The IPSec-Provisioning contract provides management services related to the provisioning (i.e. configuration) of IPSec tunnels using policies
delta.dk/form/ipsecpCOPSPRContract	1.0	http://www.annecto.dk/annecto/delta.dk/form/ipsecpCOPSPRContract/contract-index.xml	VPNS-CM	The IPSec-Provisioning COPS-PR contract provides an interface for COPS-PR (Common Open Policy Service for Policy Provisioning) enabled CPEs to access the IPSec-P building Block to obtain Provisioning Policies.
ResourceAllocation Manager				

2.2.1.6 Test Environment



Hardware Environment

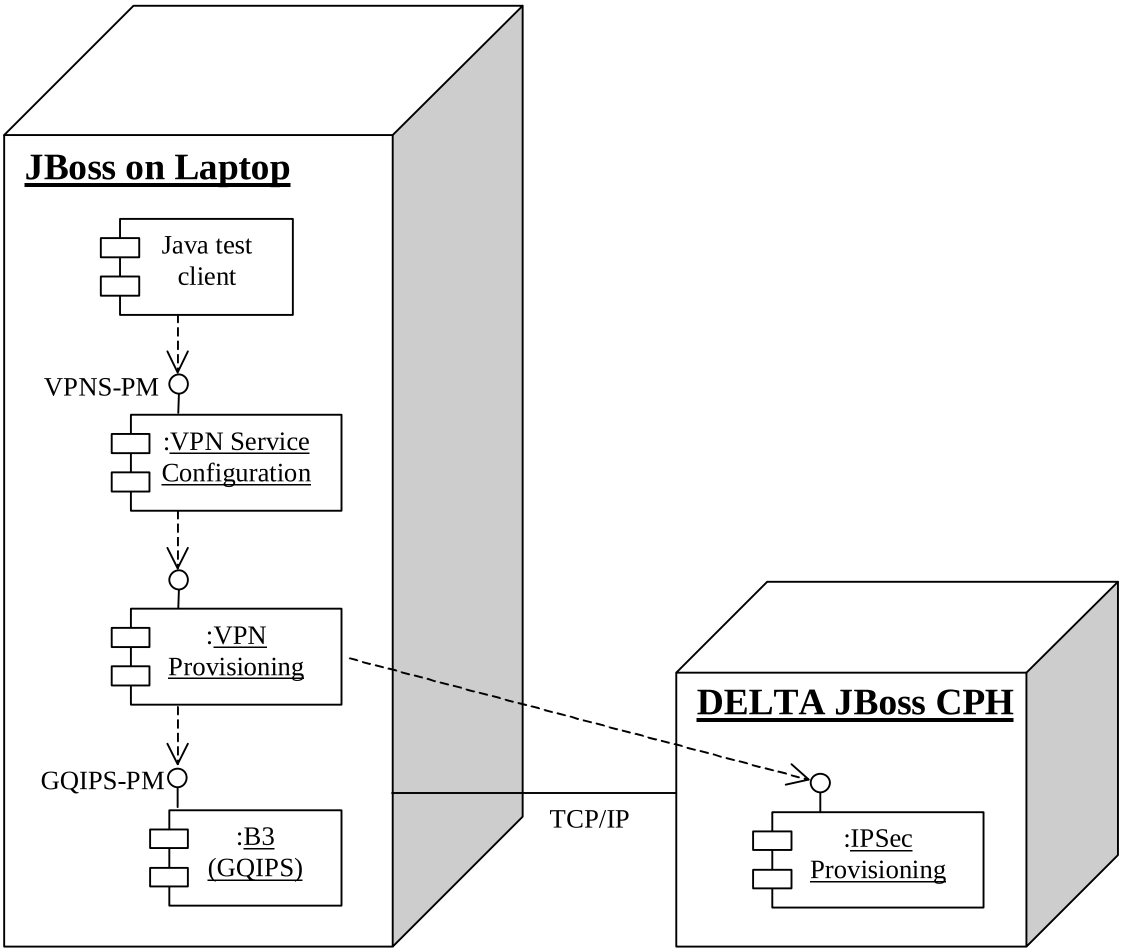
Product	Version	Used By	Provider	Comments
PC 800 MHz 256 MB Ram	PIII	Atos, BRI and LMD		Used for JBoss Application Server for running Atos, BRI and LMD EJBs.
PC 300 MHz 32 MB Ram	K6	DLT		iesp: Inter-Enterprise Service Provider host.
PC 200 MHz 32 MB Ram	K6	DLT		isp: Internet Service Provider host.
PC 200 MHz 32 MB Ram	K6	DLT		cpe1: Customer Premise Equipment host 1.
PC 300 MHz 32 MB Ram	K6	DLT		cpe2: Customer Premise Equipment host 2.
Sun Ultra 1 creator	sparc	LMD, Atos, BRI, DLT		www.annecto.dk:
PIX 506	5.1(2)	DLT	www.cisco.com	Commercial grade Firewall/Security Gateway w/ 3DES encryption

Software Environment

Product	Version	Used By	Provider	Comments
Linux	RedHat 6.2	DELTA	www.redhat.com	Kernel 2.2.x
MS NT 4.0 SP6 or MS Windows 2000 SP1	4.0	Atos, BRI, LMD	www.microsoft.com	Used on above PC
SunOS	5.6	Atos, BRI, DLT, LMD	www.sun.com	
FLASH		DLT		
Application Server: JBoss	2.2.2	Atos, BRI, LMD, DLT	www.jboss.org	
J2SE, Java 2 Standard Edition, i.e. Java 2 SDK, Standard Edition (Software Development Kit) And Java 2 Platform, Standard Edition, Documentation	1.3	Atos, BRI, DLT, LMD,	java.sun.com/j2se	
J2EE, Java 2 Enterprise Edition, i.e. J2EE SDK And J2EE Documentation	1.2.1	Atos, BRI, DLT, LMD	java.sun.com/j2ee	Relies on SDK v1.3
Xerces	1.4.3	Atos, BRI, DLT, LMD,	Freeware available at xml.apache.org	XML parser
MySQL	3.23	DLT	Freeware available at www.mysql.com	Used for storing the information models.
Freeswan	1.9	DLT	Freeware available at www.freeswan.org	IPSEC and IKE implementation for Linux.

Deployment diagram

As DLT has very specific hardware requirements for their IPSec test-bed, they have made it accessible via the Internet. Therefore the Trial could be conducted anywhere in the world. Currently the remaining BBs are all deployed on the same machine, but this is mostly for convenience and in principle the three BBs could also be running on 3 separate machines.



2.2.1.7 Trial Results Specification and Evaluation Criteria

- The participants of the trial notice most of the results visually. There are several ways to do that, complementary or redundant, depending on the BB:
  - **Event displayed by the Flash tool on screen**. These events were defined by the developers of each BB and should represent important step of processes (ex: create VPN object in VPN-P BB, SLA accepted in GQIPS BB, activate PEP in the IPSEC-P BB).
    - ➢ **All the BB of the VPNWG implements a flash event sender.**
  - **Event displayed by the reporting console.** These events were defined by developers and, as flash events, should represent important step of processes.
    - ➢ **GQIPS BB and VPN-P BB implements a report sender.**
  - **Event displayed by non-persistent logging system.** Each BB displays these events on the server DOS console. They represent successes or fails of processes, exception stacktrace for example.
    - ➢ **All the BB of the VPNWG implements this logging mechanism.**
  - **Event displayed by persistent logging system.** GQIPS BB writes events in a log file on the server.
    - ➢ **GQIPS BB BB implements this logging mechanism.**

- For each result waited in test case post-conditions chapter, the BB operator must define an event specification:

Result[1]	Log media[2]	Success statement[3]	Fail statement[4]
Creation of the SAG Object	VPNP; Flash	SAG created	
Creation of the SAG Object	VPNP; R-console	SAG creation	
Creation of the SAG Object	VPNP; S-console	VirtualTopologyManagerBean.createSAG: SAG created with id *xxxx*	InterfaceException:VirtualTopologyManagerBean.createSAG: + *error*

(1) Should be a post condition statement

(2) Should be: "BB Name";{Flash | R-console | S-console | File}

(3) Should be: the text displayed

(4) **Should be: the text displayed**

- The Operational Requirements relations to the various test cases are managed through the FORM trial-to-requirement mapping web-system. http://skinfaxe.delta.dk/reqsys_private using the evaluation criteria in: *Evaluation Criteria for Operational Requirements (*IST-1999-103571/DLT/WP4/0338*)*.

2.2.1.8 Trial 2 set up

Trial 2 Network infrastructure

Network infrastructure for IPSec-P testbed

The JBoss Application Server is located on a host called *form.delta.dk*. The hostname is not resolvable through DNS and must be resolved by external users through an entry in the users *hosts* file (that is probably /etc/hosts on a Linux-box and C:\WINNT\system32\drivers\etc\hosts on Windows2000-box).

Setup for BBs using IPSec-P from outside firewall (*130.226.137.80*).

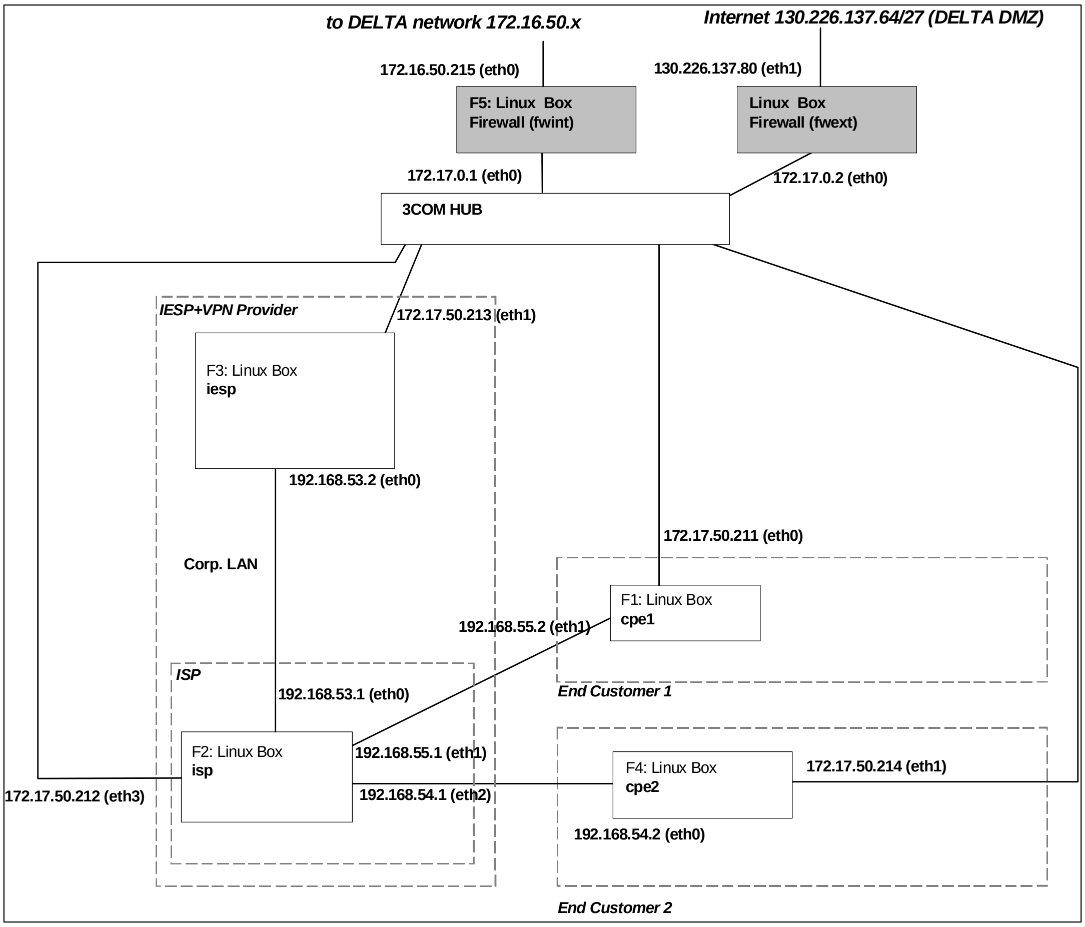
The IPSec- P testbed is located behind a firewall (*130.226.137.80*).

form.delta.dk must be resolved to *130.226.137.80* in the *hosts* file.

Users must be able to telnet outbound on ports 1036, 1099, 4444 (used by the JBoss Application Server) and 9009 (used by the FlashServer).

Setup for BBs using IPSec-P from the same net (*172.17.0.0/255.255.0.0*)

form.delta.dk must be resolved to *172.17.50.213* in the *hosts* file.



Standard set-up script and environment variables

Like any Java program, the application needs a PATH and CLASSPATH well positioned environment variables to run properly. These variables are positioned into two set-up scripts COMPUTERNAME_env.bat and env.bat.

The former is dependant on the host where the program is running; it contains especially the definition of HOME variables that represent absolute path of the root directory of library needed. The latter is independent on the host, and position relatively the environment variable PATH and CLASSPATH using the variables defined in COMPUTER_NAME_env.bat. Therefore installing the application on an other host needs only to update the COMPUTER_NAME_env.bat and a user has just to know the root directory of component needed (JDK, J2SDKEE, JAKARTA_ANT, JBOSS…).

VPN-SC and VPN Customer configuration/set up

VPN Customer

The VPN customer is a normal Java program, which calls the VPN-SC BB. It is pack in a .jar archive and is provided with a .bat script, which sets up a classpath, which relies upon the standard set-up described above.

VPN-SC BB

The VPN-SC BB is in form of a .ear archive, where the major requirement is a JBoss2.2.2 and Tomcat 3.2.2 installation.

Further more the following must be installed:

- **Properties**. The VPN-SC BB expects the following properties to be defined:

- *atos.vpnpbean.JNDIname* should contain the JNDI name of the VPN-P BB
- *vpnsc.itutbean* is internal and should contain the JNDI name of an internal VPN-SC bean the ITU-T EJB. This should normally be *ITUTConfiguration*

  These properties should be defined in the *%JBOSS_HOME%\conf\default\jboss.properties* file or *%JBOSS_HOME%\conf\tomcat\jboss.properties*

- **XML Schemas**. The XML Schemas for VPN datatypes, VPN-SC input/output and VPN-P input/output are expected to be on the DELTA web-server on the addresses below. *http://www.annecto.dk/annecto/form/shared/vpn.xsd*
  http://www.annecto.dk/annecto/form/lmd.dk/vpn-sc-services.xsd
  http://www.annecto.dk/annecto/form/atos-origin.fr/vpn-services.xsd
- **JMS properties**. To *%JBOSS_HOME%\conf\default\jbossmq.xml* the following should be added

  ```
  <Topic><Name>vpnsc</Name></Topic>
  ```

For “installation” the VPN-SC.ear can just be dropped in the *%JBOSS_HOME%\deploy* directory as it should be self-contained. The JMS2Flash mapper has been wrapped as a Message Driven Bean and is included in the archive.

VPN-P configuration/set up

The VPN-P BB is in form of a .jar archive, where the major requirement is a JBoss2.2.2. Nevertheless JBOSS must have a VPN-P proper configuration:

- **JMS properties.** The VPN-P expects the following properties to be defined:
  - A XML property should be defined in *%JBOSS_HOME%\conf\default/ jbossmq.xml* or *%JBOSS_HOME%\conf\tomcat\ jbossmq.xml:*

    ```
    <Queue><Name>Administrator</Name></Queue>
    ```

- **JAWS properties.**
  - XML properties should be defined in *%JBOSS_HOME%\conf\default/ standardjaws.xml* or *%JBOSS_HOME%\conf\tomcat\ standardjaws.xml* (at the end of the file)*:*

```
<enterprise-beans>
      <entity>
            <ejb-name>StubNetworkInterfaceBean</ejb-name>
            <finder>
                  <name>findByIpAddress</name>
                  <query>ipAddress  = {0}</query>
                  <order></order>
            </finder>
      </entity>
      <entity>
            <ejb-name>ProtocolBean</ejb-name>
            <finder>
                  <name>findByNameVersionRevisionAndVendor</name>
                  <query>
                         name = {0} AND version = {1} AND revision = {2} AND
                                                               vendor = {3}
                  </query>
                  <order></order>
            </finder>
      </entity>
            <entity>
            <ejb-name>SecurityComponentBean</ejb-name>
            <finder>
                  <name>findByTopLevelAndSubclassification</name>
                  <query>
                        topLevel = {0} AND subClassification  =  {1}
                  </query>
                   <order></order>
            </finder>
       </entity>
       <entity>
            <ejb-name>ServiceClassBean</ejb-name>
            <finder>
                  <name>findBySecAndQOSComponent</name>
                  <query>
                        securityComponentId = {0} AND qosComponentId = {1}
                  </query>
                   <order></order>
            </finder>
          <finder>
            <name>findBySecAndQOSValue</name>
            <query>
                  ,QOSComponentBean, SecurityComponentBean WHERE
                  ServiceClassBean.securityComponentId =
                  SecurityComponentBean.id AND
                  ServiceClassBean.qosComponentId = QOSComponentBean.id AND
                  SecurityComponentBean.topLevel={0} AND
                  SecurityComponentBean.subClassification={1} AND
                  QOSComponentBean.serviceType={2}</query>
            <order></order>
          </finder>
       </entity>
</enterprise-beans>
```

- **XML Schemas**. The XML Schemas for VPN datatypes, VPN-P input/output and IPSEC-P output are expected to be on the DELTA web-server on the addresses below. *http://www.annecto.dk/annecto/form/shared/vpn.xsd*
  http://www.annecto.dk/annecto/form/atos-origin.fr/vpn-services.xsd
  http://www.annecto.dk/annecto/form/atos-origin.fr/vpn-services.xsd

- **VPN-P installation.** The VPN-P.jar can just be dropped in the *%JBOSS_HOME%\deploy* directory as it should be self-contained.

- **Reporting and administration console.** The two zip files (reporterConsole.zip, administrationConsole.zip) should be extracted anywhere. The env.bat script must be called before launching with the run.bat script.

IPSec-P configuration/setup

The IPSec-P BB is in form of a *.jar* archive, where the major requirement is a JBoss2.2.2 and Tomcat 3.2.2 installation.

Further configuration/setup:

- **JMS properties.** The IPSec-P BB expects the following properties to be defined in $*JBOSS_HOME/conf/default/jbossmq.xml* and $*JBOSS_HOME/conf/tomcat/jbossmq.xml* on the JBoss application server (Iesp):

  ```
  <Topic><Name>ipsecp</Name></Topic>
  ```

- **XML Schemas.** The XML Schemas for IPSec-P BB input from VPN-P BB are expected to be on the DLT web-server *www.annecto.dk*:
  http://www.annecto.dk/annecto/delta.dk/form/ipsec-pContract/xml_interface/ipsec-p.xsd and
  http://www.annecto.dk/annecto/delta.dk/form/ipsec-pContract/xml_interface/pep-if.xsd

- **BB deployment.** The IPSec-P BB (ipsecp.jar) should be copied to $*JBOSS_HOME/deploy* directory on the JBoss application server (Iesp).

The IPSec-P testbed is distributed on 4 hosts: Iesp, Isp, Cpe1 and Cpe2.

Iesp (Inter-Enterprise Service Provider host):

- MySQL database server with IPSec-P repository tables.
- JBoss Application Server hosting IPSec-P BB.
- IPSec-P BB (ipsecp.jar).
- Jms2Flash gateway used for demonstrations.

Isp (Internet Service Provider host)**:**

- IP-Sniffer capturing IP-packets en route between CPE1 and CPE2 used for demonstrations.isp_sniffer

Cpe1 (Customer Premise Equipment host 1):

- Freeswan IPSec implementation.
- Ipsec-proxy used for reconfiguration of Freeswan.
- Echo-client used for demonstration.

- IP-Sniffer capturing IP-packets from CPE1 to CPE2 and vise versa used for demonstrations.

Cpe2 (Customer Premise Equipment host 2):

- Freeswan IPSec implementation.
- Ipsec-proxy used for reconfiguration of Freeswan.
- Echo-server used for demonstration.

GQIPS configuration/set up

The GQIPS BB is in form of a .jar archive, where the major requirement is a JBoss2.2.2. Nevertheless JBOSS must have a GQIPS proper configuration:

- **XML Schemas**. The XML Schemas for GQIPS datatypes, GQIPS input/output are expected to be on the FORM web site, in the BB Contract specification:

http://www.cs.ucl.ac.uk/research/form/models/ContractCatalogue/broadcom.ie/FORM/ResourceAllocationManager/Contract.xml

- **GQIPS BB Installation.** The b3-jboss.jar can just be dropped in the *%JBOSS_HOME%\deploy* directory as it should be self-contained. Then the b3-jboss-client.jar should be dropped into the *%JBOSS_HOME%\lib* directory.

- **Configuration of the network topology for GQIPS.**
  GQIPS BB needs the network topology (endpoints, provider nodes, links, resources available) to proceed.

  GQIPS BB is delivered with a graphic console that allows the topology to be created or imported from an XML file (following an XML-Schema defined by BRI). The topology should be exported after alteration into an XML file and stored into the database of the application server via the B3 entity bean (menu *store*). The console should be started by running the *jb.r.B3Console.ie.bri1.bat* script.

FlashServer configuration/setup

- The FlashServer shall be running on *www.annecto.dk* before any demos are started.
- It listens to port 9009 for incoming connections.

2.2.2 Test Cases

Before the test cases are described the general business scenario is described. The set-up is as follows:

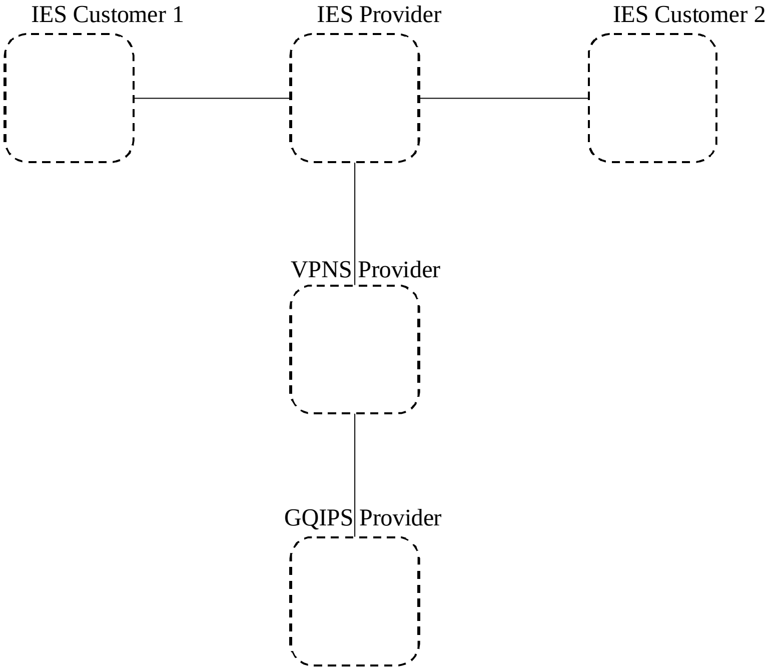


Figure 1 VPN Value Chain

IES customer 1 and 2 want to establish a VPN connection between themselves using the services provided by the IES Provider. The IES Provider in turn bases his services on the VPNS Provider, which in turn uses the services of the GQIPS provider.

In order to establish a VPN connection an abstract topology for the connection between the two customers must be defined. This topology is shown below.

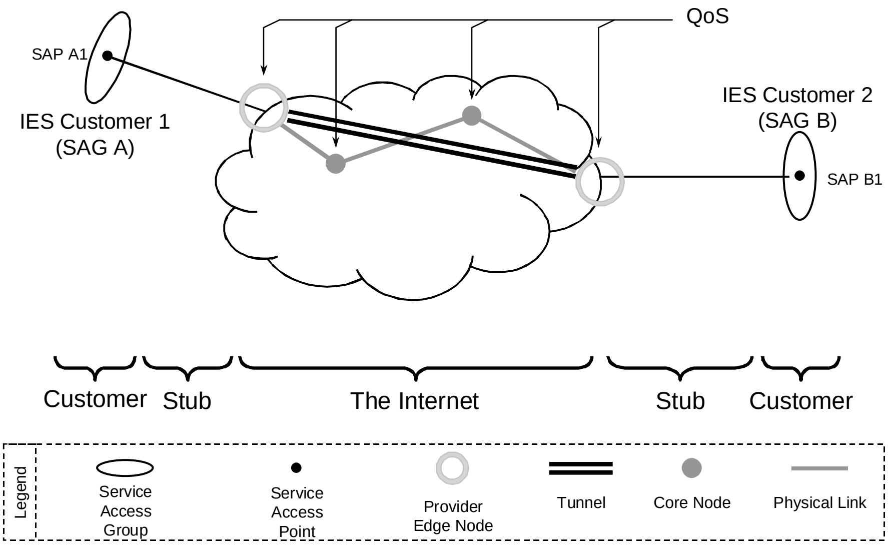


Figure 2 Abstract topology for the VPN connection

The F-VPN test cases consist of three test cases, which can be decomposed into quite a number of sub-test cases covering the interaction between two specific BBs. This is illustrated in the test-case trees below.

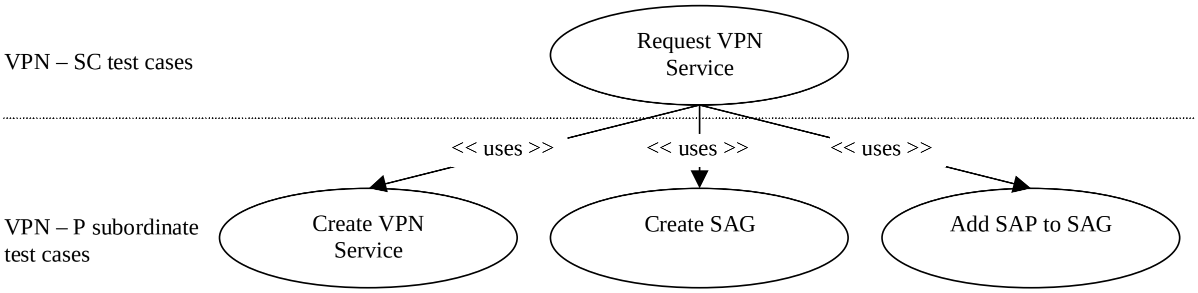


Figure 3 "Request VPN service” test case and its decomposition into subordinate test cases

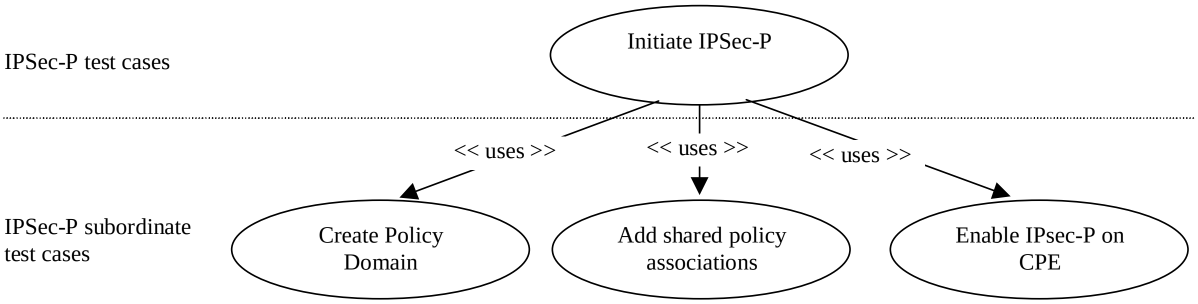


Figure 4 "Initiate IPSec" test case

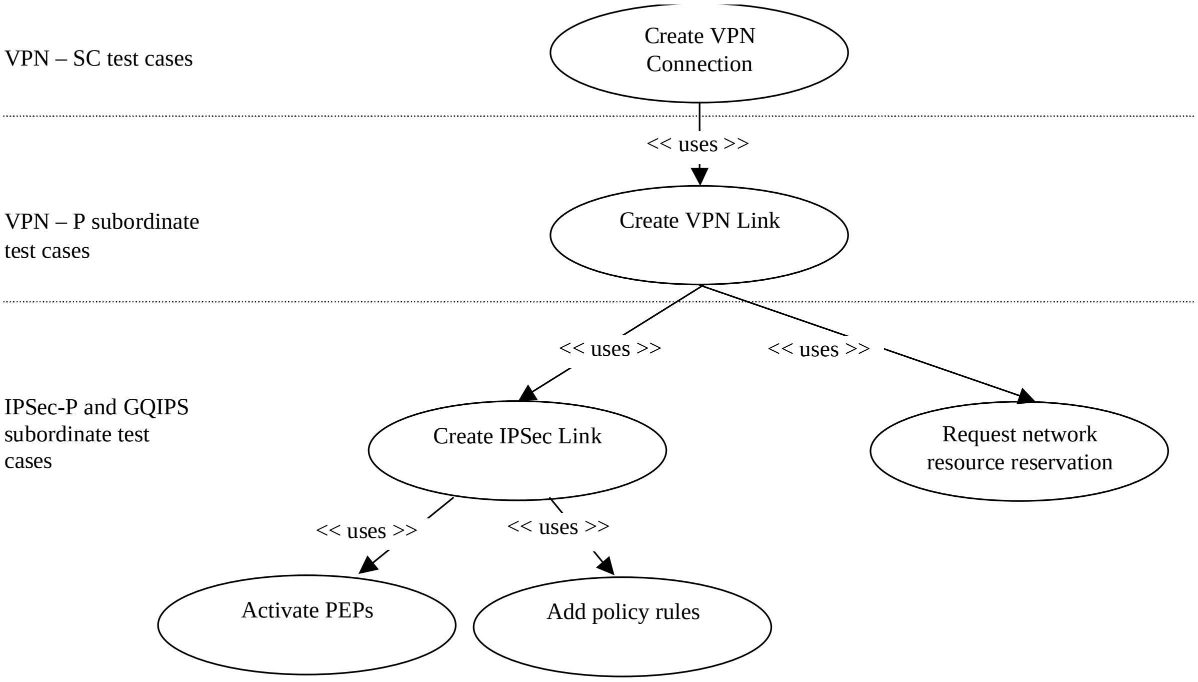


Figure 5 "Create VPN Connection" test case and its decomposition into subordinate test cases

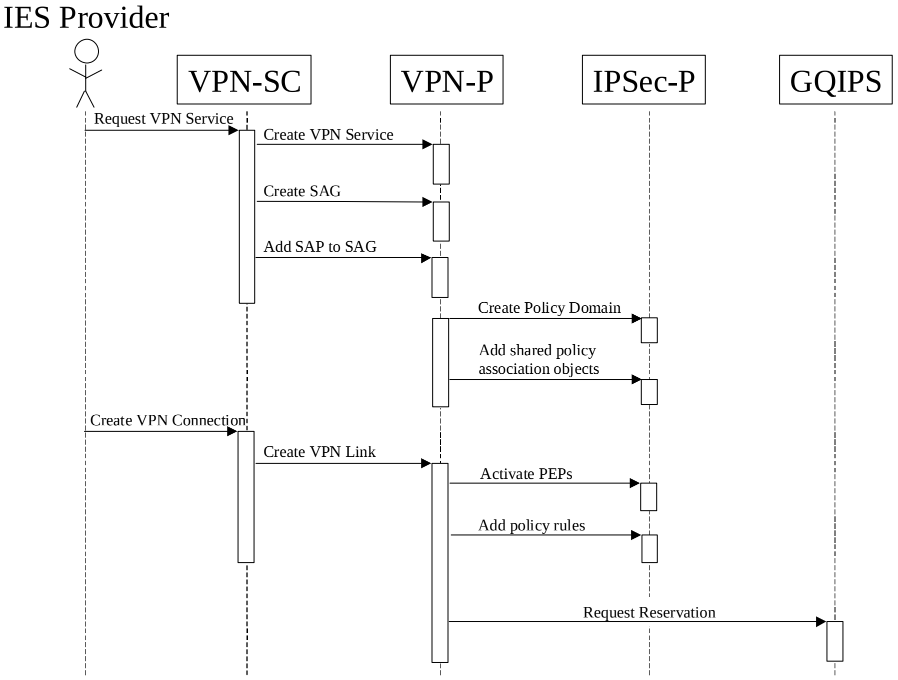


Figure 6 Sequence diagram for all three test cases

All 3 test cases are defined in detail in the following.

2.2.2.1 Test Case 1: "Request VPN Service"

Test Case Identification

Test ID:	T2-TT2-1
Event Type:	Common
Location(s):	Copenhagen, DELTA
Partners involved:	Atos, BRI, DELTA and LMD
Planned Date:	Start December 2001
Trial Planner(s):	F-VPN group
Trial Evaluator(s):	F-VPN group
Developer(s):	Olivier Savoie, Atos Stefan Penter, DELTA Lars Peter Jensen, DELTA Henrik Røn, LMD

Purpose

This test case allows test of the whole interactions necessary for the creation of a VPN Service requested by a VPN Customer.

The test case concerns creation of the entire virtual topology needed for T2-TT2-3: "Create VPN Connection". This test case deals with the creation of the virtual topology for the VPN.

Test Scenario

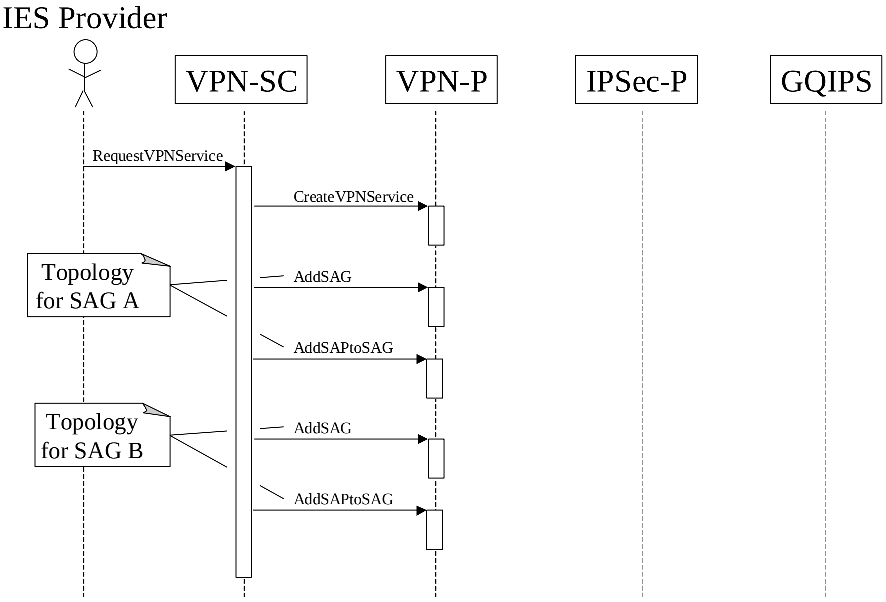


Figure 7 Sequence diagram for "Request VPN Service" test case

Pre-conditions

- Input to VPN-SC: Must be valid according to the XMLSchema located at

  http://www.annecto.dk/annecto/form/lmd.dk/vpn-sc-services.xsd and the **Request_VPN_Service_Argument** tag.

- Pre-conditions for Test Case 1.1, 1.2 and 1.3.

Post-conditions

- Output of VPN-SC: Must be valid according to the XMLSchema located at

  http://www.annecto.dk/annecto/form/lmd.dk/vpn-sc-services.xsd

  and the **Request_VPN_Service_Return_Value** tag.
- Virtual topology created in VPN-SC datamodel.

Test Case Success Criteria

All the sub test cases were successful.

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system http://skinfaxe.delta.dk/reqsys_private

Subordinate Test Cases

Sub-ordinate test cases are T2-TT2-1.1 “Request VPN Service”, T2-TT2-1.2 “Create SAG” and T2-TT2-1.3 “Add SAP to SAG”.

2.2.2.2 Test Case 1.1: “Create VPN Service”

Test Case Identification

Test ID:	T2-TT2-1
Event Type:	Common
Location(s):	Copenhagen, DELTA
Partners involved:	Atos, LMD
Planned Date:	Start December 2001
Trial Planner(s):	F-VPN group
Trial Evaluator(s):	F-VPN group
Developer(s):	Olivier Savoie, Atos Henrik Røn, LMD

Purpose

This sub-ordinate test case is the first part of the T2-TT2-1: “Request VPN Service” test case.

Test Scenario

This test scenario is part of the larger test case depicted in the figure. In more detail it looks like this:

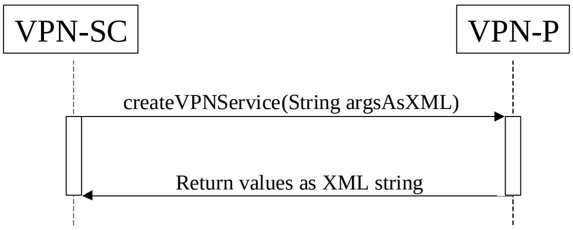

VPN-SC
VPN-P
createVPNService(String argsAsXML)
Return values as XML string

Figure 8 Sequence diagram for test case 1.1

Pre-conditions

- The JBoss server is running.
- VPN-SC and VPN-P have successfully been deployed on the JBoss server.
- The VPN-SC has processed the input from the IES Provider and is ready to call the VPN-P.
- Input to VPN-P: Must be valid according to the XMLSchema located at

  http://www.annecto.dk/annecto/form/atos-origin.fr/vpn-services.xsd

  and the **Create_VPN_Service** tag.

Post-conditions

- The VPN Service object has been created.
- Output of VPN-P: Must be valid according to the XMLSchema located at

  http://www.annecto.dk/annecto/form/atos-origin.fr/vpn-services.xsd

  and the **Create_VPN_Service_Return_Value** tag.

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system http://skinfaxe.delta.dk/reqsys_private

Result	Log media	Success statement	Fail statement
Creation of the VPN Object	VPNP; Flash	VPN created	
Creation of the VPN Object	VPNP; R-console	VPN creation	
Creation of the VPN Object	VPNP; S-console	VirtualTopologyManagerBean.createVPN: VPN created with id *xxxx*	InterfaceException:VirtualTopologyManagerBean.createSAG: + *error*
VPN Service Object created	VPNSC; Flash	VPN-P created VPN service	

2.2.2.3 Test Case 1.2: "Create SAG"

Test Case Identification

Test ID:	T2-TT2-1.2
Event Type:	Common
Location(s):	Copenhagen, DELTA
Partners involved:	Atos, LMD
Planned Date:	Start December 2001
Trial Planner(s):	F-VPN group
Trial Evaluator(s):	F-VPN group
Developer(s):	Olivier Savoie, Atos Henrik Røn, LMD

Purpose

This sub-ordinate test case is the second part of the T2-TT2-1: "Request VPN Service" test case.

Test Scenario

This test scenario is part of the larger test case depicted in the figure. In more detail it looks like this:

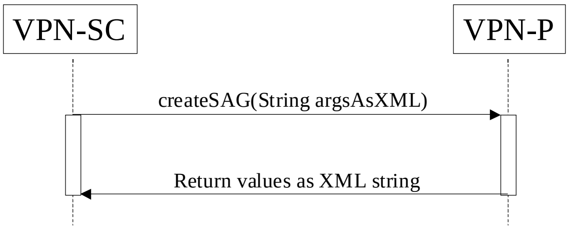


Figure 9 Sequence diagram for test case 1.2

Pre-conditions and test case input

- The test case T2-TT2 1.1 has been executed.
- Test case input: As part of the scenario the "addSAG" is called 2 times.
- Input to VPN-P: Must be valid according to the XMLSchema located at http://www.annecto.dk/annecto/form/atos-origin.fr/vpn-services.xsd and the **Create_SAG** tag.

Post-conditions

- The SAG object has been created.
- Output of VPN-P: Must be valid according to the XMLSchema located at http://www.annecto.dk/annecto/form/atos-origin.fr/vpn-services.xsd and the **Create_SAG_Return_Value** tag.

Test Case Success Criteria

- The two SAGs described in the general scenario have been created.

Result	Log media	Success statement	Fail statement
Creation of the SAG Object	VPNP; Flash	SAG created	
Creation of the SAG Object	VPNP; R-console	SAG creation	
Creation of the SAG Object	VPNP; S-console	VirtualTopologyManagerBean.createSAG: SAG created with id *xxxx*	InterfaceException:VirtualTopologyManagerBean.createSAG: + *error*
SAG object created	VPNSC; Flash	VPN-P created SAG	

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system http://skinfaxe.delta.dk/reqsys_private

2.2.2.4 Test Case 1.3: “Add SAP to SAG”

Test Case Identification

Test ID:	T2-TT2-1.3
Event Type:	Common
Location(s):	Copenhagen, DELTA
Partners involved:	Atos, LMD
Planned Date:	Start December 2001
Trial Planner(s):	F-VPN group
Trial Evaluator(s):	F-VPN group
Developer(s):	Olivier Savoie, Atos Henrik Røn, LMD

Purpose

- This sub-ordinate test case is the third part of the T2-TT2-1 : “Request VPN Service” test case.
- Add one SAP (virtual endpoint) to each SAG created in T2-TT2-1.2. Each SAP is different from one to the other. They represent the two endpoints of the next tunnel.

Test Scenario

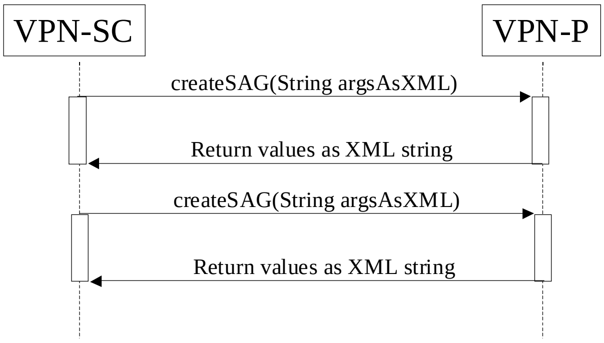

VPN-SC
VPN-P
createSAG(String argsAsXML)
Return values as XML string
createSAG(String argsAsXML)
Return values as XML string

Figure 10 Sequence diagram for test case 1.3

Pre-conditions

- The test case T2-TT2 1.1 has been executed.
- The test case T2-TT2 1.2 has been executed twice.
- Test case input: As part of the scenario the “addSAPToSAG” is called 2 times.

- Input to VPN-P: Must be valid according to the XMLSchema located at

  http://www.annecto.dk/annecto/form/atos-origin.fr/vpn-services.xsd

  and the **Add_SAP_to_SAG** tag.

Post-conditions

- The SAP object has been created.
- The SAP object has been added to the SAG
- Output of VPN-P: Must be valid according to the XMLSchema located at

  http://www.annecto.dk/annecto/form/atos-origin.fr/vpn-services.xsd

  and the **Add_SAP_to_SAG_Return_Value** tag.

Test Case Success Criteria

Result	Log media	Success statement	Fail statement
Creation of the SAP Object	VPNP; Flash	SAP added	
Creation of the SAP Object	VPNP; R-console	SAP addition	
Creation of the SAP Object	VPNP; S-console	VirtualTopologyManagerBean.addSAP: SAP added with id *xxxx*	InterfaceException:VirtualTopologyManagerBean.addSAP: + *error*
SAP added to SAG	VPNSC; Flash	VPN-P created SAP	

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system http://skinfaxe.delta.dk/reqsys_private

2.2.2.5 Test case 2: “Initiate IPSec-P”

Test Case Identification

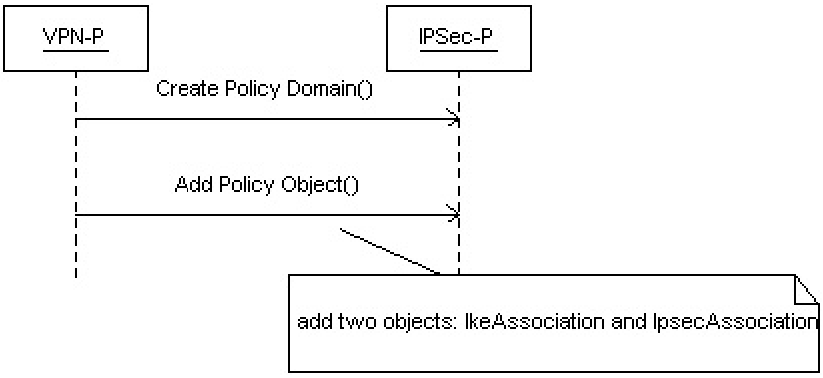
Test ID:	T2-TT2-2
Event Type:	Common
Location(s):	Copenhagen, DELTA
Partners involved:	Atos, DELTA
Planned Date:	Start December 2001
Trial Planner(s):	F-VPN group
Trial Evaluator(s):	F-VPN group
Developer(s):	Olivier Savoie, Atos Stefan Penter, DELTA Lars Peter Jensen, DELTA

Purpose

- Load the IPSec-P repository with IPSec policy associations defining high-level security service.
- Install/deploy IPsec-P on CPEs.

Test Scenario

BBs involved in the test cases are: VPN-P and IPSec-P.



Pre-conditions

- Cf. Pre-conditions for Test Case 2.1, 2.2 and 2.3.

Post-conditions

IPSec-P initialised for interacting with VPN-P.

Test Case Success Criteria

All the sub test cases were successful.

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system http://skinfaxe.delta.dk/reqsys_private

Subordinate Test Cases

- T2-TT2-2.1 “Create Policy Domain”
- T2-TT2-2.2 “Add shared policy associations to the IPSec-P repository”
- T2-TT2-2.3 “Enable IPSec-P on CPEs”

Result	Log media	Success statement	Fail statement
Creation of the policy domain	VPNP; Flash	Policy domain created	
Creation of the policy domain	VPNP; R-console	Policy domain creation	
Creation of the policy domain	VPNP; S-console	TunnelFactoryBean: PolicyDomain created	InterfaceException:VirtualTopologyManagerBean.createVPNLink: + *error*
CREATE Policy Domain	IPSec-P; Flash	CREATE Policy Domain [OK]	FAILED
CREATE Policy Domain	IPSec-P; JMS-log file	BEGIN + END policy domain entries	BEGIN + EXCEPTION policy domain entries

2.2.2.6 Test case 2.1: "Create Policy Domain"

Test Case Identification

Test ID:	T2-TT2-2.1
Event Type:	Common
Location(s):	Copenhagen, DELTA
Partners involved:	Atos, DELTA
Planned Date:	Start December 2001
Trial Planner(s):	F-VPN group
Trial Evaluator(s):	F-VPN group
Developer(s):	Olivier Savoie, Atos Stefan Penter, DELTA Lars Peter Jensen, DELTA

Purpose

- Partitioning of the IPSec-P repository.
- Integration between VPN-P and IPSec-P.

This is subordinate test case of Test Case 2 ("Initiate IPSec-P").

Pre-conditions

- Database server for IPSec-P repository is up and running.
- Tables for IPSec-P repository are created.
- IPSec-P BB shall be deployed on application server.

Post-conditions

- Policy Domain Name is registered in the IPSec-P repository (not implemented).

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system http://skinfaxe.delta.dk/reqsys_private

2.2.2.7 Test case 2.2: “Add shared policy associations to the IPSec-P repository”

Test Case Identification

Test ID:	T2-TT2-2.2
Event Type:	Common
Location(s):	Copenhagen, DELTA
Partners involved:	Atos, DELTA
Planned Date:	Start December 2001
Trial Planner(s):	F-VPN group
Trial Evaluator(s):	F-VPN group
Developer(s):	Olivier Savoie, Atos Stefan Penter, DELTA Lars Peter Jensen, DELTA

Purpose

- Integration between VPN-P and IPSec-P during "Request VPN Service".
- Initiate the IPSec-P repository with objects that maps the high-level link security service(s) requested by the VPN customer to specific IPSec policy parameters.

This is subordinate test case of Test Case 2 (“Initiate IPSec-P”).

Pre-conditions

- Successful execution of subordinate Test Case 2.1 "Create Policy Domain".

Post-conditions

- Ike and ipsec associations are stored in the IPSec-P repository.

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system http://skinfaxe.delta.dk/reqsys_private

Result	Log media	Success statement	Fail statement
Creation of the shared ike association	VPNP; Flash	IkeAssociation created	
Creation of the shared ike association	VPNP; R-console	IkeAssociation creation	
Creation of the shared ike association	VPNP; S-console	TunnelFactoryBean: ike Association created	InterfaceException:VirtualTopologyManagerBean.createVPNLink: + *error*
Creation of the shared ipsec association	VPNP; Flash	ipsec Association created	
Creation of the shared ipsec association	VPNP; R-console	ipsec Association creation	
Creation of the shared ipsec association	VPNP; S-console	TunnelFactoryBean: ipsec Association created	InterfaceException:VirtualTopologyManagerBean.createVPNLink: + *error*
ADD ike-association	IPSec-P; Flash	ADD ike-association [OK]	ADD ike-association FAILED
ADD ike-association	IPSec-P; JMS-log file	BEGIN + END ike-association entries	BEGIN + EXCEPTION ike-association entries

2.2.2.8 Test case 2.3: “Enable IPSec-P on CPEs”

Test Case Identification

Test ID:	T2-TT2-2.3
Event Type:	Common
Location(s):	Copenhagen, DELTA
Partners involved:	DELTA
Planned Date:	Start December 2001
Trial Planner(s):	F-VPN group
Trial Evaluator(s):	F-VPN group
Developer(s):	Stefan Penter, DELTA Lars Peter Jensen, DELTA

Purpose

- Allow CPEs to be configured by IPSec-P in Test Case 3.2 "Create IPSec Link".
- Start proxy software on CPEs in order to simulate IPSec policy enabled CPEs.

Pre-conditions

- Database server for IPSec-P repository is up and running.
- Tables for IPSec-P repository are created.

Post-conditions

- CPEs checks the IPSec-P repository for possible activation every 10 seconds.
- CPEs activates changes made to IPSec policies.

Test Case Success Criteria

Execution of Test Case 3 ends successfully.

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system http://skinfaxe.delta.dk/reqsys_private

2.2.2.9 Test case 3: "Create VPN Connection"

Test Case Identification

Test ID:	T2-TT2-3
Event Type:	Common
Location(s):	Copenhagen, DELTA
Partners involved:	Atos, BRI, DELTA and LMD
Planned Date:	Start December 2001
Trial Planner(s):	F-VPN group
Trial Evaluator(s):	F-VPN group
Developer(s):	Olivier Savoie, Atos Stefan Penter, DELTA Lars Peter Jensen, DELTA Henrik Røn, LMD

Purpose

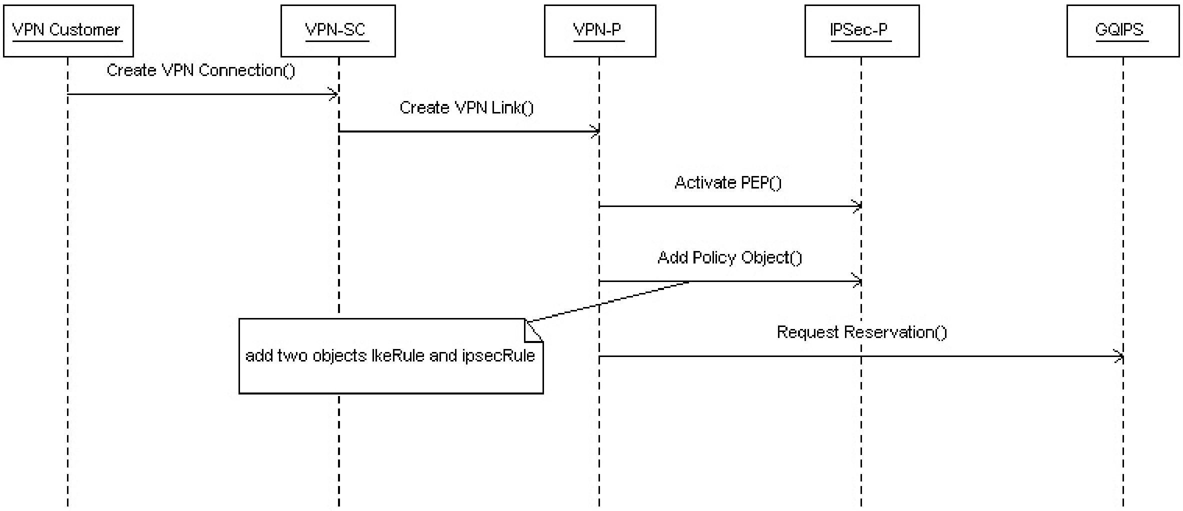
This test case allows test of the whole interactions necessary for the creation of a VPN connection requested by a VPN Customer.

Test Case Success Criteria

- All the sub test cases were successful.

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system http://skinfaxe.delta.dk/reqsys_private



Pre-conditions

The following is a prerequisite for running the test.

- Test cases T2-TT2-1 “Request VPN Service” and T2-TT2-2 “Initiate IPSec-P” have been executed successfully.
- VPN-P: Topology of the border nodes has been configured.
- IPSec-P: IPSec policy associations have been stored in the IPSec-P repository.
- The CPH test-bed and the JBoss server is running.
- VPN-SC, VPN-P and GQIPS have successfully been deployed on the JBoss server.
- Input to VPN-SC: Must be valid according to the XMLSchema located at

  http://www.annecto.dk/annecto/form/lmd.dk/vpn-sc-services.xsd

  and the **Create_VPN_Connection_Argument** tag.

Post-conditions

- Objects created at the VPN-SC: VPN Connection.
- Objects created at the VPN-P: VPNLink
- IPSec-P: An IPSec link between two CPEs is established.
- Output of VPN-SC: Must be valid according to the XMLSchema located at

  http://www.annecto.dk/annecto/form/lmd.dk/vpn-sc-services.xsd

  and the Create_VPN_Connection_Return_Value tag.

Subordinate Test Cases

• T2-TT2-3.1	“Create VPN Link (VPN-SC – VPN-P)”
• T2-TT2-3.2	“Create IPSec Link”
• T2-TT2-3.2.1	“Activate PEPs”
• T2-TT2-3.2 2	“Add policy rules to the IPSec-P repository”
• T2-TT2-3.3	“Create VPN Connection (VPN-P – GQIPS)”

2.2.2.10 Test case 3.1: “Create VPN Link (VPN-SC – VPN-P)”

Test Case Identification

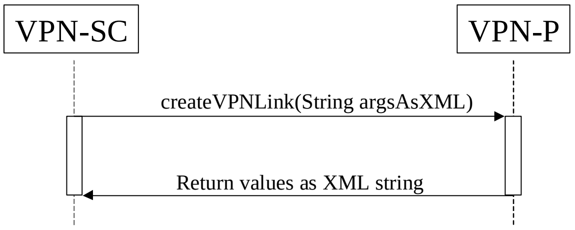
Test ID:	T2-TT2-3.1
Event Type:	Common
Location(s):	Copenhagen, DELTA
Partners involved:	Atos, LMD
Planned Date:	Start December 2001
Trial Planner(s):	F-VPN group
Trial Evaluator(s):	F-VPN group
Developer(s):	Olivier Savoie, Atos Henrik Røn, LMD

Purpose

This test case allows test of interactions between VPN-SC and VPN-P during the Create VPN Connection.

Test Scenario

This test scenario is a sub-test case of T2-TT2-3: “Create VPN Connection” depicted in the figure and the BBs involved in the test cases are: VPN-SC and VPN-P. The sequence diagram:



Pre-conditions

- T2-TT2-1 “Request VPN Service” and T2-TT2-2 “Initiate IPSec-P” have been carried out successfully.
- The Topology has been configured manually in the VPN-P.

Post-conditions

Objects created at the VPN-SC: VPN Connection

Objects created at the VPN-P: VPNLink

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system http://skinfaxe.delta.dk/reqsys_private

Result	Log media	Success statement	Fail statement
Creation of the VPNLink Object	VPNP; Flash	VPNLink created	
Creation of the VPNLink Object	VPNP; R-console	VPNLink creation	
Creation of the VPNLink Object	VPNP; S-console	VirtualTopologyManagerBean.createVPNLink: VPNLink created	InterfaceException:VirtualTopologyManagerBean.createVPNLink: + *error*
VPN connection object created	VPNSC; Flash	VPN-P activated VPN connection	

2.2.2.11 Test case 3.2: “Create IPSec Link”

Test Case Identification

Test ID:	T2-TT2-3.2
Event Type:	Common
Location(s):	Copenhagen, DELTA
Partners involved:	Atos, DELTA
Planned Date:	Start December 2001
Trial Planner(s):	F-VPN group
Trial Evaluator(s):	F-VPN group
Developer(s):	Olivier Savoie, Atos Stefan Penter, DELTA Lars Peter Jensen, DELTA

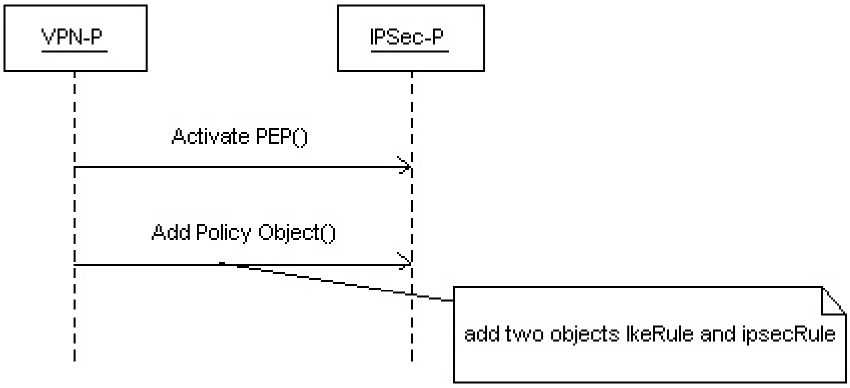
Purpose

- This test case allows test of interactions between VPN-P and IPSec-P during the Create VPN Connection.

This is a subordinate test case of TC 3 (“Create VPN Connection”).

Test Scenario

BBs involved in the test cases are: VPN Customer, VPN-P, IPSec-P.



Pre-conditions

- Test case 1 and 2 and 3.1 have been executed successfully.
- VPN-P: Topology of the border nodes has been configured.

Post-conditions

The IPSec Link is established.

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system http://skinfaxe.delta.dk/reqsys_private

Subordinate Test Cases

- T2-TT2-3.2.1 "Activate PEPs "
- T2-TT2-3.2.2 "Add policy rules to the IPSec-P repository"

Result	Log media	Success statement	Fail statement
Creation of the IPSEC Tunnel	VPNP; Flash	IPSEC tunnel created	
Creation of the IPSEC Tunnel	VPNP; R-console	IPSEC tunnel creation	
Creation of the IPSEC Tunnel	VPNP; S-console	TunnelFactory: ipsecTunnel created	InterfaceException:VirtualTopologyManagerBean.createVPNLink: + *error*
IPSec Link established	IPSec-P; Flash	Link shown as shielded. IP proto field in packet header changes from 0x06 (TCP) to 0x32 (IPSec)	Link stays unshielded. IP proto field in packet header changes does not change from 0x06 (TCP)

2.2.2.12 Test case 3.2.1: "Activate PEPs"

Test Case Identification

Test ID:	T2-TT2-3.2.1
Event Type:	Common
Location(s):	Copenhagen, DELTA
Partners involved:	Atos, DELTA
Planned Date:	Start December 2001
Trial Planner(s):	F-VPN group
Trial Evaluator(s):	F-VPN group
Developer(s):	Olivier Savoie, Atos Stefan Penter, DELTA Lars Peter Jensen, DELTA

Purpose

- Integration between VPN-P and IPSec-P.
- Store IP address and roles of PEPs in the IPSec-P repository "pushing" the changes to CPEs.
- Activate PEPs located on CPEs.

This is a subordinate test case of TC 3.2 ("Create IPSec Link").

Pre-conditions

- Database server for IPSec-P repository is up and running.
- Tables for IPSec-P repository are created.
- IPSec-P BB shall be deployed on application server.

Post-condition

- PEP IPSec roles are cached in the PEP.
- PEPs checks the IPSec-P repository for changes related to themselves.

Test Case Success Criteria

Result	Log media	Success statement	Fail statement
Activate PEP	VPNP; Flash	PEP activated	
ACTIVATE pep	IPSec-P; Flash	ACTIVATE pep [OK]	ACTIVATE pep FAILED
ACTIVATE pep	IPSec-P; JMS-log file	BEGIN + END pep entries	BEGIN + EXCEPTION pep entries

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system http://skinfaxe.delta.dk/reqsys_private

2.2.2.13 Test case 3.2.2: "Add policy rules to the IPSec-P repository"

Test Case Identification

Test ID:	T2-TT2-3.2.2
Event Type:	Common
Location(s):	Copenhagen, DELTA
Partners involved:	Atos, DELTA
Planned Date:	Start December 2001
Trial Planner(s):	F-VPN group
Trial Evaluator(s):	F-VPN group
Developer(s):	Olivier Savoie, Atos Stefan Penter, DELTA Lars Peter Jensen, DELTA

Purpose

- Integration between VPN-P and IPSec-P.
- Add policy rules to the IPSec-P repository for border notes (CPEs)
- Establish the basis for creation of an IPSec secured link between two CPEs.

This is subordinate test case of Test Case 3.2 ("Create IPSec Link").

Pre-conditions

- Cf. Pre-conditions for Test Case 3.2.1.

Post-condition

- Ike and IPSec policy rules stored in the IPSec-P repository.

Test Case Success Criteria

Result	Log media	Success statement	Fail statement
Add IKE rule	VPNP; Flash	IKE rule added	
Add IPSECrule	VPNP; Flash	IPSEC rule added	
ADD ike-rule	IPSec-P; Flash	ADD ike-rule [OK]	ADD ike-rule FAILED
ADD ike-rule	IPSec-P; JMS-log file	BEGIN + END ike-rule entries	BEGIN + EXCEPTION ike-rule entries
ADD ipsec-rule	IPSec-P; Flash	ADD ipsec-rule [OK]	ADD ipsec-rule FAILED
ADD ipsec-rule	IPSec-P; JMS-log file	BEGIN + END ipsec-rule entries	BEGIN + EXCEPTION ipsec-rule entries

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system http://skinfaxe.delta.dk/reqsys_private

2.2.2.14 Test case 3.3: "Request network resource reservation (VPN-P – GQIPS)"

Test Case Identification

Test ID:	T2-TT2-3.2.3
Event Type:	Common
Location(s):	Copenhagen, DELTA
Partners involved:	Atos, BRI
Planned Date:	Start December 2001
Trial Planner(s):	F-VPN group
Trial Evaluator(s):	F-VPN group
Developer(s):	Olivier Savoie, Atos Vincent Alexandre, BRI

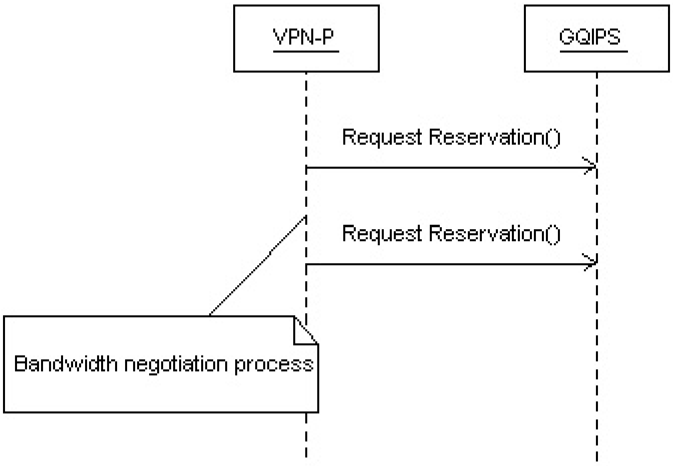
Purpose

This test case allows to test interactions between VPN-P and GQIPS during the Create VPN Connection. This test case could include bandwidth negotiation process between VPN-P and GQIPS.

This is sub-test case of TC 3 ("Create VPN Connection").

Test Scenario

BBs involved in the test cases are: VPN-P, GQIPS.



Pre-conditions

- Test case 1 and 2 and 3.1 have been executed successfully.
- VPN-P: Topology of the border nodes has been configured.
- Input to GQIPS: Must be valid according to the XMLSchema located at

  http://www.cs.ucl.ac.uk/research/form/models/ContractCatalogue/broadcom.ie/FORM/ResourceAllocationManager/Contract.xml

Post-condition

- Output of GQIPS: Must be valid according to the XMLSchema located at

http://www.cs.ucl.ac.uk/research/form/models/ContractCatalogue/broadcom.ie/FORM/ResourceAllocationManager/Contract.xml

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system http://skinfaxe.delta.dk/reqsys_private

Result	Log media	Success statement	Fail statement
Reservation accepted	GQIPS; Flash	SLA Accepted	
Reservation accepted	GQIPS; S-Console	<SLA>Accepted</SLA>	
Reservation accepted	GQIPS; File	<SLA>Accepted</SLA>	

2.2.3 Test Team 2 Conclusions

Match Findings/Results with Purpose

As part of Trial 2, Test Team (TT2) conducted *integration* and *basic functionality* tests of the three developed VPNS building blocks. A fourth BB - the GQIPS BB - was integrated in simulated mode to support the overall creation of a VPN service with security and bandwidth QoS. The test encompassed three main test cases and 10 subordinate cases. Only mappings to Operational Requirements where specified for the main test cases.

The purpose of Trial 2 for TT2 was thus twofold:

- Integration of BBs from four FORM partners.
- Test of basic BB functionality for creation of a VPN Service, containing the virtual topology, and activation of the VPN connection between two endpoints in the virtual topology.

Initial integration was done and demonstrated at the M3 review in a distributed environment and all test cases were conducted successfully in Copenhagen in December 2002, where the four building blocks from four partners were integrated.

The main problems encountered during integration were of the following nature:

- *Agreeing on naming*:
  Each of the participating EJBs has a number of configuration and deployment files, which describe JNDI names of the EJB, which plug-ins to use, etc.
- *Agreeing on location of naming server*:
  The EJB's client locates the EJB using a JNDI naming server. The location (IP address and port) of the naming server must also be agreed.

- *The classpath environment variable* on the machine on which the JBoss server is running must be set-up correctly to avoid shadowing problems, i.e. that jar file A implements a certain interface and jar file B also implements the same interface. If the EJB wants to use the implementation in jar A, but if jar B is first in the classpath.
- Minor problems were also encountered in the complicated test bed regarding some of the test-tools for visualisation.

We consider therefore that most integration problems have been related to configuration of EJB server platform. It is also important to note that only one EJB server platform (JBoss) as been used by all partners. This fact certainly avoids platform interoperability problems.

However we estimate that correction of the integration problems encountered required less resources that would have been used if we had developed the functionality using a non component-based technology, e.g. C++. The J2EE platform delivers a number of services. Using a non component-based technology would have force us to agree on which third party libraries to use for each of the services or develop them ourselves. We did not encounter any problems, which needed further investigation, but the tests conducted were focused on a normal-path through the system and further testing would require examination of error-paths.

One main factor for successful integration in projects where components are developed by geographically distributed partners from different organisations is well-defined interfaces. Building Blocks and contracts have been developed in respect of the development methodology proposed by the ODF, which supports ODF principles. Therefore, main conclusion regarding integration process and use of ODF is that integration of complex component based system can be eased using well-adapted methodology.

In the same way the development methodology supports a top down approach allowing integration of user requirement at the beginning of the development process. Trial 2 allowed to validate user requirements, captured at beginning of the project, have been fulfilled by developed Building Blocks and corresponding integrated system.

Requirements Impact

Of the originally collected requirements only few were specific to VPN, many functionally addressed a generic Inter Enterprise Service concerning outsourcing, security or establishment. The requirements were very broad and basic such as dynamic establishment of service, dynamic modifiability of service, etc. Main reason is that the project started from a very broad vision of Inter-Enterprise service to be supported by an IESP.

The system design of the Trial 2 system and the BBs within the Trial 2 system was based on concepts and ideas from standards: from ITU-T [M.3108.1], [M.3108.3], [M.3208.1], [M.3208.3]), IETF [IPSec Configuration], [IPSec Policy]) and the QBone ([Internet2 QBone]) initiative. During the analysis-phase the requirements served as guidance on the functional level, whereas in the design and implementation phases strict adherence to requirements was not prioritised.

The planned test cases for Trial 2 dealt with the most basic VPN functionality as integration had focus, and it was needed, to enable testing of the functionality in the individual EJBs. However this simple functionality designed and partially implemented for Trial 2 was traced back - using the web-tool - to many of the original requirements of which a large number were addressed.

Anyway, operational requirements, as defined initially, allowed assessment of provision and activation of service in a B2B context.

2.3 Test Team 3 – Assurance

2.3.1 Trial Planning

2.3.1.1 Trial Objective

The purpose of Trial 2 is to demonstrate and evaluate the prototype assurance system's support for the overall assurance scenario. In this scenario an SLA is submitted to the assurance system for support. The system is then configured based on the metrics contained within the SLA before finally monitoring of the service, at both the server and network level, begins. While the service is being monitored it is possible for the customer to request SLA conformance reports from the assurance system to asses the quality of the service they are receiving.

As part of Trial 2 the following aspects of the assurance system will be tested and evaluated.

<u>Bandwidth Brokerage</u>

The purpose of the Bandwidth Broker is to allow the negotiation and reservation of guaranteed bandwidth for a point-to-point link that may span several different domains. For Trial2 it is proposed to test the deployment of a number of Bandwidth Brokers on a real test bed as well as the support provided for router access and QoS configuration.

<u>Service Assurance</u>

The purpose of the service assurance system is the configuration and operation of distributed management components that monitor the performance of a network based service as a whole through statistical aggregation. The main focus for Trial 2 is testing policy creation for system configuration and ensuring that the system functions correctly when provided with this configuration.

<u>Customer Reporting</u>

The purpose of the customer reporting system is the reporting of service statistics generated by the assurance system to customers in various different formats. For Trial2 a number different features of the customer reporting prototype will be tested including the following:

- <u>Automatic</u> creation of reports.
- Automatic translation of reports into <u>any</u> mark-up language e.g. HTML, WML or XHTML.
- <u>Secure</u> customisation of reports.

<u>Workflow Framework</u>

The purpose of the workflow framework is to provide support for assurance business process implementation by integrating the assurance BBs in a flexible way. For Trial2 the main feature that is to be tested is the implementation of data flow that enables the passing of parameters between the Building Blocks

2.3.1.2 Trial Plan

Test Case ID	Name	Partner(s)	Planned
T2-TT3-1.1	Customer Login and Validation	TDC	T2
T2-TT3-1.2	Reporting Template Completition	TDC	T2
T2-TT3-1.3	Report Translation Configuration	TDC	Before M3
T2-TT3-2.1	Production of Assurance Configurations	TCD	T2, Week 50 2001, Broadcom Dublin

T2-TT3-2.2	Service Monitoring	TCD	T2, Week 50 2001, Broadcom Dublin
T2-TT3-2.3	Service Violation Reporting	TCD	T2, Week 50 2001, Broadcom Dublin
T2-TT3-2.4	Workflow implementation of Assurance Business Processes	TCD	T2, Week 50 2001, Broadcom Dublin
T2-TT3-3.1	B3 Setting	BRI	T2, Week 50 2001, Broadcom Dublin
T2-TT3-3.2	Single domain service negotiation	BRI	T2, Week 50 2001, Broadcom Dublin
T2-TT3-3.3	Events subscription and notification	BRI	T2, Week 50 2001, Broadcom Dublin
T2-TT3-3.4	Multi domain RAR Negotiation	BRI	T2, Week 50 2001, Broadcom Dublin

2.3.1.3 What is Tried/Tested

Building Block(s) (BBs)

BB	Version	Provider	Comments
CRA	0.01	TDC	Current version is implemented as one web-application on one web-server. The idea of having two BBs connected by a Web-Service (XML/HTML) has not yet been implemented.
GQIPS	0.01	BRI	With ResourceAllocationManager contract.
Assurance Configurator	0.1	TCD	Supports the AssuranceService and AssuranceConfiguration contracts.
Server Monitor	0.1	TCD	Supports the ServiceMonitor contract.
Performance Monitor	0.1	TCD	Supports the PerformanceMonitor contract.

Contract(s)

Contract	Ver.	Specification URI	RP	Description
Customer Reporting Service	0.1	http://www.cs.ucl.ac.uk/research/form/models/ContractCatalogue/tdc.dk/FORM/CustomerReportingService/TDC_CRS_BBC_v1.xml	IES-CM	This contract offers a Web-based service which enable a customer to login as service user and use the web service to request selected data to be displayed on his browser or saved in a file.
XML Document Generator	xx	http://www.cs.ucl.ac.uk/research/form/models/ContractCatalogue/tdc.dk/FORM/XMLDocumentGen	internal/ Third-party SP-PM	This contract offers a Webservice which enable a SOAP client to request a SQL Query to a database, and have the result formatted as an XML document. (not implemented)

		erator/TDC_XDG_BBC_v1.xml		
Resource Allocation Manager	0.01	http://www.cs.ucl.ac.uk/research/form/models/ContractCatalogue/broadcom.ie/FORM/ResourceAllocationManager/Contract.xml	GQIPS-PM	The ResourceAllocationManager contract provides management services related to the negotiation, or renegotiation, of a bandwidth brokered SLA. The contract is intended to be used by a service user, with particular Quality of Service needs in terms of bandwidth, delay and jitter
Assurance Service	1.0	http://www.cs.ucl.ac.uk/research/form/models/ContractCatalogue/fokus.fhg.de/FORM/SLAHandlingService/Contract.xml	IES-CM / Internal	This contract provides the operational interface to a Assurance service. This contract serves two main functions. The first is to allow services that the system is to support to be registered and the second is to allow SLAs to be introduced or removed.
Assurance Configuration	1.0	http://www.cs.ucl.ac.uk/research/form/models/ContractCatalogue/cs.tcd.ie/FORM/AssuranceConfiguration/Contract.xml	IES-CM / Internal	The purpose of this contract is to allow access to CIM policies that are used to configure the distributed managment components.
Server Monitor	1.0	http://www.cs.ucl.ac.uk/research/form/models/ContractCatalogue/cs.ucl.ac.uk/FORM/SlaNegReq/Contract.xml	Internal	This contract allows access to the CIM information base stored in the Server Monitor building block. This building block monitors server statistics, calculating secondary combinatory statistics when necessary.
Performance Monitor	1.0	http://www.cs.ucl.ac.uk/research/form/models/ContractCatalogue/uhc.dk/FORM/SLARepository/Contract.xml	Internal	This contract has a dual purpose. The first is to allow the statistics collected by the Performance Monitor to be accessed. The second is to allow policies to be downloaded through the contract to specify which statistics to collect and calculate.

Other

Software	Version	Provider	Comments
Workflow framework	v 2	TCD	

2.3.1.4 Test Environment

Hardware Environment

Product	Version	Used By	Provider	Comments

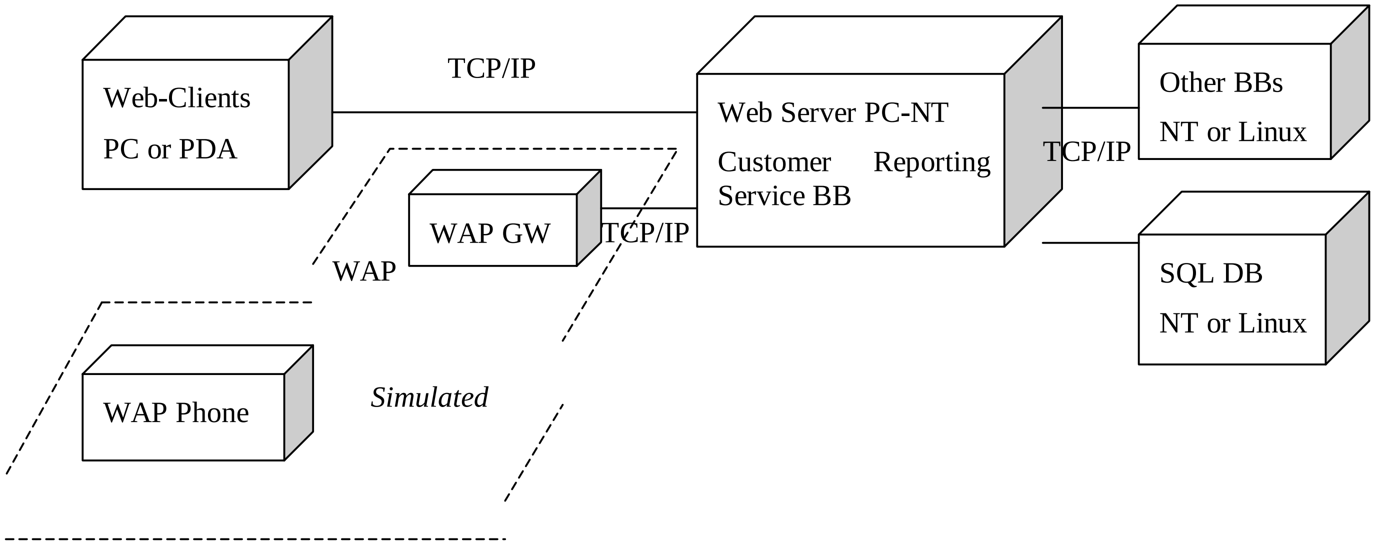
PC	P 100	TDC	ICL	32 Mb (Slow)
PC	P II 800	TDC	ZITECH	128 Mb (Faster)
Server	Pro-liant	TDC	Compaq/TDC Mobile	Quite fast
1 PC (>266 MHz)*, 128 Mb RAM		BRI		Run a first Orion Application Server (BRI side) to deploy a first BBr
1 PC (>266 MHz)*, 128 Mb RAM		BRI		Run a second Orion Application Server (BRI side), to deploy a second BBr
Windows2000 PC		TCD	DELL Desktop	Workflow framework
Windows2000 PC		TCD	Artist Laptop	Assurance Configurator
Windows NT4 PC		TCD	Hyundai Laptop	Server Monitor

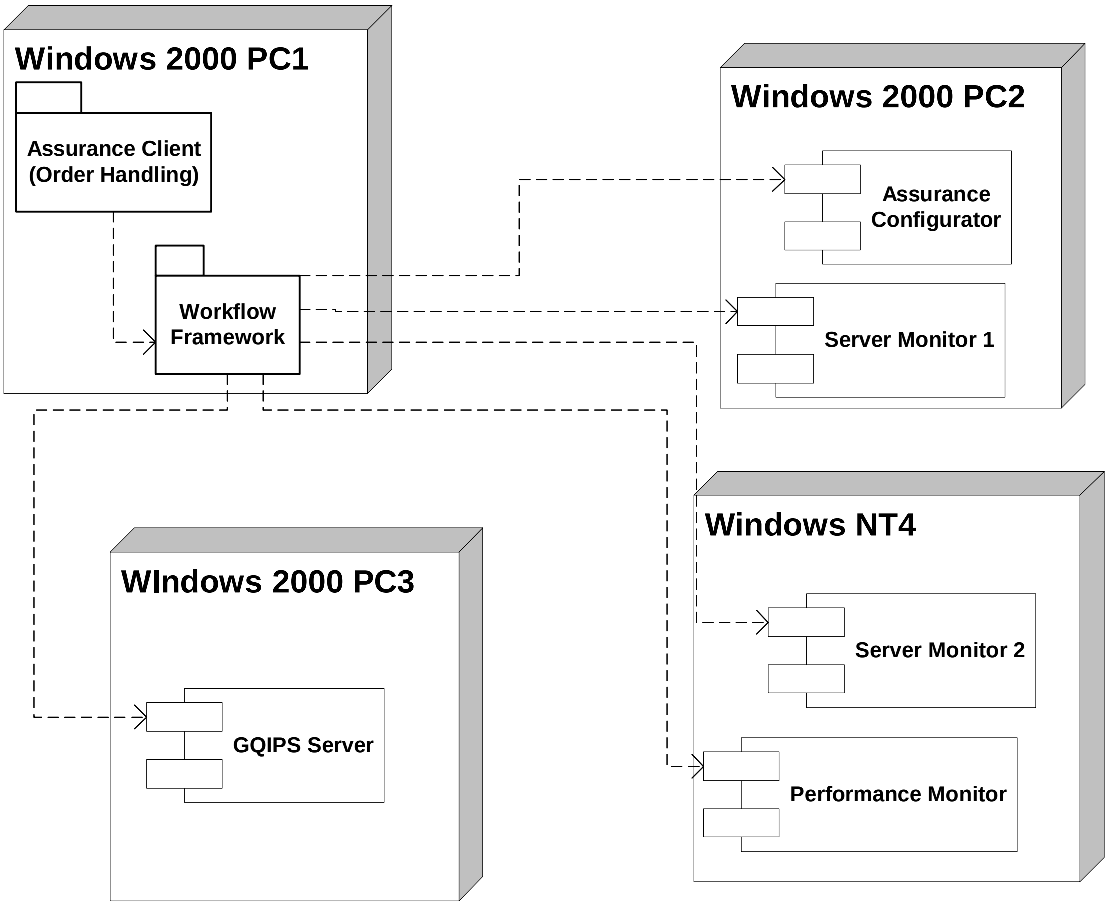
Software Environment

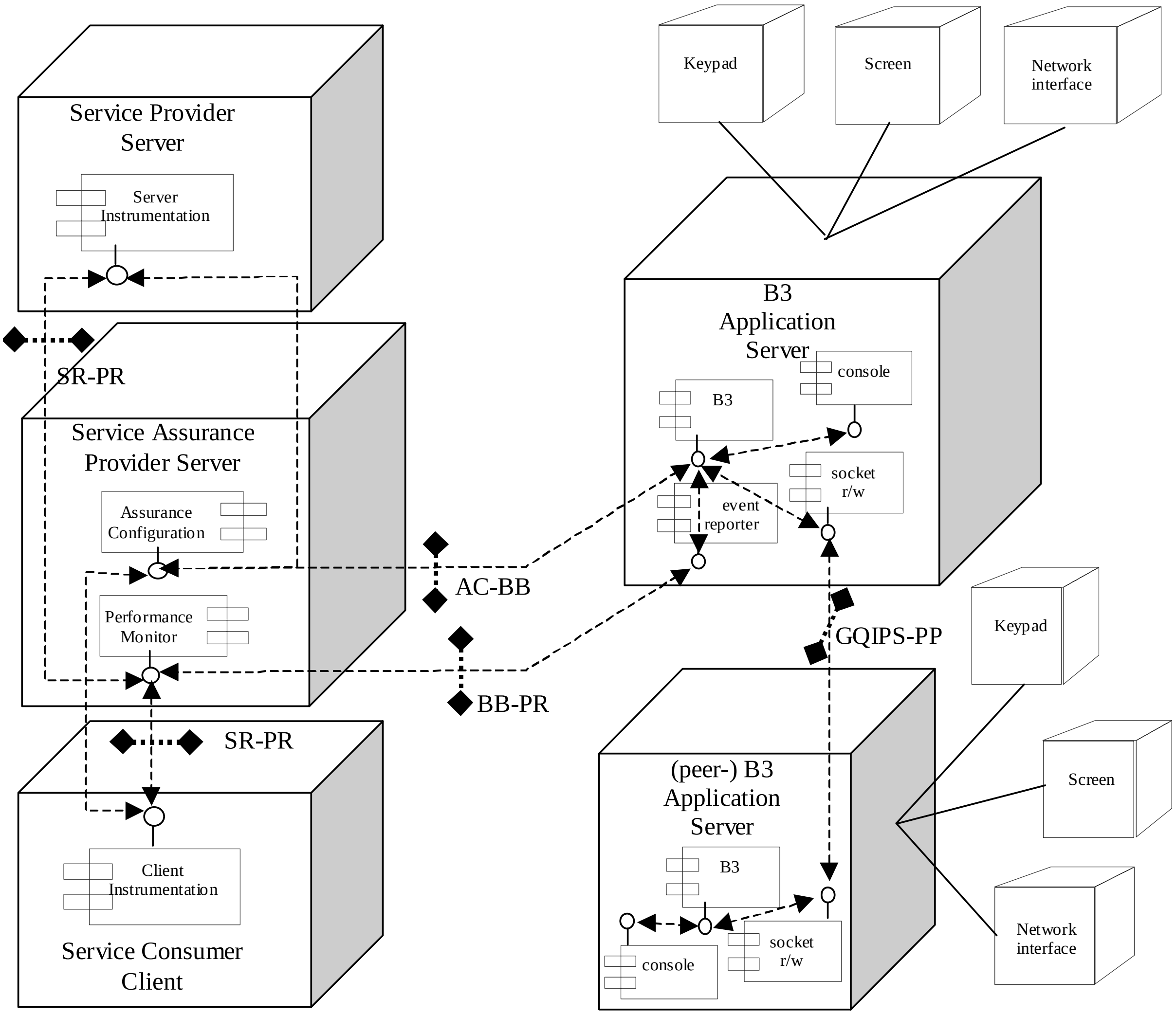
Product	Version	Used By	Provider	Comments
J2SDK	1.3.1	TDC/BRI/TCD	www.sun.com	Open source
Tomcat	4.0	TDC	www.apache.org	Open source
Xalan	2.0	TDC	www.apache.org	Open source
JDOM	Beta-7	TDC	www.jdom.org	Open source
WAPToolkit	3.0	TDC	www.nokia.com	Open source
NT / Win 2K	4.0 / ?	TDC/BRI/TCD	www.microsoft.com	
MS IE	5.0 or higher	TDC	www.microsoft.com	With versions below 6.0 user must install SVG viewer.
SVG Viewer	2.0 or higher	TDC	www.adobe.com	Plug-in (see above)
J2EE, Java 2 Enterprise Edition	1.2.1	BRI/TCD	http://java.sun.com/j2ee	Relies on J2SE v1.3
Orion Application Server	1.3.8	BRI	http://www.orionserver.com	Implements some J2EE 2.0 features
Xerces Java Parser	1.2.3	BRI/TCD	http://xml.apache.org/xerces-j/index.html	A Java API to parse/format XML documents
Gizma SDK	1.1	BRI	http://gizma.go.to	A Java API with

				some useful packages and graphical components
Jboss	2.4.1a	TCD	Jboss	
Orbix 2000		TCD	Iona	
CIM Server		TCD	SNIA	

Deployment Diagram




Windows 2000 PC1
Assurance Client (Order Handling)
Workflow Framework
Windows 2000 PC2
Assurance Configurator
Server Monitor 1
Windows NT4
Server Monitor 2
Performance Monitor
WIndows 2000 PC3
GQIPS Server



Assurance Deployment Diagram

2.3.2 Test Cases

2.3.2.1 Test Case 1.1: "Customer Login and Validation"

Test Case Identification

Test ID:	T2-TT3-1.1	Customer Login and Validation
Event Type:	Common	
Location(s):	Copenhagen/DELTA	
Partners involved:	TDC	
Planned Date:	Start December	
Trial Planner(s):	Assurance Group	
Trial Evaluator(s):	Assurance Group	
Developer(s):	Catherine Goret Nielsen TDC Jens Dyhre Mouritzsen TDC	

Purpose

The selected web programming techniques must enable generation of dynamic client web-pages, where the information and menu options are generated dynamically based on customer ID.

The web application should enable dynamic retrieval of customer specific information both locally and external i.e. from other management -systems or –components.

The web application should enable that information regarding individual customers or customer types are stored in the XML format and are handled with ‘open source’ XML tools by the web application.

The web application must be able to identify the customer client browser during a session and secure that information generated or exchanged during a session will not be seen by be available to other sessions i.e. customers.

The web application must be able to identify the customer client browser type e.g. WAP phone and select type specific templates and information.

Pre-conditions

Customer specific information are formatted in XML and made available to the web application. This includes the name used for login to the web service the password to be used for a name and the templates and filters to be used to generate dynamically the customers menu option web pages.

Post-conditions

If the customer makes a login from a normal web browser, the web application will dynamically generate an HTML page with customer specific information and menu options.

If the customer makes a login from a browser supporting the Wireless Application Protocol (WAP), the web application will dynamically generate a WML or XHTML page with customer specific information and menu options.

Test Case Success Criteria

- Wrong user names and or passwords are detected and error messages are shown on the login page.

- Dynamically generation of menu pages using the latest web programming techniques must be faster than using 'old style' CGI programming.
- When a user makes a correct login he receives a menu page which is not just customer specific but also specific for the type of browser used by the customer.

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system (http://skinfaxe.delta.dk/reqsys_public)

Test Scenario

1. Customer login from Client browser.
2. Customer is validated by Web Server.
3. Web Server returns customer specific and browser specific page with menu options.

2.3.2.2 Test Case 1.2: "Reporting Template Completition"

Test Case Identification

Test ID:	T2-TT3-1.2	Reporting Template Completition
Event Type:	Common	
Location(s):	Copenhagen/DELTA	
Partners involved:	TDC	
Planned Date:	Start December	
Trial Planner(s):	Assurance Group	
Trial Evaluator(s):	Assurance Group	
Developer(s):	Catherine Goret Nielsen TDC Jens Dyhre Mouritzsen TDC	

Purpose

Use customer id and customer menu selections to collect reporting data to fill out a customer specific reporting template with 'dynamic' data.

Pre-conditions

Customer specific information are formatted in XML and made available to the web application. This includes the templates, filters and XML style-sheets to be used to generate dynamically the customers report pages.

Post-conditions

If the customer uses a normal web browser, the web application will dynamically generate an HTML page with customer specific -information and -report data and -graphics.

If the customer uses a browser supporting the Wireless Application Protocol (WAP), the web application will dynamically generate a WML or XHTML page with customer specific -information and -report data but no graphics.

Test Case Success Criteria

- Missing input from customer's e.g. menu selections are detected and error messages are shown on the menu page.
- Dynamically generation of report pages using the latest web programming techniques must be faster than using 'old style' CGI programming.
- When a user provide valid input/selections on the menu pages the customer will receive a report page where the out-line and presentation of the report is based on selected template and style-sheets, and the content of the report is based on selected filters.

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system (http://skinfaxe.delta.dk/reqsys_public)

Test Scenario

1. Customer provide menu input and selections and submit a request to the web application.
2. The web application validates the request and may either generate a new customer- and report type specific menu page, or select report template and filters and execute queries for report data.
3. The web application translates report data to fit the report template
4. The web application returns a customer specific report to the customer Client browser.

2.3.2.3 Test Case 1.3: "Report Customisation"

Test Case Identification

Test ID:	T2-TT3-1.3	Report Customisation
Event Type:	Local	
Location(s):	Copenhagen / TDC	
Partners involved:	TDC	
Planned Date:	Start November	
Trial Planner(s):	Assurance Group	
Trial Evaluator(s):	TDC	
Developer(s):	Catherine Goret Nielsen TDC Jens Dyhre Mouritzsen TDC	

Purpose

The customer specific reports are based on information that can be changed and adapted to individual customer needs. Configuration and customisation of reports should be controlled by updates of XML documents or by adding new XML documents local or external to the web application.

Pre-conditions

Customer specific information are formatted in XML and made available to the web application. This includes the templates; filters and XML style-sheets to be used to generate the customers report pages.

Post-conditions

Changes made to reporting templates will effect the out-line of the report.

Changes made to reporting filters will effect the information and data in a report.

Changes made to reporting style-sheets will effect the presentation of data e.g. text, tables or graphics.

Test Case Success Criteria

- Changes made to reporting templates will effect the out-line of the report, but only for the customers which uses these templates.
- Changes made to reporting filters will effect the information and data in a report, but only for the customers which uses these filters.
- Changes made to reporting style-sheets will effect the presentation of data e.g. text, tables or graphics, but only for the customers which uses these style-sheets.

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system (http://skinfaxe.delta.dk/reqsys_public)

Test Scenario

1. Administrator login on Web Server.
2. Changes are made to a reporting -template, -filter or -style-sheet.
3. The web application is updated to support the updated template.
4. The customer login to the web application and selects a report based on the updated template.
5. The web application generates a report where changes made to reporting -templates, -filters or -style-sheets are visible in the report page presented on the customers browser.

2.3.2.4 Test Case 2.1: "Production of Assurance Configurations"

Test ID:	T2-TT3-2.1
Event Type:	Local | Common
Location(s):	BRI
Partners involved:	TCD, BRI
Planned Date:	13/12/2001
Trial Planner(s):	BC/TCD, CH/TCD
Trial Evaluator(s):	VW/TCD
Developer(s):	BC/TCD, CH/TCD

Purpose

When an SLA is submitted to the assurance system it is necessary to configure the various components of the system to support it. The purpose of this test case is to evaluate how the SLA is processed by the system and to ensure that the correct configurations are produced for distribution to the other components of the system.

Pre-conditions

An SLA is agreed between the customer and the service provider.

Post-conditions

Configurations are produced and stored for each of the assurance system components.

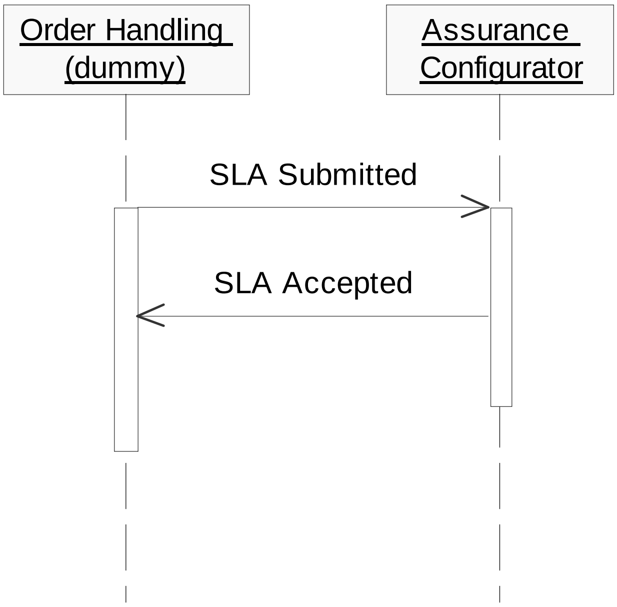
Test Case Success Criteria

The test case can be judged to be successful if coordinated configurations are produced, including an RAR for the bandwidth broker, which have the effect of monitoring all the terms and conditions applicable in the SLA.

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system (http://skinfaxe.delta.dk/reqsys_public)

Test Scenario



2.3.2.5 Test Case 2.2: "Service Monitoring"

Test ID:	T2-TT3-2.2
Event Type:	Local | Common
Location(s):	BRI
Partners involved:	TCD, BRI
Planned Date:	13/12/2001
Trial Planner(s):	BC/TCD, CH/TCD
Trial Evaluator(s):	VW/TCD
Developer(s):	BC/TCD, CH/TCD

Purpose

Once the assurance system has been configured in response to a new SLA the system will begin to monitor the service. This involves a number of different components distributed in the customer, provider and IES domains. Each of the components, called Server Monitors, in the customer and provider domains are responsible for collecting the statistics produced locally and processing them, if necessary, for use by the performance monitor. The performance monitor, in the IES domain, is then responsible for aggregating the statistics into metrics that match those specified in the SLA. The purpose of this test case is to evaluate how this process is currently supported by the system.

Pre-conditions

An SLA has been registered with the system and configurations produced from it.

Post-conditions

The metrics in the SLA are calculated and compared to the thresholds specified in the SLA.

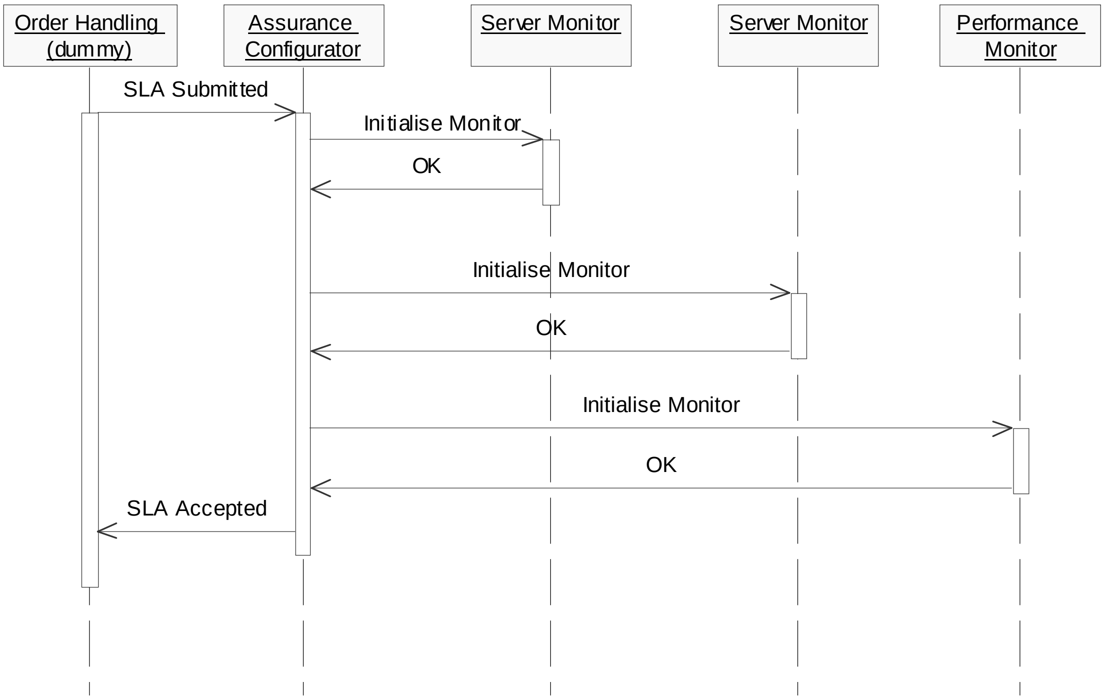
Test Case Success Criteria

This test case can be judged to be successful if the metrics specified in the SLA are correctly calculated from their constituent statistics. The final aggregated statistics will be accessible through the PerformanceMonitor contract and it is through this contract that the overall success of the can be judged.

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system (http://skinfaxe.delta.dk/reqsys_public)

Test Scenario



2.3.2.6 Test Case 2.3: “Service Violation Reporting”

Test ID:	T2-TT3-2.3
Event Type:	Local | Common
Location(s):	BRI
Partners involved:	TCD, BRI
Planned Date:	13/12/2001
Trial Planner(s):	BC/TCD, CH/TCD
Trial Evaluator(s):	VW/TCD

Developer(s): BC/TCD, CH/TCD

Purpose

While monitoring a service the assurance system calculates the values of the metrics used within the SLA. However it must also compare the values of these metrics to thresholds specified in the SLA to ensure that it has not been violated. If a violation does occur then the event must be generated to indicate this to interested parties. The purpose of this test case is to ensure that these events are produced and correctly identify the parameters that caused the violation to occur.

Pre-conditions

The Assurance System is monitoring a service in accordance to a specific SLA.

Post-conditions

A service violation report has been produced.

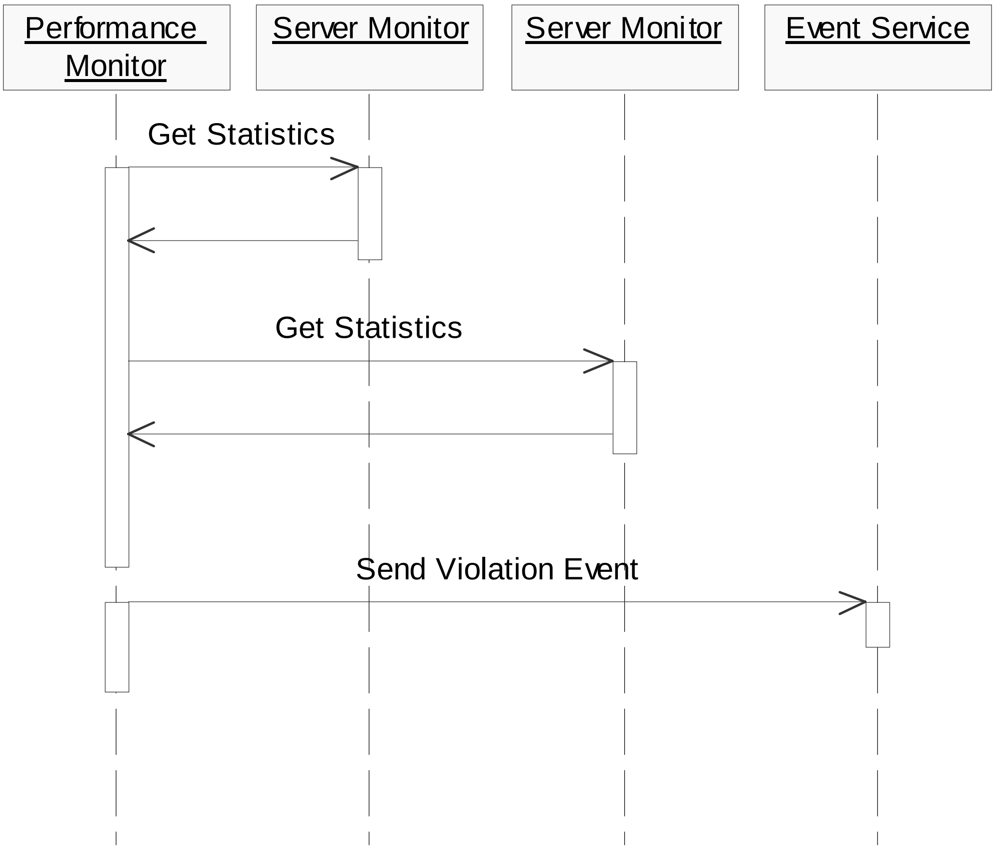
Test Case Success Criteria

This test case can judged to be successful if a violation event is generated and sent to interested parties. This event should also correctly identify which of the SLA metrics violated their threshold.

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system (http://skinfaxe.delta.dk/reqsys_public)

Test Scenario



2.3.2.7 Test Case 2.4: “Workflow implementation of assurance processes”

Test ID:	T2-TT3-2.4
Event Type:	Local | Common
Location(s):	BRI
Partners involved:	TCD, BRI
Planned Date:	13/12/2001
Trial Planner(s):	BC/TCD, CH/TCD
Trial Evaluator(s):	VW/TCD
Developer(s):	BC/TCD, CH/TCD

Purpose

The workflow framework enables flexible management of business processes within a system. The purpose of this test case is to evaluate the implementation of assurance business processes using the workflow framework. The assurance client invokes assurance processes. The workflow framework implements the control flow and data flow for the Building Blocks to implement the processes. Two different assurance processes were tested for configuration of the assurance Building Blocks to support an SLA.

Pre-conditions

The SLA is registered with the Assurance system.

Post-conditions

The Assurance system Building Blocks are configured to support the SLA.

Test Case Success Criteria

The assurance configuration processes are defined as UML activity diagrams, with related information models for the data passed between the activities. These models are mapped to the workflow framework process definitions. The success criteria are that the FORM Methodology for defining the processes is complete and that the workflow framework can implement the control and data flow for these processes.

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system (http://skinfaxe.delta.dk/reqsys_public)

Test Scenario

Figure 11 and Figure 12 show the activity diagrams describing the two Assurance processes that were implemented at the trial.

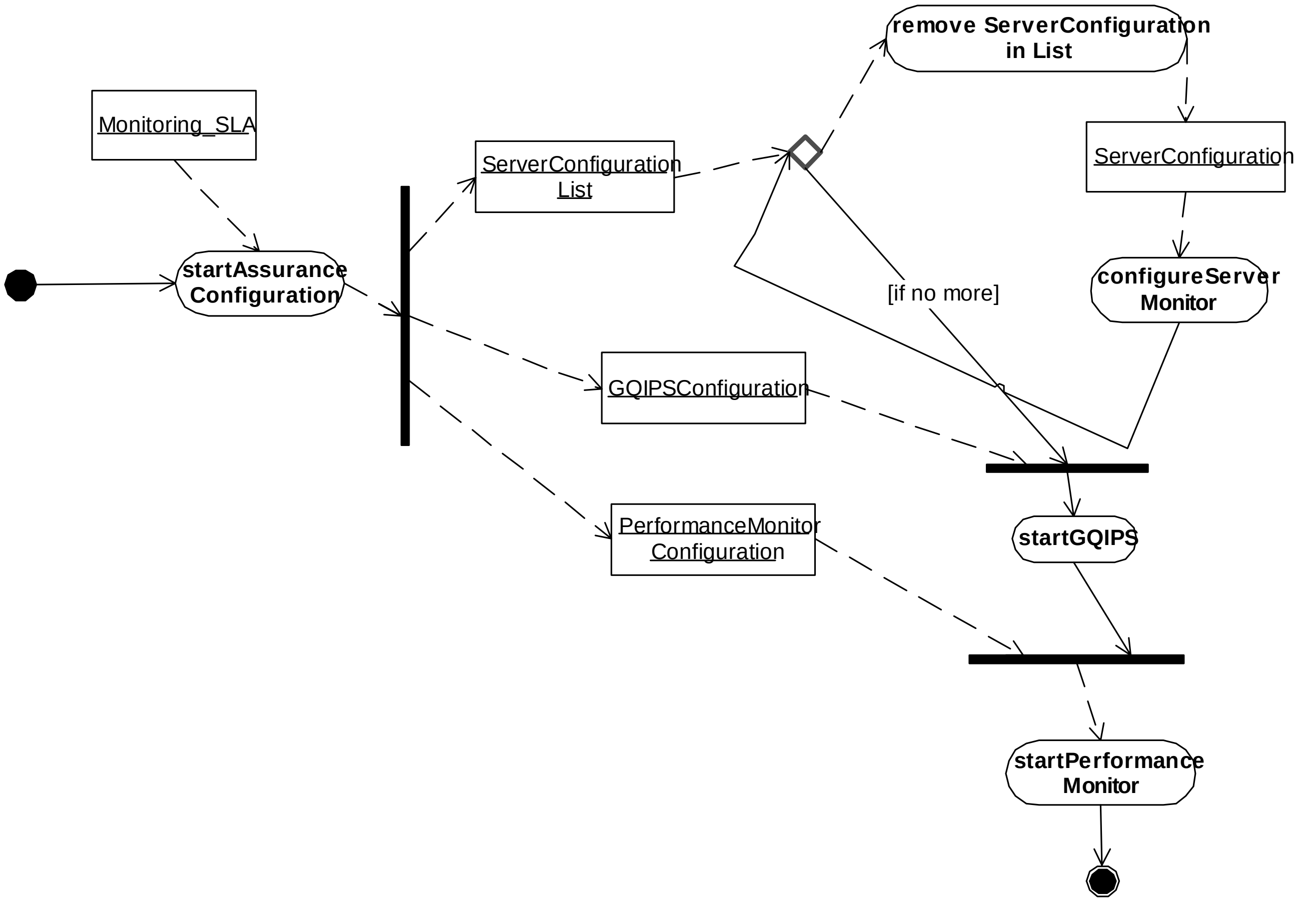


Figure 11: Assurance Configuration Process – serial invocation of server monitors

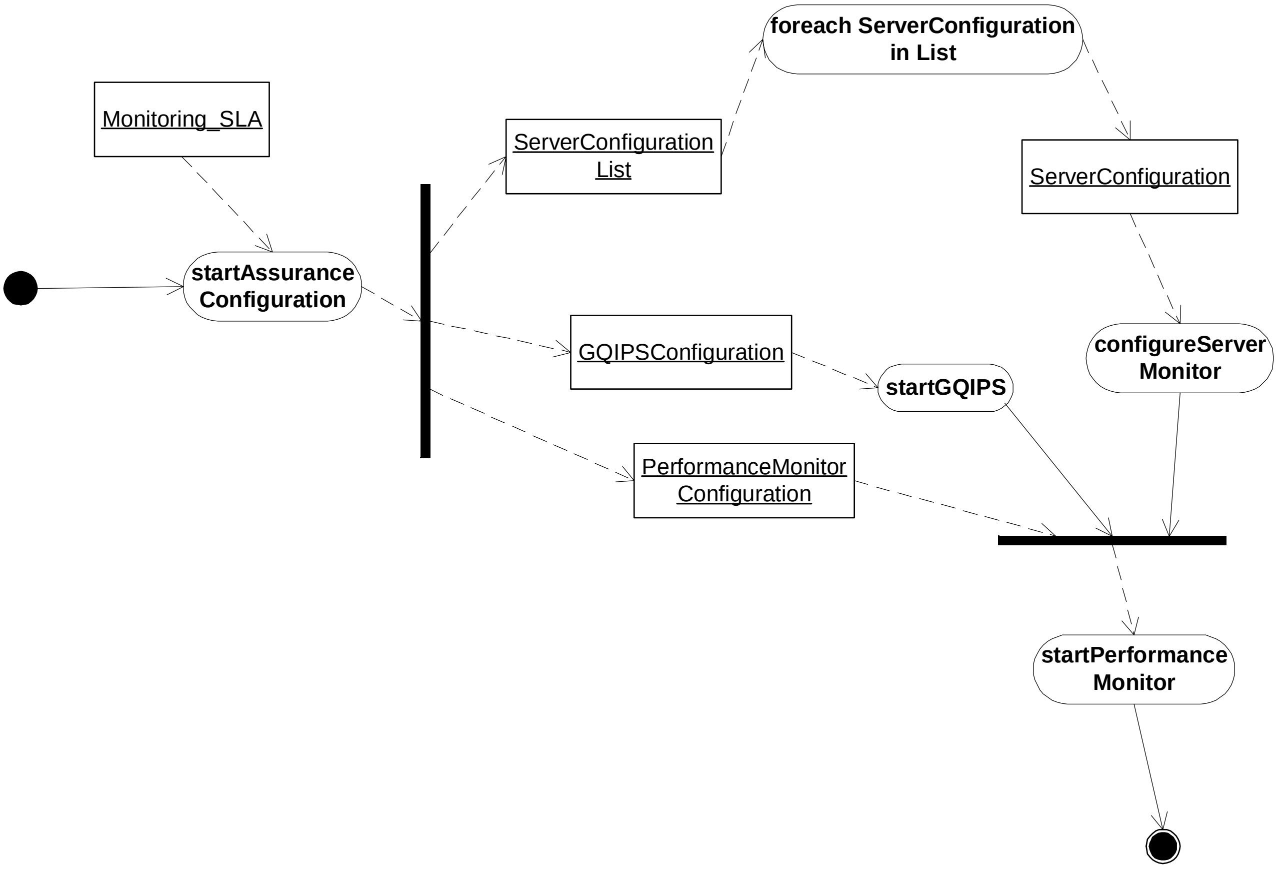


Figure 12: Assurance Configuration Process – parallel invocation of server monitors

2.3.2.8 Test Case 3.1 “B3 Setting”

Test Case Identification

Test ID:	T2-TT3-3.1
Event Type:	Local | Common
Location(s):	<Ireland>/<Broadcom>
Partners involved:	<Broadcom>

Planned Date:	Week 50 2001
Trial Planner(s):	Vincent Alexandre/BRI, Ronan McMahon/BRI
Trial Evaluator(s):	BRI
Developer(s):	Vincent Alexandre/BRI, Ronan McMahon/BRI

Purpose

The purpose of this test case is to show how a network operator sets the domain information, inputs and draws a Network Topology (NT) into the GQIPS sub-system, using the B3 console.

Pre-conditions

B3 sits on a (test-bed) network

Post-conditions

A network topology is drawn into the GQIPS sub-system

Test Case Success Criteria

The test bed network has been sucessfully drawn in the GQIPS sub-system.

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system (http://skinfaxe.delta.dk/reqsys_public)

Test Scenario

The network operator performs a login into the B3 console, providing some user name and password information. The corresponding B3 process lookups (through a naming service) for the EJB server/container, and establishes a connection.The network operator sets the domain information: domain's name and key, BBr's IP address. It then adds some *Hosts* and *Segment Hubs* network elements using the B3 console's NT tool. Finally it draws the (test bed) network, adding some network element links between these network elements, and setting for each of them the two connections points, and the link's bandwidth reserved for EF traffic.

2.3.2.9 Test Case T2-TT3-3.2: "Single domain service negotiation"

Test Case Identification

Test ID:	T2-TT3-3.2
Event Type:	Local | Common
Location(s):	<Ireland>/<Broadcom>
Partners involved:	<Broadcom>
Planned Date:	Week 50 2001
Trial Planner(s):	Vincent Alexandre/BRI, Ronan McMahon/BRI
Trial Evaluator(s):	BRI
Developer(s):	Vincent Alexandre/BRI, Ronan McMahon/BRI

Purpose

The purpose of this test case is to check the formulation, formatting, sending, receiving, and answering of a service negotiation, considering only a single domain and a QoS request which is not to resource-hungry (i.e. whose request can be fulfilled).

Pre-conditions

The network assurance components receive an RAR based on an agreed SLA.

Post-conditions

The B3 formats the answer to the customer's video on demand service request, as an XML file of the Bandwidth Brokered SLA XML schema, and sends it back to the QoS customer.

Test Case Success Criteria

The B3 console process is notified that a new service activation is requested and the set of activations requests handled by the console is updated to reflect this new one.

The B3 formats the answer to the customer's video on demand service request, as an XML file of the Bandwidth Brokered SLA XML schema, and sends it back to the QoS customer.

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system (http://skinfaxe.delta.dk/reqsys_public)

Test Scenario

The network assurance components receive an RAR based on an agreed SLA and parse the request. An object information model representing this request is then built. The B3 console process is notified that a new service is asked to be negotiated, and the set of negotiations requests handled by the console is updated to reflect this new one.

Path to route the service is computed by the B3 instance, figuring out the network element links that have to be crossed to route the traffic. For each of these links, resources and available resources are calculated.

Available resources are updated to reflect that the service request can be fulfilled and the service has been accepted.

An activation request is automatically formulated by the B3; as a matter of fact the B3 console process is notified that a new service activation is requested, and the set of activations requests handled by the console is updated to reflect this new one.

The B3 formats the answer to the customer's video on demand service request, as an XML file of the Bandwidth Brokered SLA XML schema, and sends it back to the QoS customer.

2.3.2.10 Test Case T2-TT3-3.3 : "Events subscription and notification"

Test Case Identification

Test ID:	T2-TT3-3.3
Event Type:	Local | Common
Location(s):	<Ireland>/<Broadcom>
Partners involved:	<Broadcom>

Planned Date:	Week 50 2001
Trial Planner(s):	Vincent Alexandre/BRI, Ronan McMahon/BRI
Trial Evaluator(s):	BRI
Developer(s):	Vincent Alexandre/BRI, Ronan McMahon/BRI

Purpose

The purpose of this test case is to show how an interested party can subscribe to B3's event notification service, in order to be informed latter, when events will occur onto the service. Because there is no use of routers in this first trial, and that therefore no user traffic will be routed, the word *event* in this document is used to represent issues happening when the service is expired, or cancelled.

Pre-conditions

Service assurance components provides some user name and password information, and lookup (through a naming service) on the EJB server/container for the B3 instance responsible for the domain these service assurance components are deployed on.

Post-conditions

One minute before that the video on demand's SLA expires (see first test case), the B3 instance notifies the service assurance components that the SLA will soon expire. In the same time the B3 console, which is first subscriber of all the services, is notified also and its log window catches and displays the event.

Test Case Success Criteria

The B3 instance notifies the service assurance components that the SLA will soon expire. The B3 console, which is first subscriber of all the services, is notified also and its log window catches and displays the event.

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system (http://skinfaxe.delta.dk/reqsys_public)

Test Scenario

Service assurance components provides some user name and password information, and lookup (through a naming service) on the EJB server/container for the B3 instance responsible for the domain these service assurance components are deployed on. A connection is finally established.

Service assurance components register to the subscription service, providing the SLA identifier of the service they are interested to be notified in. As a matter of fact, the B3 console process is informed that a new party has requested to subscribe to the events occurring on this service, and the set of events' subscribers handled by the console is updated to reflect this new one.

One minute before that the video on demand's SLA expires, the B3 instance notifies the service assurance components that the SLA will soon expire. In the same time the B3 console, which is first subscriber of all the services, is notified also and its log window catches and displays the event.

2.3.2.11 Test Case T2-TT3-3.4 : "Multi domains RAR negotiation"

Test Case Identification

Test ID:	T2-TT3-3.3
Event Type:	Local | Common

Location(s):	<Ireland>/<Broadcom>
Partners involved:	<Broadcom>
Planned Date:	Week 50 2001
Trial Planner(s):	Vincent Alexandre/BRI, Ronan McMahon/BRI
Trial Evaluator(s):	BRI
Developer(s):	Vincent Alexandre/BRI, Ronan McMahon/BRI

Purpose

The purpose of this test case is to test the inter-domain service negotiation protocol, through a GQIPS'B3 to GQIPS's B3 communication.

Pre-conditions

Network assurance components receive an RAR based on a previously agree SLA.

Post-conditions

This first B3 instance formats the answer to the video on demand service customer's request, as an XML file of the Bandwidth Brokered SLA XML schema, and sends it back to the QoS customer.

Test Case Success Criteria

The B3 console process is notified that a new service negotiation is requested, and the set of negotiations handled by the console is updated to reflect this new one.

This B3 instance formulates the negotiation request to be sent to a second B3, the one responsible for the domain where this second movie is served. This request is formulated into a Bandwidth Brokered SLA XML file, and sent to this second B3 instance.

The second B3 console process is notified that a new service negotiation has been requested, and the set of negotiations handled by this console is updated to reflect this new one.

This second B3 instance formats the answer, as an XML file of the Bandwidth Brokered SLA XML schema, and sends it back to the first B3 instance.

The available resources set of the first B3 instance are updated to reflect that the service request can be fulfilled and the service has been accepted. An activation request is then automatically formulated by this first B3 instance; as a matter of fact its console process is notified that a new service activation is requested, and the set of activations handled by this console is updated to reflect this new one.

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system (http://skinfaxe.delta.dk/reqsys_public)

Test Scenario

Network assurance components receive an RAR based on a previously agree SLA and parse this request, and build an object information model representing it. The B3 console process is notified that a new service negotiation is requested, and the set of negotiations handled by the console is updated to reflect this new one.

Path to route the service is computed by the B3 instance, figuring out the network element links that have to be crossed to route the traffic. For each of these links, the resources and available resources are calculated.

This B3 instance formulates the negotiation request to be sent to a second B3, the one responsible for the domain where this second movie is served. This request is formulated into a Bandwidth Brokered SLA XML file, and sent to this second B3 instance.

This second B3 instance receives and parses the request, and builds an object information model representing it. Its console process is notified that a new service negotiation has been requested, and the set of negotiations handled by this console is updated to reflect this new one. Path to route the service is computed by this second B3 instance, figuring out the network element links that have to be crossed to route the traffic. For each of these links, available resources are calculated, and then updated to reflect that the service can be fulfilled and has been accepted. An activation request is then automatically formulated by this second B3; as a matter of fact the B3 console process is notified that a new service activation is requested, and the set of activations handled by this console is updated to reflect this new one. This second B3 instance finally formats the answer, as an XML file of the Bandwidth Brokered SLA XML schema, and sends it back to the first B3 instance.

The available resources set of the first B3 instance are updated to reflect that the service request can be fulfilled and the service has been accepted. An activation request is then automatically formulated by this first B3 instance; as a matter of fact its console process is notified that a new service activation is requested, and the set of activations handled by this console is updated to reflect this new one.

This first B3 instance finally formats the answer to the video on demand service customer’s request, as an XML file of the Bandwidth Brokered SLA XML schema, and sends it back to the QoS customer.

2.3.3 Test Team 3 Conclusions

2.3.3.1 Customer Login and Validation.

Customer specific information is XML formatted, and the web application uses 'standard' XML techniques to make such information available for the application.

Testcase Evaluation

To save programming resources by implementing an open source XML parser software, it was required to update the selected open source Web server to the latest beta version, which resulted in lack of portability of the Web service to older Web servers. One problem which came up was that the Web server itself included an XML parser which it uses for configuration, so trying to install a new one resulted in class conflicts between Java classes. The problem was later recognised by the Web server provider and a solution was provided in a later beta version.

Requirements impact

It should be possible to define counter actions for security violations or violation attempts.

This was a very general requirement but also very important since the client Web page returned to the customer after successful login, was customer specific and should only be shown to the right customer. It was addressed to examine the benefit of using XML to mark-up information about customers in the IESP customer base.

2.3.3.2 Reporting Template Completion

'Standard' web programming techniques are used to define 'browser specific' dynamic client pages (templates) to present customer specific information and selected report data. 'Standard' web programming techniques are used to enable generation of 'browser specific' dynamic menu pages with customer specific information and menu options, and customer menu selections are used to initialise search filters for collection of reporting data. Web application detects missing customer client input, and adds help-messages to the customer menu page.

Testcase evaluation

The use of Java Server Pages enabled changes in the client web pages to be implemented with very little programming effort. Again to take advantage of this new technique required that the latest versions of the Java platform used by the Web server was used, so again there was a lack of portability to older Java platforms.

Requirements impact

End-customers can receive information about performance and usage of end-customer equipment.

This was also a general requirement and it was seen as a requirement for a very flexible solution that could be customised to specific end customer demands with very little programming effort.

Status and statistics. IESP requires management functions, which enables end-customers to get information regarding status or statistics from managed equipment on-demand and on schedule.

Since most existing reporting services support on schedule reports this was addressed by focusing on on-demand reports where the customer uses a menu to select only that information which are required here and now by the customer.

2.3.3.3 Report Customisation.

Information used for customisation is XML formatted, and 'Standard' XML techniques are used to add or change information. Translation to customer client browser mark-up language, can be done by web application or by client browser.

Testcase evaluation

The use of open source software for translation of XML documents also required the use of the latest beta version of the Web server. The selected XSL Translation technique enabled translation of XML documents into other XML documents with very little programming effort, but it did not support the use of variables to add dynamic information like e.g. counters to be used in reports. As a result of that all dynamic information had to be added to the XML document before the translation, or handled by using temporary XML documents.

Requirements impact

Presentation of service information. MSP requires components that support presentation of service information on end-customer terminals.

Since most existing reporting services support presentation on Web browsers this requirements was addressed by focusing on the Web services ability to detect if the customer browser supported Wireless Application Protocol WAP or XHTML which are used in the latest version of WAP. In addition to adapting to the protocol version used by the customer, an attempt was made to take advantage of a new technique to create scaleable graphics that can be scaled to match the dimension of the customer terminal display. The use of Scaleable Vector Graphics (SVG) also enabled reuse of the XML translation software since SVG is an XML based specification language. The test showed that XML to SVG translation might be handled by the customer's own browser if it has the correct SVG software plug-in installed. A major advantage of SVG is that it reduces the size of the graphics data that needs to be transmitted to and stored on the customer terminal. Another advantage is that SVG enable graphics to be interactive e.g. a customer can zoom in on graphics e.g. on a small display on a mobile terminal display.

2.3.3.4 Production of Assurance Configurations

Stated Purpose: When an SLA is submitted to the assurance system it is necessary to configure the various components of the system to support it. The purpose of this test case is to evaluate how the SLA is processed by the system and to ensure that the correct configurations are produced for distribution to the other components of the system.

Comments on Test Case:

This test was carried out using simplified SLAs containing just one or two metrics that could be easily calculated. The system successfully produced and distributed the configuration policies required by the other components of the system. No serious problems were encountered in the implementation of this test case although certain deficiencies in the information model being used were identified.

In particular it was found in certain areas that associations, necessary to traverse the information model successfully, were missing and had to be added. Another more difficult problem was the way in which the CIM Object Manager (CIMOM) used in the trial dealt with references to CIMOMs on other hosts. It was found that by default a CIM Object Path object does not have it’s host name component set to any value. Also there is no way to transparently access multiple CIMOMs simultaneously. Therefore for the purposes of implementation it was found necessary to define the points in the information model where other hosts could be referenced. This area will need to be further addressed in the future.

Comments on Requirements:

For the most part the requirements to be met by this use case were addressed. In particular those relating to the SLA and Service Architecture information models, IA-I.02 and IA-I.04, and the requirement for Policy Construction, IA-II.06, were fully addressed although it was identified were further improvements can still be made.

This leaves two requirements that were only partly validated by this trial. The first of these, IA-II.05, relates to the subject of SLA Admission. Currently the SLA is only checked to ensure that it is well formed and relates to a known server. Further work needs to be done in this area to deal with multiple SLAs and the conflicts that can arise between them.

2.3.3.5 Service Monitoring

Stated Purpose: Once the assurance system has been configured in response to a new SLA the system will begin to monitor the service. This involves a number of different components distributed in the customer, provider and IES domains. Each of the components, called Server Monitors, in the customer and provider domains are responsible for collecting the statistics produced locally and processing them, if necessary, for use by the performance monitor. The performance monitor, in the IES domain, is then responsible for aggregating the statistics into metrics that match those specified in the SLA. The purpose of this test case is to evaluate how this process is currently supported by the system.

Comments on Test Case:

The results of this test case can be presented in two parts. After configuration the Server Monitors performed as expected refreshing metrics at specified intervals using the calculation method specified in the configuration. There was, however, a problem with the Perl DLL that was used to perform the calculation of the metrics that caused the system to stop working on several occasions. It was decided therefore that different methods of performing these calculations should be investigated to make the system more stable.

Unfortunately at the time of the trial the functionality of the Performance Monitor was incomplete. Therefore only the ability of the Performance Monitor to gather statistics and events from the various server monitors was evaluated. While statistics were gathered from the Server Monitors successfully issues did arise concerning the information models used to store them. In particular there was some discussion over the best method for storing previous metric values (for trend analysis etc).

Comments on Requirements:

Three requirements were addressed by this trial. The first, that the management service should be able to cover several geographical locations (EC-II.22), was addressed by the production of the Server Monitor components and the extraction of statistics from them by the Performance Monitor.

The other two requirements, EC-II.30 and IA-II.10, both relate to the production of service statistics and notifications. These requirements were only partly fulfilled as although the statistics relating to the service were collected and could be presented in debug format they were not placed into a proper format. This issue will be addressed with the finalisation of the report generator component.

2.3.3.6 Service Violation

Stated Purpose: Reporting While monitoring a service the assurance system calculates the values of the metrics used within the SLA. However it must also compare the values of these metrics to thresholds specified in the SLA to ensure that it has not been violated. If a violation does occur then the event must be generated to indicate this to interested parties. The purpose of this test case is to ensure that these events are produced and that they correctly identify the parameters that caused the violation to occur.

Comments on Test Case:

For the purposes of this test case an SLA was submitted to the system that had a threshold that was known would be violated. For this test the workflow engine was also setup to start a process on the receipt of these events. In this way we hoped to simulate part of the one of the MCG processes, namely the Billing-Assurance process.

As before the Server Monitor calculated the statistics successfully. When compared to the specified threshold the Server Monitor then threw an event (in the form of a JMS message). This message was then received and interpreted correctly by the workflow engine. During this test it was identified that further information may need to be stored in the event to properly identify the context from which it was raised. Also although it did not have a direct bearing on the test case another area that needs to be addressed is the quantity of events produced and when notification should be suppressed.

Comments on Requirements:

The most important requirement to be met by this testcase was the “QoS Monitoring” requirement, IA-II.07, and this was indeed fulfilled by the trial in the way in which both the Server Monitors and the Performance Monitor could calculate/collect statistics relating to the service performance and determine when thresholds had been broken.

The other requirements, EC-II.29, IA-II.08 and IA-III.12, all relate to the production and reception of asynchronous notifications or events. Mechanisms for fulfilling these requirements, through the use of JMS, have been identified and tested to a certain degree although further testing needs to be carried out before these requirements can be considered properly fulfilled.

2.3.3.7 Workflow implementation of Business Processes

Stated Purpose: The workflow framework enables flexible management of business processes within a system. The purpose of this test case is to evaluate the implementation of assurance business processes using the workflow framework. The assurance client invokes assurance processes. The workflow framework implements the control flow and data flow for the Building Blocks to implement the processes. Two different assurance processes were tested for configuration of the assurance Building Blocks to support an SLA.

Comments on Test Case:

The test case successfully executed the two variations of the assurance business process and raised one important issue concerning the specification of the control and data flow in UML. The UML v1.3 activity diagram is not able to specify correctly the dynamic invocation of multiple instances of the same activity and these instances subsequent synchronisation. We partly specified this control flow requirement using the "Foreach Configuration in List" activity but the subsequent synchronisation of the instances was left unspecified in the diagram. This control flow requirement was hand coded into the control flow rule code.

There were no significant problems encountered during the test. Further investigation is necessary in the mapping of activity diagram to process control and data flow rules, in particular, how best to deal with cases where the activity diagram cannot specify the desired control flow. Future work will look into providing extensions to the UML activity diagram to enable specification of these more complex control flow structures. Also further implementation of coarser grained business processes needs to be carried out to demonstrate the workflow frameworks full potential.

Comments on Requirements:

As the workflow framework is seen as a platform service and not a Building Block, the requirements it addresses belong to the Generic Framework Requirements. These requirements are general software engineering requirements and are related to the separation of Process from Entity. The workflow framework encourages a clear separation of process from entity, which produces a more flexible and scalable system. These generic requirements did not change throughout the project.

2.3.3.8 GQIPS

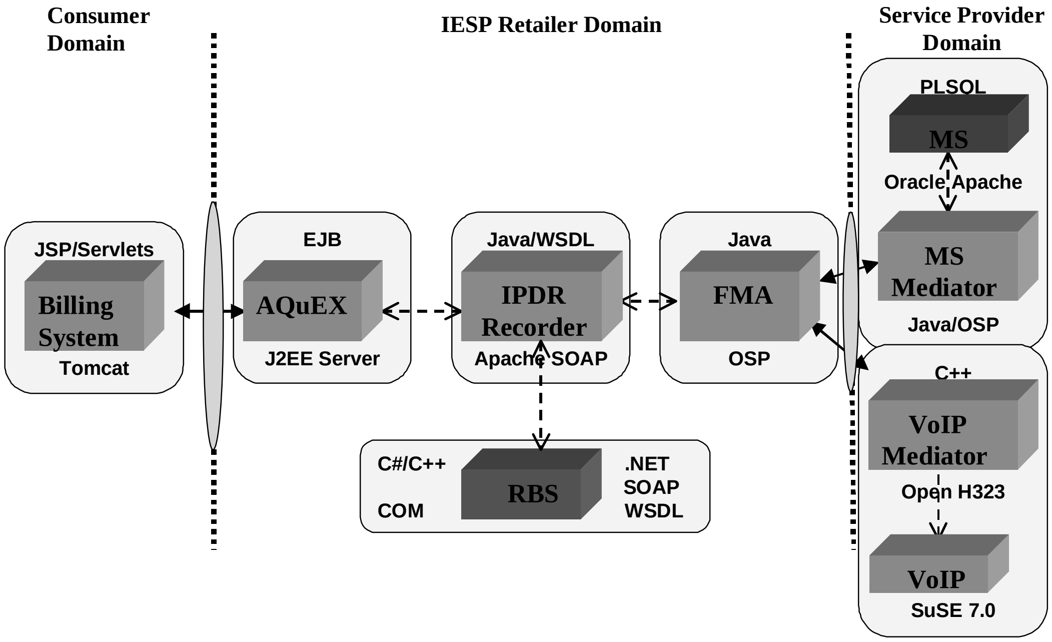
The GQIPS Trial 2 Test cases consisted of "B3 Setting", "Single domain service negotiation", "Events subscription and notification" and "multi-domain RAR Negotiation". For trial 2 the GQIPS system was integrated with an existing policy server and mediation device. These test cases took place on real router with the Broadcom test lab. The Assurance Trial 2 (in Dublin, December 2001) demonstrated the integration of the GQIPS with the Assurance group and the GQIPS test cases demo on the test network. GQIPS was also integrated in the VPN (test team 2) trial in Copenhagen, December 2001.

Comments on Requirements:

Of the operational requirements which were originally collected, all remained relevant for the test cases. It was noted that nearly all were fulfilled at design phase. The requirements were used as guidelines at design phase. The ideas of the Qbone initiative were another driving factor at the design phase of the GQIPS. Those that were not fulfilled at implementation phase, were due to resource limitations.

2.4 Test team 4 – Billing

This section contains information relating only to Trial Team TT4. The figure given bellow shows the technical architecture of the system whose test cases are specified in this document.



2.4.1 Trial Planning

2.4.1.1 Trial Objective

The trial is based on the execution of two trial scenarios. The first will demonstrate single service (VoIP) provision and rating/discounting for customer charging and service provider settlement. The second will demonstrate composed service provision and rating.

These scenarios will support the evaluation of:

- Preliminary test of InterdomainAcctMan contract: This was done in Trial 2 through the aggregation of multiple usage sessions.
- Support for convergence of services (voice and data): This was demonstrated in Trial 2 by a composite service called Online Collaboration Service.
- Evaluation of composite service information model: This is largely based on and makes use of IPDR information model. The usage information sent by Online Collaboration Service model is modelled on composite service information model.
- Mediation of the usage of multiple services in real-time and adaptable and practicability of federated mediation in multiple SP environment Fulfilment and Billing MCG sub-scenario
- Fulfilment and Billing MCG sub-scenario
- OSP (Open Service Platform) support for Federated Mediation Adaptor (FMA) Building Block
- 3 Phase service discounting – usage discounting, periodic discounting and incentive discounting
- E-IPDR rating and discounting

- Aggregated rating for composed service usage
- IESP broker settlement rating
- SLA/SLS based rating algorithms
- VoIP service provision and usage mediation
- An E-IPDR recorder and Database
- SOAP/.Net webservices

2.4.1.2 Trial Plan

Test Case ID	Name	Partner(s)	Planned
T2-TT4-1.1	Monitoring of Online Collaboration Service Session	FOKUS	[end] 11
T2-TT4-1.2	Usage Mediation of Online Collaboration Service	FOKUS	[end] 11
T2-TT4-1.3	Transfer of OCS E-IPDR document and making use of it	FOKUS	[end] 11
T2-TT4-2.1	Rating, Settlement and discounting for a VoIP service	WIT	M3 – FOKUS/Berlin 16/11/01
T2-TT4-2.2	Rating for a composed service (OCS)	WIT/FOKUS	M3 – FOKUS/Berlin 16/11/01

2.4.1.3 What is Trialed/Tested

Building Block(s) (BBs)

BB	Version	Provider	Comments
FMA	v.1.0	FOKUS	
RBS	V1.5	WIT	Re-implemented to incorporate settlement, discounting and composed service rating
E-IPDR Recorder	V1.0	WIT	

Contract(s)

Contract	Ver.	Specification URI	RP	Description
fokus.fhg.de/FORM/InterdomainAcctMan	2.1	http://www.cs.ucl.ac.uk/research/form/models/ContractCatalogue/fokus.fhg.de/FORM/InterdomainAcctMan/Contract.xml	IES-BS	This is a service management contract and supports accounting management in a federated environment where multiple SPs provide their services to the customer. This contract is designed to perform accounting management tasks on

				application-level services (e.g., delivery of video, sound and text content to user applications), as well as network-level service (e.g., a VPN). The primary function of this contract is the exchange of accounting management information, which, in turn, enables Billing operation processes to perform mediation, charging, and the rest. This contract is provided by the Federated Mediation Adaptor (FMA) building block. The services provided by this contract are defined within TOM's Billing business process (functional domain).
E-IPDRecCtr	1.0	http://www.cs.ucl.ac.uk/research/form/models/ContractCatalogue/tssg.wit.ie/FORM/E-IPDRecCtr/Contract.xml	None	This is the contract between the E-IPDR recorder and the Federated Mediation Adaptor. This contract supports the passing of E-IPDRs between the two BBs.
RBSCtr	1.0	http://www.cs.ucl.ac.uk/research/form/models/ContractCatalogue/tssg.wit.ie/FORM/RBSCtr/Contract.xml	None	This contract supports the retrieval and return of E-IPDRs between the RBS and the E-IPDR recorder.

2.4.1.4 Test Environment

Hardware Environment

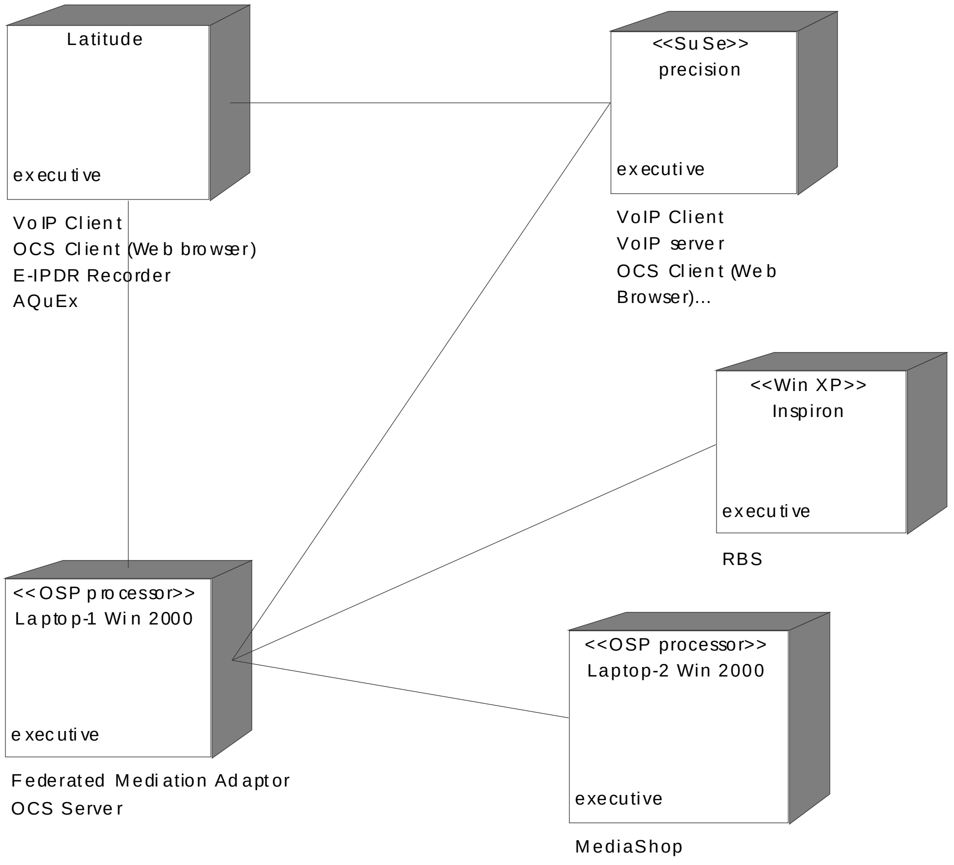
Product	Version	Used By	Provider	Comments
Windows2000 PC	--	FOKUS	--	OSP & FMA & OCS
Precision 220 512 RAM 1GHz	PIII	WIT	DELL	VoIP service and mediator
Latitude Cpi 256 RAM 550 MHz	PII	WIT	DELL	E-IPDR Recorder and E-IPDR Database, VoIP client (NetMeeting)
Inspiron 8100 512 RAM 833 MHz	PIII	WIT	DELL	RBS

Software Environment

Product	Version	Used By	Provider	Comments

Oracle	8i	FOKUS	Oracle	
OSP	0.92	FOKUS	FOKUS	
Oracle	8i	WIT	Oracle	E-IPDR Database
Win 2K Adv Server	2000	WIT	Microsoft	Operating system for Latitude Cpi
Win XP	2001	WIT	Microsoft	Operating system for Inspiron 8100
SuSe Linux	7.0	WIT	SuSe	Operating system for Precision 220
Office XP	2001	WIT	Microsoft	Excel XP used by RBS
.NET ASP	???	WIT	Microsoft	RBS Webservices
Apache SOAP		WIT	Apache	
OpenPhone	??	WIT		
Visual Studio .NET	7.0	WIT		
Jbuilder	5.0	WIT		

Deployment Diagram



2.4.1.5 Trial Results Specification and Evaluation Criteria

The Operational Requirements relation to the various test-cases are managed through the FORM trial-to-requirement mapping web-system. (http://skinfaxe.delta.dk/reqsys_public)

2.4.1.6 Risk List and Contingency Plans

The Risk are prioritised according to impact rating, which is severity (1=Lowest, 5=highest) multiplied by probability of occurrence/100%.

Risk	Severity	Occurrence probability (%)	Impact rating	Contingency plan
Database Failure	5	30%	1.5	E-IPR recorder simulation batch file
MediaShop service failure	3	30%	.6	Simulation of E-IPDR delivery to FMA using a batch file
VoIP Service Failure	3	20%	.6	Simulate service usage and delivery of E-IPDR using a batch file

2.4.2 Test Cases

2.4.2.1 Test Case 1.1: "Monitoring of Online Collaboration Service Session"

Test ID:	T2-TT4- 1.1
Event Type:	Local | Common
Location(s):	D/FOKUS
Partners involved:	FOKUS
Planned Date:	[end] 11
Trial Planner(s):	Bhushan, Gringel/FOKUS
Trial Evaluator(s):	Bhushan, Gringel/FOKUS, Ryan, Leray, Brazil, Cloney/WIT
Developer(s):	Gringel/FOKUS

Purpose

The Online Collaboration Service (OCS) enables the end-user to use MediaShop and VoIP services (or constituent services) simultaneously and within a single online session. When end-user attempts to use the OCS, the OCS session branches off MediaShop and VoIP sessions. There are two types of sessions involved in this scenario: OCS session and constituent services sessions. Therefore it is important to verify whether FMA monitors OCS session, called parentSession, and records its duration in real-time. The OCS session denotes the duration within which the constituent services are used (or, MediaShop and VoIP sessions existed). There is another purpose of this test, which is to verify whether FMA monitors and knows about the services (i.e., MediaShop and VoIP service IDs) that are being used as parts of OCS.

Pre-conditions

Two preconditions concerning this test case are:

1. The Open Service Platform is up and running.
2. The end-user has started using the OCS.

Post-conditions

The expected results of this test case are:

1. Recording of duration for which the OCS session was alive.
2. Sending of OCS session ID (i.e., parentSession ID) to MediaShop and VoIP Mediation Adatpors.
3. Recording of MediaShop and VoIP service IDs.

Test Case Success Criteria

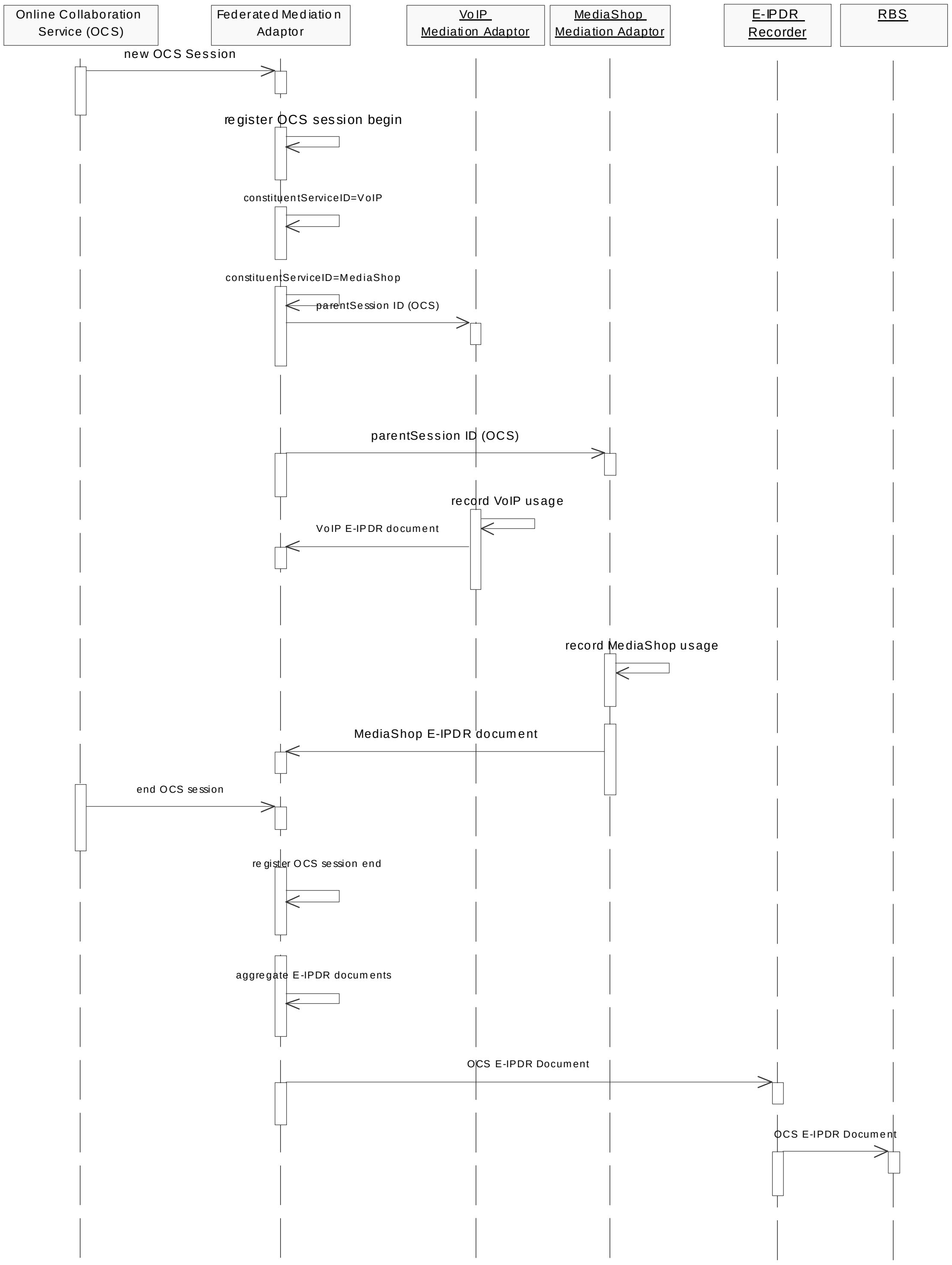
The test cases is considered to be successful if the following conditions are fulfilled:

1. Start and end of OCS session is registered in OCS E-IPDR document produced by FMA.
2. The OCS E-IPDR document carries the identifiers of MediaShop and VoIP services (or, constituent services).

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system (http://skinfaxe.delta.dk/reqsys_public)

Test Scenario



2.4.2.2 Test Case 1.2: "Usage Mediation of Online Collaboration Service"

Test ID:	T2-TT4- 1.2
Event Type:	Local | Common
Location(s):	D/FOKUS
Partners involved:	FOKUS, WIT
Planned Date:	[end] 11
Trial Planner(s):	Bhushan, Gringel/FOKUS
Trial Evaluator(s):	Bhushan, Gringel/FOKUS, Ryan, Leray, Brazil, Cloney/WIT
Developer(s):	Gringel/FOKUS Brazil, Cloney/WIT

Purpose

The VoIP and MediaShop Mediation Adaptors communicate with FMA and transfer service usage data packaged in E-IPDR documents to FMA. The purpose of this test case is to verify whether the FMA can receive and aggregate the E-IPDR documents in real-time and usage-by-usage manner.

The aggregation must be done in a manner that each of E-IPDR documents aggregated can be correlated with the OCS E-IPDR document by means of a single parentSession or OCS session. The RBS should be able to track the usage of OCS through unique parentSession ID that FMA assigns to OCS E-IPDR documents as well as the VoIP and MediaShop E-IPDR documents. The RBS should also be able identify VoIP and MediaShop E-IPDR documents unambiguously.

Pre-conditions

Two preconditions concerning this test case are:

1. The Open Service Platform is up and running.
2. The end-user has started using the OCS.
3. MediaShop and VoIP Mediation Adaptors are up and running.

Post-conditions

1. The VoIP and MediaShop E-IPDR documents are generated for usage-by-usage event.
2. The VoIP and MediaShop E-IPDR documents are aggregated and correlated with OCS E-IPDR document by the means of parentSession ID.
3. The VoIP and MediaShop E-IPDR documents are listed in their entirety within the OCS E-IPDR document.
4. The VoIP and MediaShop E-IPDR documents carry OCS session ID as the parent session ID.

Test Case Success Criteria

This test case is considered to be successful if the RBS is able to relate the information contained (or, VoIP and MediaShop E-IPDR documents, to be precise) in the OCS E-IPDR document with any SLA that it might be holding for OCS service.

If the SLA states that OCS consists of VoIP and MediaShop service, the RBS must be able to charge the customer for the usage of these two services solely on the basis of the OCS E-IPDR document. For example, the customer is charged by volume of content downloaded and uploaded using MediaShop service. For VoIP service, the customer is charged by duration of phone call.

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system (http://skinfaxe.delta.dk/reqsys_public)

Test Scenario

Please see the test case T2-TT4-1.1 scenario.

2.4.2.3 Test Case 1.3: "Transfer of OCS E-IPDR document and making use of it"

Test ID:	T2-TT4- 1.3
Event Type:	Local | Common
Location(s):	D/FOKUS
Partners involved:	FOKUS
Planned Date:	[end] 11
Trial Planner(s):	Bhushan, Gringel/FOKUS Ryan, Leray, Brazil, Cloney/WIT
Trial Evaluator(s):	Bhushan, Gringel/FOKUS, Ryan, Leray, Brazil, Cloney/WIT
Developer(s):	Gringel/FOKUS, Ryan, Leray, Brazil, Cloney/WIT

Purpose

The purpose of this test case is to verify whether FMA is able to send the OCS E-IPDR document to RBS and RBS is able to make use of it in applying tariffs and calculating charges and discount.

Pre-conditions

1. The Open Service Platform is up and running.
2. The end-user has stopped using the OCS.
3. RBS is up and running and ready to receive OCS E-IPDR document.

Post-conditions

1. The RBS receives the OCS E-IPDR document and listed MediaShop and VoIP E-IPDR documents in their entirety.
2. RBS is able to identify all documents unambiguously by their docIds.

Test Case Success Criteria

The test case is considered to be successful if the following can be demonstrated:

1. The RBS is able to extract all the information contained in the OCS E-IPDR document and is able to populate its database. The RBS should be able to find information usage information (data encapsulated in SC, SS UE, CE elements).
2. The SC, SS UE, CE elements and data encapsulated within these elements can be correlated with the SLA and QoS information for charge processing and apply appropriate tariffs and discount.
3. The number of usage event should agree with the number of E-IPDR documents generated.
4. On the basis of usage data received, a correct MediaShop operation can be identified from an E-IPDR document and appropriate charging scheme can be invoked.

5. From SE element, the RBS is able to find customer types apply appropriate tariff and discount appropriately for the usage of MediaShop and VoIP service.
6. Charges for all the operations are summed up and RBS displays the correct total charges (in ChDR) for the usage of the service.

Related Operational Requirements

Test Scenario

Please see the test case T2-TT4-1.1 scenario.

2.4.2.4 Test Case 2.1: “Rating, Settlement and Discounting for a VoIP service”

Test ID:	T2-TT4- 2.1
Event Type:	Local | Common
Location(s):	D/FOKUS
Partners involved:	WIT
Planned Date:	16/11/01
Trial Planner(s):	Ryan/WIT
Trial Evaluator(s):	Ryan, Leray, Brazil, Cloney/WIT
Developer(s):	Brazil,Leray,Cloney,Ryan/WIT

Purpose

The purpose of this test case is to:

- ❑ Test the provision of a VoIP service and the subsequent usage of the service
- ❑ Test the ability of the VoIP mediator to perform E-IPDR mediation

- Test if the E-IPDR recorder can record E-IPDRs and notify the RBS that E-IPDRs require rating
- Test the integration between the VoIP mediator, the E-IPDR recorder and the RBS
- Test the ability of the RBS to perform usage/periodic/incentive discounting
- Test the ability of the RBS to perform customer charge and settlement rating
- Test the ability of the RBS to rate against parameters extracted from an SLA/SLS

Pre-conditions

- The VoIP service, RBS and E-IPDR recorder are running
- The E-IPDR database exists
- An SLA and an SLS exist for the respective customer and service provider
- The RBS can retrieve SLA/SLS accounting information from the SLA/SLS manager

Post-conditions

- A rated/discounted E-IPDR is generated and stored for each VoIP service usage
- An XML Bill Details Document is created that can be used by a billing system to construct a periodic Bill.
- An XML Settlement Invoice Details document is created to be used by a Service Provider invoicing system.
- Bill Details.xml should incorporate usage, periodic and incentive discounting based on parameters that were originally negotiated in an SLA.
- Settlement invoice Details.xml should incorporate usage and periodic discounting based on parameters that were originally agreed in an SLS.

Test Case Success Criteria

- The rated E-IPDRs must exhibit accurate charging/settlement relative to the QoS violations specified in the SLSs/SLAs
- The E-IPDRs contain useful usage information to be later viewed by the customer/service provider
- All rating is achieved in real-time

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system (http://skinfaxe.delta.dk/reqsys_public)

Test Scenario

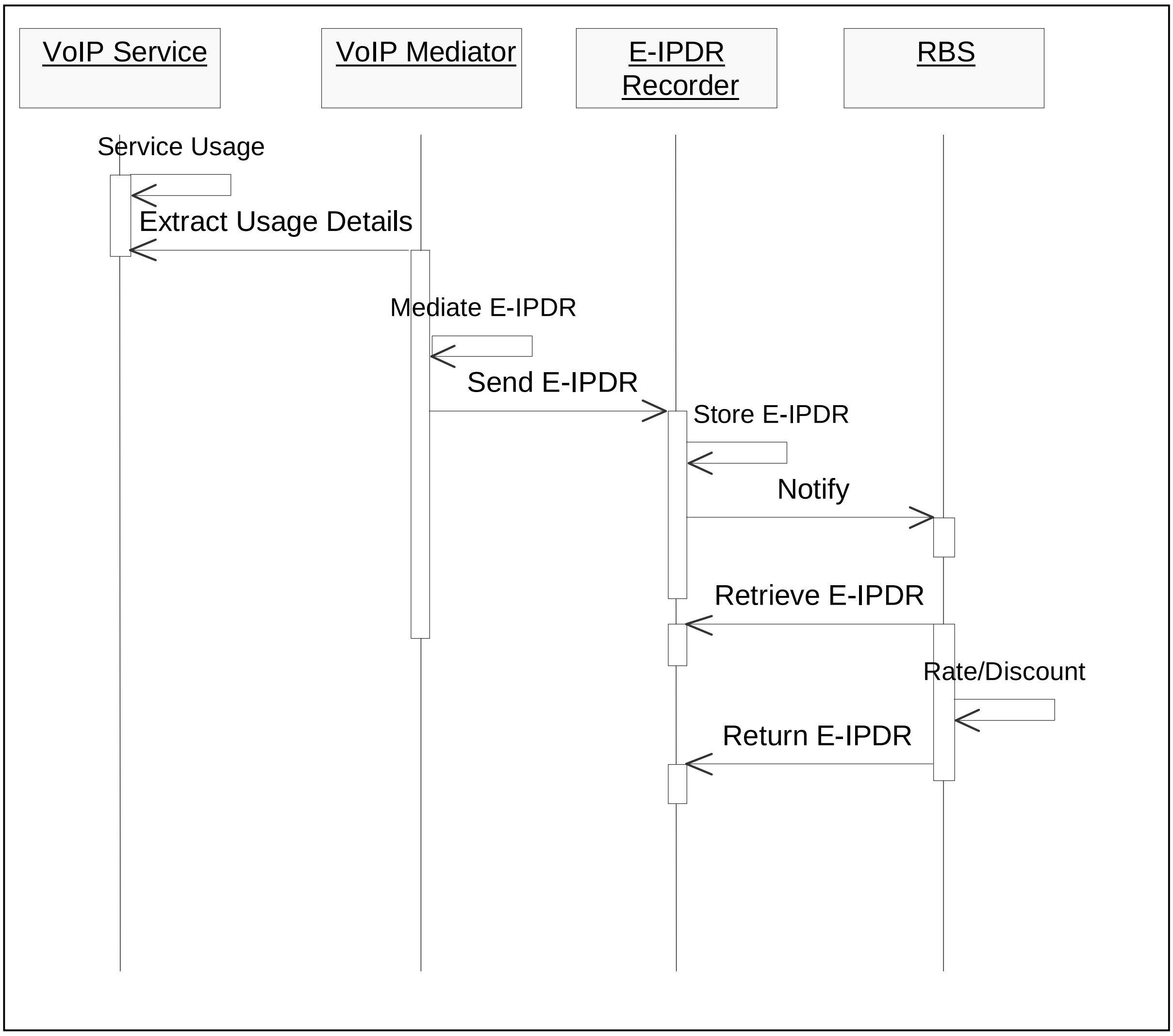


Figure 13: Test case T2-TT4-2.1 Scenario

2.4.2.5 Test Case 2.1: "Rating for a composed service (OCS)"

Test ID:	T2-TT4- 2.2
Event Type:	Local | Common
Location(s):	D/FOKUS
Partners involved:	WIT/FOKUS
Planned Date:	16/11/01
Trial Planner(s):	Ryan/WIT
Trial Evaluator(s):	Ryan, Leray, Brazil, Cloney/WIT
Developer(s):	Brazil,Leray,Cloney,Ryan/WIT, Gringle/FOKUS

Purpose

The purpose of this test case is to:

- Test the provision of an Online Collaboration Service (OCS)
- Test if the E-IPDR recorder can record OCS E-IPDRs and notify the RBS that OCS E-IPDRs require rating
- Test the integration between the VoIP mediator, the FMA, the E-IPDR recorder and the RBS
- Test the ability of the RBS to perform OCS usage discounting
- Test the ability of the RBS to perform OCS customer charge and settlement rating
- Test the ability of the RBS to rate against parameters extracted from VoIP/MediaShop SLAs/SLSs
- Test the ability of the RBS to aggregate the charges for each usage of the constituent services of a composed service (within the composed service accounting session) into a single composed service (OCS) charge.

Pre-conditions

- The RBS and E-IPDR recorder are running
- The E-IPDR database exists
- An SLAs and an SLSs exist for the respective customer and service providers
- The RBS can retrieve SLA/SLS accounting information from the SLA/SLS manager

Post-conditions

- A rated/discounted E-IPDR is generated and stored for each constituent service usage
- A rated/discounted E-IPDR is generated and stored for the OCS single charge

Test Case Success Criteria

- The rated E-IPDRs must exhibit accurate charging/settlement relative to the QoS violations specified in the SLSs/SLAs
- The E-IPDRs contain useful usage information to be later viewed by the customer/service provider
- All rating is achieved in real-time
- The charges/discounts for each of the constituent services are accurately aggregated into a single OCS charge

Related Operational Requirements

The related operational requirements are maintained through the FORM requirements to trials mapping system (http://skinfaxe.delta.dk/reqsys_public)

Test Scenario

See Figure: Test case T2-TT4-1.1 Scenario.

2.4.3 Test Team 4 Conclusions

2.4.3.1 Match Findings/Results with Purpose

One of the objectives of this trial case was to deliver IP services, mediate usage data for the service usages into E-IPDRs and perform rating and discounting on the E-IPDRs. Each of these objectives were fully achieved during the trial. However, the trial did raise the issue of guaranteed delivery of E-IPDRs to the Rating Bureau Service (RBS). The reliability of any such system would heavily depend on the assurance that all usage records are passed for rating and subsequent charging/billing. The failure to guarantee that all records are delivered could result in substantial revenue losses for the IP service providers. Other issues that were not addressed include:

- the security of the records passed between the relevant domains
- stress testing of the RBS for large numbers of records
- real-time capabilities of the RBS
- measurement of overheads due to usage data collection, mediation and delivery
- the communication channel between the RBS and the SLA management system
- the traceability of the audit trail generated

These issues were identified prior to the generation of the trial test cases but were classified as out of scope for the trial. The main objective of the trial was to validate the use of the IPDR as a means for passing usage data between domains and the subsequent investigation of the validity of the addition of a Charge Element to the IPDR schema. The granularity of the information contained in the E-IPDR supported flexible charging encompassing accurate quality of service related discounting.

The Federated Mediation Adaptor (FMA) forms a key component in mediation of aggregated service usage and service value chain. The tests carried on it proved that it must be robust during operation and must maintain consistency of usage data.

Aggregation of a composite usage session and binding it to a set of E-IPDR documents proved to be more difficult than we had earlier envisaged. IPDR specifications do not address this requirement very clearly. Nor do they provide practicable means to implement aggregated service mediation. The means that were devised to meet this requirement were based on the idea of having **parentSession** in Master IPDR Schema. They were successfully tested and proved to be practicable.

2.4.3.2 Requirements Impact

Standards (eg, TMForum, ETSI, IRTF/IETF, IPDR) and recent trends in the industry (Billing solution vendors, etc) were studied to capture the initial requirements. Study of billing business process in general also helped greatly in capturing requirement. Difficulties did arise when we attempted to use useful concepts from organizations such as IRTF/IETF and then tried to provide feed back. Here the research goals and background appears to be the main reasons. IRTF/IETF saw billing processes from point of view of the Internet engineering, and terms such as use cases and business model did not play as important a part as it was in FORM project.

The main driver for addressing the subset of requirements that were met was current telecommunications industry requirements for IP service accounting. As the new IP-based services market expands rapidly, the upsurge in the level of B2B interactions creates new service requirements in the areas of customer service access, security, billing and Quality of Service (QoS). An important feature of the new environment is the creation of composite services (service sets) created from the integration of services provided by ISPs, Virtual Private Network (VPN) and application service providers, as well as backbone operators. In such an environment B2B requirements can no longer be economically met through the provision of non-dependent standalone services. A critical factor in the growth of this environment is addressed by the requirements CB-I.01, CB-I.04, CB-I.08 etc. These requirements describe the need for a standard for the accurate exchange of usage data between these various providers. The trial was concerned with validating the IPDR against these and other related requirements.

Requirements captured and listed under **Abnormal Conditions** did not have considerable impact on the design of BB. However, many of the requirements captured under **Dynamic Functionality** proved to be important and influenced BB design.

Those requirements that did not have considerable impact on BB design did play the role of a set of guidelines with which we tracked the course of development work and later on evaluated the result.

3 Operational Requirements and Test cases

This section of the annex contains data regarding the linkage between Operational Requirements and Test Cases conducted during Trial 2 and was the basis of the D10 main document input relating to operational requirements. The four respective Test Teams entered the test-case data and the linkage to operational requirements in the web-tool and the Operational Requirements were transferred from WP2.

The appendix is organised in the following three main sub-sections:

- *List of all test cases and a description of their main points* (All test-case details can be found in this annex)
- *List of Test Cases and their associated requirements* together with an assessment by the respective test team of the fulfilment degree both concept- and implementationwise.
- *List of all requirements not associated with any test-cases*

3.1 List of Test Cases for Trial 2

Test Case Id	Expressed By	Date Done	Performed By	Present	Main Points
T2-TT1-1	IESP, ISP	2001-12-04	AO/UHC,TT/UCL	AO/UHC, TT/UCL, TG/GMD	The purpose of this test case is to evaluate the functionality of and interaction between the SNE and the SLAR.
T2-TT1-2	IESP,ISP,ASP	2001-12-04	AO/UHC,TT/UCL, TG/GMD	AO/UHC, TT/UCL, TG/GMD	The purpose of this test case is to evaluate the interaction between building blocks, SHS, SNE and SLAR.
T2-TT2-1	IESP,ISP,EC	2001-12-04	SP,LPJ/DLT, HR,BL,IT/LMD, OS,HK/ATOS	ALL	Request VPN Service This test case deals with the creation of the virtual topology for the VPN and allows allows test of the whole interactions necessary for the creation of a VPN Service requested by a VPN Customer. The focus in on 'proof of concept'. The test case concerns creation of the entire virtual topology needed for T2-TT2-3: 'Create VPN Connection'.
T2-TT2-2	IESP,ISP,EC	2001-12-04	SP,LPJ/DLT, HR,BL,IT/LMD, OS,HK/ATOS	ALL	Initiate IPSec-P The purpose is to show integration between VPN-P and IPSec-P and to load the IPSec-P repository with IPSec policy associations defining high-level security service. Focus is on proof-of-concept regarding integration of the

					BBs and mapping of a 'high-level' security component to IPSec specific parameters. NB! Only Requirements nor included by T2-TT2-1 and T2-TT2-3 are included.
T2-TT2-3	IESP,ISP,ASP	2001-12-04	SP,LPJ/DLT, HR,BL,IT/LMD, OS,HK/ATOS	ALL	Create VPN Connection The purpose is to show integration between VPN-P, IPSec-P and GQIPS. Regarding the IPSec-P interactions, the test will add policy rules to the IPSec-P repository for border nodes (CPEs) and to establish the basis for creation of an IPSec secured link between two CPEs. Regarding GQIPS interactions, the test includes bandwidth negotiation process between VPN-P and GQIPS. (GQIPS is running in simulated mode)
T2-TT3-1.1	IESP, EC, ASP	2001-12-04	CGN, JDM / TDC	FORM T2 DELTA participants	Customer Login and Validation. Customer specific information are XML formatted, and the web application uses 'standard' XML techniques to make such information available for the application.
T2-TT3-1.2	IESP, EC, ASP	2001-12-04	CGN, JDM / TDC	FORM T2 DELTA participants	Reporting Template Completition. 'Standard' web programming techniques are used to define 'browser specific' dynamic client pages (templates) to present customer specific information and selected report data. 'Standard' web programming techniques are used to enable generation of 'browser specific' dynamic menu pages with customer specific information and menu options, and customer menu selections are used to initialise search filters for collection of reporting data. Web application detects missing customer client input and add help-messages to the customer menu page.
T2-TT3-1.3	IESP, EC, ASP	2001-11-01	CGN, JDM / TDC	TDC	Report Customisation. Information used for customisation is

					XML formatted, and 'Standard' XML techniques are used to add or change information. Translation to customer client browser mark-up language, can be done by web application or by client browser.
T2-TT3-2.1	IESP	2001-12-13	BC,CH/TCD	BC,VW,CH/TCD,VA,RM,TT/BRI	Production of Assurance Configurations When an SLA is submitted to the assurance system it is necessary to configure the various components of the system to support it. The purpose of this test case is to evaluate how the SLA is processed by the system and to ensure that the correct configurations are produced for distribution to the other components of the system.
T2-TT3-2.2	IESP,ISP,EC,ASP	2001-12-13	BC,CH/TCD,VA,CM/BRI	BC,VW,CH/TCD,VA,RM,TT/BRI	Service Monitoring Once the assurance system has been configured in response to a new SLA the system will begin to monitor the service. This involves a number of different components distributed in the customer, provider and IES domains. Each of the components, called Server Monitors, in the customer and provider domains are responsible for collecting the statistics produced locally and processing them, if necessary, for use by the performance monitor. The performance monitor, in the IES domain, is then responsible for aggregating the statistics into metrics that match those specified in the SLA. The purpose of this test case is to evaluate how this process is currently supported by the system.
T2-TT3-2.3	IESP,ISP,EC,ASP	2001-12-13	BC,CH/TCD,VA,RM/BRI	BC,VW,CH/TCD,VA,RM,TT/BRI	Service Violation Reporting While monitoring a service the assurance system calculates the values of the metrics used within the SLA. However it must also compare the values of these metrics to thresholds specified in the SLA to ensure that it has not been violated. If a violation does occur then the event must be generated to indicate this to interested parties. The purpose of this test case is to ensure that these events are produced and correctly identify the parameters

					that caused the violation to occur.
T2-TT3-2.4	IESP	2001-12-13	BC,CH/TCD	BC,VW,CH/TCD,VA,RM,TT/BRI	Workflow implementation of Business Processes The workflow framework enables flexible management of business processes within a system. The purpose of this test case is to evaluate the implementation of assurance business processes using the workflow framework. The assurance client invokes assurance processes. The workflow framework implements the control flow and data flow for the Building Blocks to implement the processes. Two different assurance processes were tested for configuration of the assurance Building Blocks to support an SLA.
T2-TT3-3.1	IESP, ISP, ASP	2001-12-13	RM,VAE/BRI	RM,VAE,TT/BRI; CH,BC,VW/TCD	B3 Setting
T2-TT3-3.2	IESP, ISP, ASP	2001-12-13	VAE,RM/BRI	TT,VAE,RM/BRI; BC,CH,VW/TCD	Single domain service negotiation
T2-TT3-3.3	IESP, ISP, ASP	2001-12-13	VAE,RM/BRI	VAE,RM,TT/BRI; VW,BC,CH/TCD	Events subscription and notification
T2-TT3-3.4	IESP, ISP, ASP	2001-12-13	VAE,RM/BRI	VAE,RM,TT/BRI; VW,BC,CH/TCD	Multi domain RAR Negotiation
T2-TT4-1.1	IESP, ISP, ASP	2001-11-15	TG/FOKUS, JB/WIT	(BB,TG/FOKUS)(CR,EL,JB,JC/WIT)	Monitoring of Online Collaboration Service Session The purpose of this test case is to verify whether FMA can (federated mediation adaptor)monitor OCS (on-line collaboration service)session, called parentSession, and records its duration in real-time. The OCS session denotes the duration within which the constituent services are used (or, MediaShop and VoIP sessions existed). There is another purpose of this test, which is to verify whether FMA monitors and knows about the services

					(i.e., MediaShop and VoIP service IDs) that are being used as parts of OCS.
T2-TT4-1.2	IESP, IESP, ASP	2001-11-15	TG/FOKUS, JB/WIT	(BB, TG/FOKUS) (CR, EL, JB, JC/WIT)	Usage Mediation of Online Collaboration Service: The MA (Mediation Adaptors) dealing with VoIP and MediaShop services communicate with and transfer service usage data to the FMA (Federated Mediation Adaptors). Data is packaged in E-IPDR documents. The main purpose of this test case is to verify whether the FMA can receive and aggregate the E-IPDR documents in real-time and usage-by-usage manner.
T2-TT4-1.3	IESP, ISP, ASP	2001-11-15	(BB, TG/FOKUS), (CR, EL, JB, JC/WIT)	(BB, TG/FOKUS), (CR, EL, JB, JC/WIT)	Transfer of an OCS E-IPDR document and its utilisation: The purpose of this test case is to verify whether FMA (Federated Mediation Adaptor) is able to send an OCS E-IPDR document to RBS (Rating Bureau Service) and RBS is able to use it in applying appropriate tariffs and calculating charges.
T2-TT4-2.1	IESP, ASP	2001-11-15	(CR, EL, JB, JC/WIT)	ALL	To deliver a VoIP service, mediate usage data for a service usage into an E-IPDR and perform rating & discounting on the E-IPDR

3.1.1 Requirements associated with Test Cases

Test Case ID	Req. ID	Addr.	Conceptwise fulfilment degree	Impl.-wise fulfilment degree	Comment
T2-TT3-1.1	EC-II.20	Partly	Partly Fulfilled	Partly Fulfilled	The web application detects wrong user names and/or passwords. Currently only user help-messages are generated and dynamically added to the users login page.
T2-TT3-1.2	IE-II.7	Partly	Partly Fulfilled	Partly Fulfilled	No scheduling function implemented.
T2-TT3-1.2	MS-II.08	Yes	Fulfilled	Fulfilled	Both fixed and mobile end-customer terminals can be supported.
T2-TT3-1.2	EC-IV.42	Yes	Fulfilled	Partly Fulfilled	Requires that information about end-customer equipment is available to the IESP e.g. by an outsourcing solution.
T2-TT2-1	EC-II.02	Yes	Fulfilled	Out-of-scope	If the 'service' is a VPN Service. The latter should allow for dynamic modification of the VPN connection. This was not planned to be implemented in the scope of FORM.
T2-TT2-1	EC-IV.43	Yes	Partly Fulfilled	Partly Fulfilled	You can recieve information on abnormal conditions through JMS but only during provisioning and activation phase, the 2 phases supported by the VPN service. There is no VPN assurence implemented, only the fulfilment.
T2-TT2-1	SC-II.18	Yes	Partly Fulfilled	Not Fulfilled	Derivation of Security parameters from the SLA is supported by the VPN, but the link between SLA handeling and VPN has not been implemented/tested for T2.
T2-TT2-1	SC-III.19	Yes	Fulfilled	Partly Fulfilled	The VPN system will pass on the policies from the SLA. However, the link to the SLA handling has not been implemented/tested for T2.
T2-TT2-3	EC-IV.18	Yes	Partly Fulfilled	Partly Fulfilled	VPN-P Buliding blocks VPN-SC, VPN-P and IPSec-P has been integrated, but no integration hae been done with end-user applications, except for VPN-P that has been integrated with a 'Administrative Console' application.
T2-TT2-3	EC-II.19	Yes	Partly Fulfilled	Partly Fulfilled	A mapping from 'high-level' to 'low-level' security parameters has been done between the VPN-P and IPSec-P building blocks for Confidentiality, Authentication and

					Authorisation as part of a Service-Class object. However, no prioritasation has been included.
T2-TT2-3	EC-II.22	Yes	Fulfilled	Partly Fulfilled	The test-bed used in Trial 2 emulated two end-customer is different domains/networks for the VPN setup.
T2-TT2-3	EC-II.23	Yes	Fulfilled	Fulfilled	The test-bed used in Trial 2 emulated multiple ISPs between end-customers for the VPN setup, but also a distribution of managements compoennts where shown.
T2-TT2-3	EC-II.37	Yes	Fulfilled	Partly Fulfilled	The protection will be present, but a link to SLA negotiated security level was not implemented.
T2-TT2-3	EC-II.38	Yes	Out-of-scope	Out-of-scope	No VPN assurence was implemented, only fulfilment.
T2-TT2-3	EC-IV.39	no	Partly Fulfilled	Not Fulfilled	This would also require the VPNSP to ensure confidentiality of end-customer data. This can be done, but it has not been addressed in T2.
T2-TT2-3	EC-IV.40	Yes	Fulfilled	Not Fulfilled	Protection of the PDP-PEP communication has not been implemented for T2.
T2-TT2-3	EC-IV.41	Yes	Fulfilled	Fulfilled	Only VPN creation was shown in T2.
T2-TT2-3	EC-IV.42	no	Out-of-scope	Out-of-scope	No VPN assurence was planned and implemented for T2.
T2-TT2-3	EC-II.48	Yes	Partly Fulfilled	Partly Fulfilled	The IPSec policies did contains IP-Filters for hosts behind the CPEs, but they where not utilised during T2.
T2-TT2-3	EC-II.51	Yes	Fulfilled	Fulfilled	Events are avaialable through JMS from all VPNS building blocks.. (Events are also stored in the VPN-P administrative console)
T2-TT2-3	SC-I.04	Yes	Fulfilled	Partly Fulfilled	A mapping between high-level security items and low-level parameters is shown by mapping the service-class onto specific IPSec related parameters. However, a link to the SLA-handler was not implemented for T2.
T2-TT2-3	SC-II.14	Yes	Partly Fulfilled	Partly Fulfilled	
T2-TT2-3	SC-II.18	Yes	Fulfilled	Partly Fulfilled	A VPN Service Class contained a security component describing the security assoicated with a service. However, this was not integrated with the SLA-handling.
T2-TT2-3	SC-III.19	Yes	Fulfilled	Partly Fulfilled	Note: No linkage with SLA-handling implemented for T2.
T2-TT2-3	SC-IV.21	Yes	Fulfilled	Partly Fulfilled	The VPN test-bed contained two end-users on different networks, but no combination with NAT/PAT was shown.
T2-TT2-3	SC-V.23	Yes	Partly	Partly	Events logged through JMS and nade

			Fulfilled	Fulfilled	available in the administrative console.
T2-TT2-3	IE-II.5	Yes	Fulfilled	Partly Fulfilled	Securing og the PDP-PEP management connections were not implemented for T2.
T2-TT3-1.3	MS-II.08	Yes	Fulfilled	Partly Fulfilled	'Standard' XML techniques used to translate XML into other formats. Formats tested include HTML and Scaleable Vector Graphics (XML-SVG) for 'fixed' client terminal browsers, plus WML and XHTML for 'mobile' browsers (WAP). Translation done either by web application or by client browser.
T2-TT2-1	SC-II.15	Yes	Fulfilled	Partly Fulfilled	The VPN system will offer functionality for enabling deletion of VPN services, this has however, not been implemented fully for T2.
T2-TT2-3	MS-II.03	Yes	Fulfilled	Partly Fulfilled	The VPNSP Building Blocks supports this. However, only the connection setup is implemented for T2.
T2-TT2-3	MS-II.04	Yes	Partly Fulfilled	Partly Fulfilled	All VPNP Building blocks provides basic validation of the management operations. However, validation of complex semantics are not implemented for T2.
T2-TT2-3	MS-II.06	Yes	Partly Fulfilled	Partly Fulfilled	IPSec-P and GQIPS supports a notion of 'thresholds', but for IPSec-P, this is not implemented fully for T2.
T2-TT2-3	MS-II.05	Yes	Out-of-scope	Out-of-scope	VPNS implemented for T2 only contains fulfilment, i.e. not VPN assurence was planned/implemented.
T2-TT2-3	MS-II.09	Yes	Partly Fulfilled	Not Fulfilled	VPNS BBs only provides notification on fulfilment events.
T2-TT4-1.1	CB-I.01	Yes	Fulfilled	Fulfilled	
T2-TT4-1.1	CB-I.07	Yes	Fulfilled	Fulfilled	
T2-TT4-1.1	CB-I.08	Yes	Fulfilled	Fulfilled	
T2-TT4-1.1	CB-I.02	Yes	Fulfilled	Partly Fulfilled	
T2-TT4-1.1	CB-II.09	Yes	Fulfilled	Partly Fulfilled	
T2-TT4-1.1	CB-II.11	Yes	Fulfilled	Fulfilled	
T2-TT4-1.1	CB-II.23	Yes	Fulfilled	Fulfilled	
T2-TT4-1.1	CB-II.25	Partly	Partly Fulfilled	Not Fulfilled	
T2-TT4-1.1	CB-IV.30	Yes	Fulfilled	Partly Fulfilled	

T2-TT4-1.1	CB-III.29	Yes	Partly Fulfilled	Partly Fulfilled	
T2-TT4-1.1	CB-V.35	Partly	Partly Fulfilled	Not Fulfilled	Overheads due to usage data collection were not measured.
T2-TT4-1.2	CB-I.01	Yes	Fulfilled	Fulfilled	
T2-TT4-1.2	CB-I.02	Yes	Fulfilled	Partly Fulfilled	
T2-TT4-1.2	CB-I.04	Partly	Partly Fulfilled	Partly Fulfilled	
T2-TT4-1.2	CB-I.07	Yes	Fulfilled	Fulfilled	
T2-TT4-1.2	CB-I.08	Yes	Fulfilled	Fulfilled	
T2-TT4-1.2	CB-II.09	Yes	Fulfilled	Partly Fulfilled	
T2-TT4-1.2	CB-II.11	Yes	Fulfilled	Fulfilled	
T2-TT4-1.2	CB-II.15	Yes	Partly Fulfilled	Partly Fulfilled	
T2-TT4-1.2	CB-II.21	Yes	Partly Fulfilled	Partly Fulfilled	
T2-TT4-1.2	CB-II.23	Yes	Fulfilled	Fulfilled	
T2-TT4-1.2	CB-III.29	Yes	Partly Fulfilled	Partly Fulfilled	
T2-TT4-1.2	CB-IV.30	Yes	Partly Fulfilled	Partly Fulfilled	
T2-TT4-1.2	CB-IV.31	Partly	Partly Fulfilled	Partly Fulfilled	
T2-TT4-1.2	CB-V.35	Yes	Fulfilled	Partly Fulfilled	
T2-TT4-1.2	CB-V.39	Yes	Partly Fulfilled	Partly Fulfilled	
T2-TT2-1	EC-II.07	Yes	Fulfilled	Partly Fulfilled	If the 'service' is a VPN service, the latter could be a third party (VPN Provider) of the IESP, as well the VPN provider could be a customer of the GQIPS (Network Provider). This has been taken into account from the definition of the business model and the impact on the architecture has been well defined in terms of Reference points between the different domains. Thus allowing to implement one-stop shopping paradigm between IESP and its customers. This has been implemented between VPN Service and GQIPS.
T2-TT2-1	EC-II.09	Yes	Partly Fulfilled	Partly Fulfilled	When VPN end user requests the creation of a VPN service or VPN connection, he requests specific service class. This one is mapped to

					specifc QoS metrics and security features which will be used for configuring the service at the network level.
T2-TT2-1	EC-II.25	Partly	Partly Fulfilled	Partly Fulfilled	SLA between the VPN SP and VPN Customer is not defined. However, it is possible to add SAG and SAP to one VPN service and therefore to allow or not some end users to access the VPN service or not.
T2-TT2-1	EC-II.27	Partly	Partly Fulfilled	Out-of-scope	There is no SLA defined between the VPN SP and VPN Customer (IESP), but it is possible from the interface provided by the VPN SP to modify a VPN service or VPN connection. This part has not been implemented.
T2-TT2-1	EC-II.28	Yes	Fulfilled	Partly Fulfilled	Service Class, provided by the IESP to the VPN SP when requesting a VPN Service or VPN connection, includes parameters from negotiated SLA between IESP and IES customer. This QoS parameters are transformed by the VPN service and pass to the GQIPS through a RAR (Resource Allocation Request). QoS parameter supported by GQIPS is bandwidth. Other QOS parameters are defined in the VPN service classes but not implemented by GQIPS.
T2-TT2-1	EC-II.37	Yes	Fulfilled	Fulfilled	Service Class, provided by the IESP to the VPN SP when requesting a VPN Service or VPN connection, includes parameters from negotiated SLA between IESP and IES customer. Some of these parameters allow to define security level. This security level is defined by generic security parameters which are mapped by the VPN service to specific security features supported by tunnelling mechanisms such as IPSec.
T2-TT4-1.3	CB-I.01	Yes	Fulfilled	Fulfilled	
T2-TT4-1.3	CB-I.06	Yes	Partly Fulfilled	Partly Fulfilled	
T2-TT4-1.3	CB-I.07	Yes	Fulfilled	Fulfilled	
T2-TT4-1.3	CB-I.08	Yes	Fulfilled	Fulfilled	
T2-TT4-1.3	CB-II.11	Yes	Fulfilled	Fulfilled	
T2-TT4-1.3	CB-II.15	Yes	Fulfilled	Partly Fulfilled	
T2-TT4-1.3	CB-II.18	Yes	Partly Fulfilled	Partly Fulfilled	
T2-TT4-1.3	CB-II.23	Yes	Fulfilled	Fulfilled	
T2-TT4-1.3	CB-IV.31	Yes	Partly	Partly	

			Fulfilled	Fulfilled	
T2-TT4-1.3	CB-II.09	Yes	Fulfilled	Partly Fulfilled	
T2-TT4-1.3	CB-V.35	Yes	Fulfilled	Partly Fulfilled	
T2-TT2-1	IA-I.01	Yes	Partly Fulfilled	Partly Fulfilled	The VPN group obviously fully supports this idea. The problem is that there does not exist a stable standard and just emerging ones at a very early stage (ITU-T, IETF ppvpn working group). Contract provided by F-VPN to end user is based on draft standard defined by ITU-T (M3208.1 and M3208.3).
T2-TT2-1	IA-I.02	Yes	Fulfilled	Fulfilled	This is requirement is fulfilled by the VPN group thanks to definition of Service Class which are mapped to configuration parameters using policy transformation rules. Service Class defined 2 parts one for QoS and the other for security level.
T2-TT2-1	IE-II.1	Yes	Partly Fulfilled	Partly Fulfilled	Registration with SLA negotiation of end customer is done at IESP level and not VPN service level. However, CPE is configured by IPSec-P for creation and actiation of IPSec tunnel and CPE is also defined in VPN-P real topology.
T2-TT2-1	IE-II.4	Yes	Fulfilled	Partly Fulfilled	Logging of events is done through JMS and a VPN Service User can subscribe to these events. Events are also logged at the VPN-P level (Admin.Console). No VPN user interface has been implemented yet.
T2-TT2-1	IE-III.6	Yes	Partly Fulfilled	Partly Fulfilled	This will be supported by the VPN service only for both processes implemented, i.e. provisioning and activation. Not continous monitoring. Events are today reported to the VPN administrative console only.
T2-TT2-1	SA-I.03	Yes	Fulfilled	Fulfilled	If the service is a VPN Service, then this requirement can be supported by the VPN in terms of dynamic configuration of the VPN service. This is mainly supported for Service Classes as when a VPN user request creation of a VPN service he defines the service class to be used when creating VPN connection.
T2-TT2-1	SA-II.06	Yes	Partly Fulfilled	Not Fulfilled	The FORM VPN service support modification of the provisioning and activation of the service. The VPN service does not implement reporting functions. Modification functions have not been implemented.

T2-TT2-1	SA-II.07	Yes	Partly Fulfilled	Not Fulfilled	Negotiation and Renegotiation of the SLA concerns the IESP. However, renegotiation of the SLA implies for the VPN SP to support modification of a VPN service. This has been defined but not implemented.
T2-TT2-1	SC-I.05	no	Not Fulfilled	Not Fulfilled	No security policies including reaction pattern have been designed.
T2-TT2-1	SC-II.08	Yes	Partly Fulfilled	Partly Fulfilled	Based on the actual design, this is already supported at the VPN (VPN-P/IPsec-P) level. It has to be included in the SLA. However, negotiation of security level when IES customer negotiates with IESP has not been envisaged.
T2-TT2-3	EC-II.02	Yes	Fulfilled	Out-of-scope	If the 'service' is a VPN Service. The latter should allow for dynamic modification of the VPN connection. This was not planned to be implemented in the scope of FORM.
T2-TT2-3	EC-II.07	Yes	Fulfilled	Partly Fulfilled	If the 'service' is a VPN service, the latter could be a third party (VPN Provider) of the IESP, as well the VPN provider could be a customer of the GQIPS (Network Provider). This has been taken into account from the definition of the business model and the impact on the architecture has been well defined in terms of Reference points between the different domains. Thus allowing to implement one-stop shopping paradigm between IESP and its customers. This has been implemented between VPN Service and GQIPS.
T2-TT2-3	EC-II.09	Yes	Partly Fulfilled	Partly Fulfilled	When VPN end user requests the creation of a VPN service or VPN connection, he requests specific service class. This one is mapped to specifc QoS metrics and security features which will be used for configuring the service at the network level.
T2-TT2-3	EC-II.25	Partly	Partly Fulfilled	Partly Fulfilled	SLA between the VPN SP and VPN Customer is not defined. However, it is possible to add SAG and SAP to one VPN service and therefore to allow or not some end users to access the VPN service or not.
T2-TT2-3	EC-II.27	Partly	Partly Fulfilled	Out-of-scope	There is no SLA defined between the VPN SP and VPN Customer (IESP), but it is possible from the interface provided by the VPN SP to modify a VPN service or VPN connection. This part has not been implemented.
T2-TT2-3	EC-II.28	Yes	Fulfilled	Partly Fulfilled	Service Class, provided by the IESP to the VPN SP when requesting a VPN Service or

					VPN connection, includes parameters from negotiated SLA between IESP and IES customer. This QoS parameters are transformed by the VPN service and pass to the GQIPS through a RAR (Resource Allocation Request). QoS parameter supported by GQIPS is bandwidth. Other QOS parameters are defined in the VPN service classes but not implemented by GQIPS.
T2-TT2-3	IA-I.01	Yes	Partly Fulfilled	Partly Fulfilled	The VPN group obviously fully supports this idea. The problem is that there does not exist a stable standard and just emerging ones at a very early stage (ITU-T, IETF ppvpn working group). Contract provided by F-VPN to end user is based on draft standard defined by ITU-T (M3208.1 and M3208.3).
T2-TT2-3	IA-I.02	Yes	Fulfilled	Fulfilled	This is requirement is fulfilled by the VPN group thanks to definition of Service Class which are mapped to configuration parameters using policy transformation rules. Service Class defined 2 parts one for QoS and the other for security level.
T2-TT2-3	IE-II.1	Yes	Partly Fulfilled	Partly Fulfilled	Registration with SLA negotiation of end customer is done at IESP level and not VPN service level. However, CPE is configured by IPSec-P for creation and actiation of IPSec tunnel and CPE is also defined in VPN-P real topology.
T2-TT2-3	IE-III.6	Yes	Partly Fulfilled	Partly Fulfilled	This will be supported by the VPN service only for both processes implemented, i.e. provisioning and activation. Not continous monitoring. Events are today reported to the VPN administrative console only.
T2-TT2-3	SA-I.03	Yes	Fulfilled	Fulfilled	If the service is a VPN Service, then this requirement can be supported by the VPN in terms of dynamic configuration of the VPN service. This is mainly supported for Service Classes as when a VPN user request creation of a VPN service he defines the service class to be used when creating VPN connection.
T2-TT2-3	SA-II.06	Yes	Partly Fulfilled	Not Fulfilled	The FORM VPN service support modification of the provisioning and activation of the service. The VPN service does not implement reporting functions. Modification functions have not been implemented.
T2-TT2-3	SA-II.07	Yes	Partly Fulfilled	Not Fulfilled	Negotiation and Renegotiation of the SLA concerns the IESP. However, renegotiation of the SLA implies

					for the VPN SP to support modification of a VPN service. This has been defined but not implemented.
T2-TT2-3	SC-I.05	no	Not Fulfilled	Not Fulfilled	No security policies including reaction pattern have been designed.
T2-TT2-3	SC-II.08	Yes	Partly Fulfilled	Partly Fulfilled	Based on the actual design, this is already supported at the VPN (VPN-P/IPsec-P) level. It has to be included in the SLA. However, negotiation of security level when IES customer negotiates with IESP has not been envisaged.
T2-TT2-3	EC-IV.43	Yes	Partly Fulfilled	Partly Fulfilled	Some events where available through JMS, but the T2 test-cases focused on a 'normal-path' not so much on error-conditions. There is no VPN assurence implemented, only the fulfilment.
T2-TT2-1	IE-II.3	no	Out-of-scope	Out-of-scope	Management connection between VPN SP and CPE or IESP and VPN SP are not secured.
T2-TT2-3	IE-II.4	Yes	Fulfilled	Partly Fulfilled	Logging of events is done through JMS and a VPN Service User can subscribe to these events. Events are also logged at the VPN-P level (Admin.Console). No VPN user interface has been implemented yet.
T2-TT2-3	SC-II.15	Yes	Fulfilled	Not Fulfilled	It will be possible to terminate a service, but this feature was not implemented for T2. Fokus was VPN creation.
T2-TT2-3	SC-V.22	Yes	Partly Fulfilled	Partly Fulfilled	The VPN system will support dynamic reconfiguration of VPN services.
T2-TT2-1	SC-V.22	Yes	Partly Fulfilled	Partly Fulfilled	The VPN system will support dynamic reconfiguration of VPN services.
T2-TT2-2	EC-IV.41	Yes	Fulfilled	Fulfilled	In fact, this is done by the IPSEC-P Building Block and the VPN service. CPEs are configured by IPSec-P for set up of IPSec tunnels.
T2-TT2-2	SC-II.10	Yes	Out-of-scope	Out-of-scope	For the trial 2 we have assumed that the infrastructure was sufficient by building a sufficient testbed.
T2-TT3-2.1	IA-II.05	Partly	Fulfilled	Partly Fulfilled	
T2-TT3-2.1	IA-II.06	Yes	Fulfilled	Fulfilled	
T2-TT3-2.1	IA-V.17	Yes	Fulfilled	Partly Fulfilled	
T2-TT3-2.1	IA-I.02	Yes	Fulfilled	Fulfilled	
T2-TT3-2.1	IA-I.04	Yes	Fulfilled	Fulfilled	

T2-TT3-2.2	IA-II.10	Yes	Fulfilled	Partly Fulfilled	
T2-TT3-2.2	EC-II.30	Yes	Fulfilled	Partly Fulfilled	
T2-TT3-2.3	IA-II.07	Yes	Fulfilled	Fulfilled	
T2-TT3-2.3	IA-II.08	Yes	Fulfilled	Partly Fulfilled	
T2-TT3-2.3	EC-II.29	Yes	Fulfilled	Partly Fulfilled	
T2-TT3-2.3	IA-III.12	Yes	Fulfilled	Partly Fulfilled	
T2-TT3-2.2	EC-II.22	Yes	Fulfilled	Fulfilled	
T2-TT3-3.1	QA-V.25	Yes	Fulfilled	Fulfilled	
T2-TT3-3.1	QA-V.26	Yes	Fulfilled	Fulfilled	
T2-TT3-3.2	IA-I.02	Yes	Partly Fulfilled	Partly Fulfilled	
T2-TT3-3.2	IA-II.05	Yes	Fulfilled	Fulfilled	
T2-TT3-3.2	IA-II.09	no	Not Fulfilled	Not Fulfilled	
T2-TT3-3.2	IA-V.16	Partly	Partly Fulfilled	Partly Fulfilled	
T2-TT3-3.2	QA-I.01	Yes	Fulfilled	Partly Fulfilled	
T2-TT3-3.2	QA-I.04	Yes	Fulfilled	Partly Fulfilled	
T2-TT3-3.2	QA-II.07	Yes	Fulfilled	Fulfilled	
T2-TT3-3.2	QA-II.09	Yes	Fulfilled	Fulfilled	
T2-TT3-3.2	QA-II.10	Yes	Fulfilled	Fulfilled	
T2-TT3-3.2	QA-II.16	Yes	Partly Fulfilled	Not Fulfilled	
T2-TT3-3.2	QA-II.17	Yes	Not Fulfilled	Not Fulfilled	
T2-TT3-3.2	QA-II.19	Yes	Fulfilled	Fulfilled	
T2-TT3-3.3	IA-II.09	Yes	Not Fulfilled	Not Fulfilled	
T2-TT3-3.3	IA-V.16	Yes	Partly Fulfilled	Partly Fulfilled	
T2-TT3-3.3	QA-II.16	Yes	Partly Fulfilled	Not Fulfilled	
T2-TT3-3.4	IA-I.02	Yes	Fulfilled	Fulfilled	
T2-TT3-3.4	IA-II.05	Yes	Fulfilled	Fulfilled	

T2-TT3-3.4	IA-II.09	Yes	Partly Fulfilled	Not Fulfilled	
T2-TT3-3.4	IA-V.16	Yes	Fulfilled	Partly Fulfilled	
T2-TT3-3.4	QA-I.01	Yes	Fulfilled	Fulfilled	
T2-TT3-3.4	QA-I.04	Yes	Fulfilled	Fulfilled	
T2-TT3-3.4	QA-II.07	Yes	Fulfilled	Fulfilled	
T2-TT3-3.4	QA-II.09	Yes	Fulfilled	Fulfilled	
T2-TT3-3.4	QA-II.10	Yes	Fulfilled	Fulfilled	
T2-TT3-3.4	QA-II.16	Yes	Partly Fulfilled	Partly Fulfilled	
T2-TT3-3.4	QA-II.17	Partly	Not Fulfilled	Not Fulfilled	
T2-TT3-3.4	QA-II.19	Yes	Fulfilled	Fulfilled	
T2-TT2-3	EC-II.20	Yes	Out-of-scope	Out-of-scope	The system does not provide assurence of the VPN links established only the provisioning.
T2-TT2-3	EC-II.45	Yes	Out-of-scope	Out-of-scope	The assumption for TT2 in T2 is that the CPEs are already installed and at the border. (Experiments whith this was conducted as part of trial 1)
T2-TT2-2	SC-I.06	Yes	Out-of-scope	Out-of-scope	The assumption in T2 for TT2 was that CPEs are deployed at 'borders' and belongs to the service provider.
T2-TT2-2	SC-I.07	Yes	Out-of-scope	Out-of-scope	The assumption in T2 for TT2 was that CPEs are deployed at 'borders' and belongs to the service provider.
T2-TT2-3	SC-III.20	Yes	Out-of-scope	Out-of-scope	The F-VPN system applies only fulfilment not assurence for T2.
T2-TT2-3	SC-II.17	no	Not Fulfilled	Not Fulfilled	
T2-TT2-2	SC-II.13	Yes	Fulfilled	Partly Fulfilled	The CPE--Management system communication is intended to be COPS compliant, though not fully implemented for T2. (This is standardised and contains simple form of authentication).
T2-TT2-2	SC-II.12	Yes	Out-of-scope	Out-of-scope	The assumption in T2 for TT2 was that CPEs are deployed at 'borders' and belongs to the service provider.
T2-TT2-2	SC-II.11	Yes	Out-of-scope	Out-of-scope	
T2-TT2-2	IE-II.3	Yes	Partly Fulfilled	Not Fulfilled	Management connection between VPN SP and CPE or IESP and VPN SP are not implemented as secure for T2. However, experiments with SSH tunneling was

					conducted.
T2-TT4-2.1	CB-I.01	Yes	Fulfilled	Fulfilled	Achieved using an Extension to the IPDR.org NDM-U V2.6
T2-TT4-2.1	CB-I.02	Partly	Partly Fulfilled	Partly Fulfilled	The test did not address Service design and performance improvement
T2-TT4-2.1	CB-I.03	no	Not Fulfilled	Not Fulfilled	
T2-TT4-2.1	CB-I.04	Yes	Fulfilled	Fulfilled	The IESP specified the E-IPDR as the granularity required
T2-TT4-2.1	CB-I.05	Yes	Fulfilled	Fulfilled	The granularity of the usage data is high enough to support accurate usage charging/discounting and customer reporting.
T2-TT4-2.1	CB-I.06	Yes	Not Fulfilled	Not Fulfilled	very accurate usage data is required
T2-TT4-2.1	CB-I.07	Yes	Fulfilled	Fulfilled	
T2-TT4-2.1	CB-I.08	Yes	Fulfilled	Fulfilled	IPDR and TMF
T2-TT4-2.1	CB-II.09	Yes	Fulfilled	Fulfilled	
T2-TT4-2.1	CB-II.10	Yes	Fulfilled	Fulfilled	
T2-TT4-2.1	CB-II.11	no	Out-of-scope	Out-of-scope	
T2-TT4-2.1	CB-II.12	no	Out-of-scope	Out-of-scope	
T2-TT4-2.1	CB-II.13	no	Out-of-scope	Out-of-scope	
T2-TT4-2.1	CB-II.14	Partly	Partly Fulfilled	Partly Fulfilled	
T2-TT4-2.1	CB-II.15	Yes	Fulfilled	Fulfilled	
T2-TT4-2.1	CB-II.16	no	Out-of-scope	Out-of-scope	
T2-TT4-2.1	CB-II.17	Partly	Partly Fulfilled	Partly Fulfilled	Introduced in rating but an interface to manipulate the tariffs was not developed/designed
T2-TT4-2.1	CB-II.18	Partly	Partly Fulfilled	Partly Fulfilled	All rating that was performed was performed in real time, however the implentation of the system ina realtime muli service provider environment was not trialed.
T2-TT4-2.1	CB-II.19	no	Not Fulfilled	Not Fulfilled	this requirement was fulfilled in T1 and was omitted from T2 on this basis.
T2-TT4-2.1	CB-II.20	no	Not Fulfilled	Not Fulfilled	as above
T2-TT4-2.1	CB-II.21	Yes	Fulfilled	Fulfilled	3 Phase discounting was demonstrated
T2-TT4-2.1	CB-II.22	no	Out-of-scope	Out-of-scope	

T2-TT4-2.1	CB-II.23	Yes	Fulfilled	Fulfilled	IPDR standard was used
T2-TT4-2.1	CB-II.24	Partly	Partly Fulfilled	Partly Fulfilled	All rating was based on accounting data extracted from prescribed SLAs/SLSs, however no negotiation mechanism was introduced i.e. SLAs/SLSs were hard coded.
T2-TT4-2.1	CB-II.25	no	Not Fulfilled	Not Fulfilled	
T2-TT4-2.1	CB-II.26	Partly	Partly Fulfilled	Partly Fulfilled	A Service Level Specification was hard coded for each service. SLAs were than based upon the parameters specified in the SLSs
T2-TT4-2.1	CB-III.27	no	Out-of-scope	Out-of-scope	
T2-TT4-2.1	CB-III.28	no	Out-of-scope	Out-of-scope	
T2-TT4-2.1	CB-III.29	no	Out-of-scope	Out-of-scope	
T2-TT1-2	EC-III.01	Yes	Fulfilled	Fulfilled	
T2-TT1-2	EC-II.02	Yes	Fulfilled	Partly Fulfilled	
T2-TT1-2	EC-II.07	Yes	Fulfilled	Partly Fulfilled	
T2-TT1-2	EC-II.08	Partly	Partly Fulfilled	Not Fulfilled	
T2-TT1-2	EC-II.19	Partly	Partly Fulfilled	Out-of-scope	
T2-TT1-2	EC-II.20	Partly	Partly Fulfilled	Out-of-scope	
T2-TT1-2	SA-II.04	Partly	Partly Fulfilled	Not Fulfilled	
T2-TT1-2	SA-I.03	Partly	Fulfilled	Not Fulfilled	
T2-TT1-2	QA-I.01	Partly	Partly Fulfilled	Out-of-scope	
T2-TT1-2	SC-II.08	Partly	Partly Fulfilled	Out-of-scope	
T2-TT1-2	SC-II.09	no	Out-of-scope	Out-of-scope	
T2-TT1-1	EC-II.03	Yes	Fulfilled	Partly Fulfilled	
T2-TT1-1	EC-II.28	Partly	Partly Fulfilled	Out-of-scope	
T2-TT1-1	QA-II.07	Partly	Partly Fulfilled	Out-of-scope	

T2-TT1-1	QA-II.08	no	Out-of-scope	Out-of-scope	
T2-TT1-1	QA-II.09	no	Out-of-scope	Out-of-scope	
T2-TT1-1	QA-II.10	no	Out-of-scope	Out-of-scope	
T2-TT1-1	QA-II.12	Yes	Fulfilled	Fulfilled	

3.1.2 Requirements NOT associated with Test Cases

Req. ID	Expressed By	Functionality Block	Description
SA-II.05	IESP	SA	On-line/Off-line SLA negotiation. SLA negotiation can take place both off-line and on-line, depending on the type of service being ordered. It should be possible to negotiate on-line services requiring little customisation.
QA-I.03	IESP	QA	QoS metrics. The SLA contract should define the metrics for assessing the agreed QoS.
EC-II.04	EC	SA	A SLA or SLA negotiation process should contain mechanisms, such as electronic signature, certificate that will allow the SLA to become legally binding,
EC-II.05	EC	SA	Security mechanisms, such as encryption and authentication, should be applied to the SLA and SLA negotiation process in order to ensure that the SLA is only accessible to agreed parties.
EC-II.06	EC	SA	It should be possible to specify through the SLA the time it takes to deploy the service.
EC-II.10	EC	CB	The service contract should lay down fees and tariffs for the service.
EC-II.11	EC	CB	The service contract should contain the penalty clauses for failure to maintain the SLA commitments as well as provision for cancellation fees.
EC-II.12	EC	CB	Inter-Enterprise Service Provider should provide the customers with flexible choices in receiving and paying bills. The main idea behind making billing process flexible is to cut costs through a greater control over service usage. Hot billing or real-time billing: Customer may want to receive bills within a few minutes of the end of service usage.Bills on Demand: Customers may want to receive bills at any time after the end of service usage.Regular and timely billing: Customers may want to receive bills at a regular interval (e.g., quarterly, monthly, weekly, etc).
EC-II.13	EC	CB	Service-sensitive billing. The key issue here is the distribution of total cost among various departments that a business may have.
EC-II.14	EC	CB	Bill suited to data analysis needs. Customers want to incorporate charges and discounts into their budgets through spreadsheet or any other data analysis software. To this end, customers may expect from their IESPs to customise the billing information to suit their data analysis needs.
EC-II.15	EC	CB	Details of information in a bill. IESPs should allow customers to choose the level of details to which charging information should be specified. This requirement may vary from customer

			to customer and will largely depend on customers' organisational structure and their internal billing procedure. Level of details can be agreed upon during signing SLA. Examples of this are: Distribution of service usage between peak-time and off peak-time, Information on top ten service users (or top ten services used) per department or company.
EC-II.16	EC	CB	Paying of bill independent of who initiates service. Service customers need to be able to specify in the SLA, which of the participants in a service (e.g. a network) is to pay for the service. In most services today it is automatically the person or organisation who orders the service (or the one who initiates the connection) that gets billed, and it is not possible to have the bill sent to the recipient instead. This needs to be flexible.
EC-II.17	EC	SC	The user (application service developer) requires access to COTS building blocks that will allow automated outsourcing of management tasks to Inter-Enterprise Service Provider.
EC-II.21	EC	SC	It should be possible to specify an exit agreement, defining which information will be transferred to the service customer when the outsourcing relationship is terminated.
EC-II.24	EC	GE	The management service should support both mobile (dial-in) and fixed participants.
EC-II.26	EC	GE	The service should offer as many unique permanent IP-addresses to any End Customers as the customer demands (e.g. a unique address to each piece of equipment on the customers' internal network).
EC-II.31	EC	QA	The end-user should have access to tools that will allow them to assess the end-to-end QoS, e.g. maximum response time.
EC-II.32	EC	CB	Cost reporting. The end-user should receive, scheduled or on demand, service logs, on e.g. accumulated cost.
EC-II.33	EC	CB	Web-based billing. According to Billing magazine (issue 3, Jan/Feb 2000) (www.billingmagazine.com), which carries a report on where the billing market place is heading, web-based billing tops the priority list service providers. Service providers surveyed included fixed phone operators, mobile phone operators, cable operators, ISPs, and satellite communication operators. This demonstrates the importance of electronic commerce and rise of EBPP (Electronic Bill Presentment and Payment). Web-based billing is gaining prominence among business customers, who prefer to deal with bills electronically (i.e., email, Web, etc). Private customers prefer Web-based bills that retain the format of the paper bills.
EC-II.34	EC	CB	Consolidated billing. Business customers, who travel frequently and use different types of services for personal and business use, would definitely prefer to receive and pay a consolidated bill of the services they use. Customer expect that ISPs and ASPs providing various services and operating is different zones exchange charging and billing information of the service usage in their zone. The customer is presented with a consolidate bill. In this case, customers subscribe to an IESP, which can act as a retailer for ISPs and ASPs, who in turn offer

			their wholesale services to the IESP. There can be two ways by which bills can be consolidated, depending on what role an IESP assumes:IESP in a role of retailer: IESP does not do repackaging of application services and acts merely as a retailer. Customers are to choose and use from various services that are offered by IESP. ASPs send their charging information to the IESP, where a final consolidated bill is prepared. The IESP can combine all the bills and give customers the advantage of a single billing view for all their bills.IESP in a role of re-packager: IESP bundles attractive applications services of various ASPs and offers the composite (bundled) services to customers on subscription basis. Customer receives a single consolidated bill of application services. Business driver for this billing is that a greater aggregation of services, bundling of services into packages that can be billed as single entity, simplifies the billing process and in particular makes business much easier for customer. Aggregation also helps the service providers by allowing for differentiation based on service packages. The winner will be those IESPs who can identify attractive service bundles (service packages) that can be offered on a subscription basis to users.Consolidated bill: Irrespective of IESPs role, the customers may want to see the following pieces of information included in the bill for ISPs or ASPs who provided the service:Names of ISPs and ASPsService providedDurationCost Discount
EC-II.35	EC	CB	Bill query. The queries on the bill can also be determining factor of customer satisfaction. There are overwhelming evidences from other types of service provider (such as PSTN and GSM). Premium Internet services as well as trends and Internet service market are relatively difficult to comprehend for customers. Owing to these facts, the customers would like to clarify information provided in bill from their IESP. The tips for IESP is to have information readily available in order to respond promptly to customers’ queries.
EC-II.36	EC	CB	Paying of bill independent of who initiates service. The End Customer must be able to select who is billed independently of who initiates the service.
EC-II.46	EC	SC	It should be possible to gain secure access to equipment located behind a firewall through the firewall without making changes to the firewall.
EC-II.47	EC	SC	It should be possible to gain secure access to equipment located behind a firewall without making changes to the firewall, even if the access is made from an IP-address, that is not known until connection is requested, and which changes each time connection is made (dynamic IP-addresses, relevant if accessed e.g. from a mobile computer).
EC-II.49	EC	SC	It should be possible to guarantee that only authorised personnel gain access to a given piece of equipment.
EC-II.50	EC	SC	It should be possible to specify different privileges (e.g. read only, read and modify data, read and modify software), for different authorised personnel, to avoid intentional or unintentional obstruction of the normal operation of the

			equipment.
EC-IV.44	EC	SC	The IESP is responsible for assuring a certain level of security.
SA-I.01	IESP	SA	SLA contents. The offer that is proposed by the provider to the customer should contain all the information necessary for negotiation of the SLA, at least all the technical and financial aspects (not the legal aspects).
SA-I.02	IESP	SA	SLA terminology. The SLA must be formulated in clear and unambiguous terms that the particular customer can understand and agree to. SLA negotiation must consider customers as an entity without great knowledge on technological issues who wish to outsource much of the technical issues concerning communication link management in order to concentrate on their main business processes
SA-IV.08	IESP	SA	One-Stop SLA negotiation. The customer should not need to know what other service providers are involved in delivering the service(s) negotiated in the SLA.
IA-I.03	IESP	IA	Policy Vocabulary Mappings. The QoS Assurance system must process the SLAs it is asked to support into a coherent system policy that can then be distributed to the various elements that make up a service (see the Policy Creation requirement below). However the form of the produced policy will depend heavily on what the underlying systems can support. It is necessary, therefore, for mappings to be stored which specify how the policy produced by the system may be translated into other formats.
IA-III.11	IESP	IA	Resource Adaptation. In the event of an error occurring, or perhaps even circumstances that indicate an error is imminent, the system should try and adapt its resource usage, that is change the system policy, in such a way as to negate the effects of the error transparently to the user of the service. For example in the simplest case it may be possible to simply use a secondary link to a network if the primary link goes down. It should be noted however that even if an error were dealt with in such a manner it would still be necessary for a notification to be produced.
IA-IV.13	IESP	IA	Heterogeneity. The finished system should be able to interface with many different underlying policy systems. This will allow it to be placed on top of existing management structures with a minimum of changes having to be made.
IA-IV.14	IESP	IA	Utilisation. The aim of every service provider is to make sure that their service is utilised as much as possible as this will produce more money in relation to the amount they spent on provisioning the service. Therefore one of the aims of this system will be to ensure that the system policy is constructed in such a way that the utilisation of the underlying service elements is as close to 100% as possible before any new SLA requests are denied.
IA-V.15	IESP	IA	QoS Management Policy. During both the process of policy creation and resource adaptation certain decisions will need to be made about which underlying resources to use and how

			heavily to load these resources. It is therefore necessary to provide a management interface which will allow the system manage to specify the policies about which resources to give preference to. For example such policies might be created on the basis of cost, giving preference to the cheaper resources, or security, giving preference to elements on secure networks.
QA-I.02	IESP	QA	Other parameters negotiation. The SLA negotiation process should allow negotiation of service information between ISPs, e.g. customer care information, service code identification, recovery behaviour, Authorisation, Authentication and Accounting (AAA) policies, out-of-profile traffic handling. This negotiation process is bilateral.
QA-I.05	IESP	QA	Charging compatibility. The QoS model should be able to deal with current and future aspects of charging for QoS.
QA-I.06	IESP	QA	Services availability. Different application categories / service levels should be available to end-users. It might be possible to choose the service inside a catalogue, or to request for specific QoS parameters.
QA-II.11	IESP	QA	Negotiated QoS fulfilment. End-user traffic should be policed and transported according to the SLA negotiated QoS level.
QA-II.13	IESP	QA	IETF compliance. Policing and policy storage should use IETF standards.
QA-II.14	IESP	QA	Measurement operations. Measurement (of e.g. delay, jitter, and loss) operations ensure that the network is meeting the required QoS, and report to the information service level.
QA-II.15	IESP	QA	End-user measurement monitoring. The end-users should have access to tools that will allow them to assess the end-to-end QoS.
QA-II.18	IESP	QA	Scalability. The QoS model should be scalable. In particular it should handle aggregate traffics rather than individual ones.
QA-III.20	IESP	QA	QoS failure report. In case of QoS failure the following information should be provided: number of customers affected; details of which customers are affected; difference between requested and delivered QoS; severity level of failures; times of the failures; why the failures occurred; how failures can be rectified; this may be automated; which customers have priorities, i.e., which can be dropped first?
QA-III.21	IESP	QA	QoS degradation report. The end-user should receive alarms/trouble reports, on e.g. service interrupts; service degradation.
QA-III.22	IESP	QA	Internet2 QBone initiative compliance. The QoS model will be Internet2 QBone initiative compliant.
QA-IV.23	IESP	QA	ISP credentials. Agreements with ISPs in order to form a trusted relationship with them.
QA-IV.24	IESP	QA	IESP credentials. Agreements required for an ISP to negotiate with an Inter-Enterprise Service Provider at a hierarchical level above them.

CB-IV.32	IESP	CB	Cost Allocation Schemes. Cost allocation schemes must be used to improve inefficient services and to optimise efficient ones.
CB-IV.33	IESP	CB	Capacity Planning. By knowing where the cost centres are where the sources of revenue, the capacity of an organisation can be well managed.
CB-V.34	IESP	CB	Principal computing overheads involved. Charging and billing operation must not incur data processing overheads (mainly due to measuring usage, maintenance, and security).
CB-V.36	IESP	CB	Maintenance Overheads. The overheads incurred due to the resources that are needed to maintain the charging record database, generating reports, and issuing bills must be minimal.
CB-V.37	IESP	CB	Security Overheads. Charging services create records from detailed information on subscribers' service usage patterns, which, in turn, may reflect subscribers' behaviour. Hence it is necessary to have mechanisms deployed to protect charging information from unauthorised access and alteration. If security mechanisms are deployed charging data collection and billing processing services, it will increase the overall running costs.
CB-V.38	IESP	CB	Administration policy for usage-sensitive charging and billing. If service providers wish to put in place an administration policy for cost recovery and generating revenue, they must be able to apply usage-sensitive charging and billing. Financial regulations and subscribers' demands for QoS with low or irregular usage patterns may actually be decisive factors in opting for usage-sensitive billing. Usage-sensitive charging and billing may benefit low-volume service users who are concerned with QoS. Usage-sensitive charging may be needed to impose usage quotas, which can be based on service usage parameters.
SC-I.01	IESP	SC	Authentication of End-Users. A set of End-Users that can be authenticated must be derived from the service subscription.
SC-I.02	IESP	SC	Authentication of IESP. The IESP must allow End-Users to authenticate the IESP, possibly by maintaining a certificate signed by a Certificate Authority (CA).
SC-I.03	IESP	SC	Business Interfaces for Feedback. A set of (Business) Interfaces must be compiled from the SLA to where status information concerning security (e.g. security violation alerts, audit trails, etc) can be fed back to (or made accessible to) the End Customer. Business interfaces for feedback can be telephone/fax numbers, e-mail addresses, web-services, etc.
SC-II.16	IESP	SC	Subscribing/unsubscribing End-Users. It must be possible to subscribe/unsubscribe End-Users if sufficient Management Rights are present.
IE-II.2	IESP	IE	Confidence of end-customer information. IESP requires management functions which handles confidence of end-customer information
IE-II.10	IESP	IE	Standardised management. Equipment independent

			management functions.
IE-III.8	IESP	IE	Automatic handling. IESP requires management functions that automate handling of messages e.g. alarms sent from managed equipment, and support distribution of such messages.
IE-IV.9	IESP	IE	Security. IESP requires state of the art security systems and high-level security certifications.
MS-II.01	MS	MS	Repository for end-customer information. MSP requires components enabling use of common repository for end-customers information.
MS-II.02	MS	MS	Access to repository. MSP requires components securing access to repository for end-customers information.
MS-II.07	MS	MS	On-demand status or statistics. MSP requires components which support on-demand and on schedule collection of status or statistics of end-customer equipment.
MS-II.11	MS	MS	Translation of management operations. MSP requires components that can translate equipment independent management operations to equipment- and location specific management operations.