Contract No. 004420

eu-DOMAIN - enabling users for
Distance-working & Organizational Mobility
using Ambient Intelligence Networks

D5.1 Communication architecture description

Specific Targeted Research or Innovation Project

Project start date 1st June 2004 **Duration 36 months**

Published by the eu-DOMAIN Consortium
Lead Contractor TID

18 April 2006 Version 3.0

Project co-funded by the European Commission
within the Sixth Framework Programme (2002 -2006)

Dissemination Level: Restricted

Document file: D5.1_Communication_architecture_description_v3.0.doc

Work package: WP5 – Communications infrastructure

Task: T5.1 + T5.2

Document owner: Pablo Antolín (TID)

Document history:

Version	Author(s)	Date	Changes made
0.9	Pablo Antolín (TID), Almudena Vicente (TID) Sara Carro Martínez (TID)	23-02-2006	First version
1.0	Pablo Antolín (TID), Almudena Vicente (TID) Sara Carro Martínez (TID)	22-03-2006	Second version
2.0	Pablo Antolín (TID), Almudena Vicente (TID) Sara Carro Martínez (TID)	04-04-2006	Deliverable rewritten (Third version)
3.0	Pablo Antolín (TID) Almudena Vicente (TID) Sara Carro Martínez (TID)	18-04-2006	GPS, Tetra discussion and Server security incorporated. Final version submitted to the EC.

Review history:

Reviewed by	Date	Validated
Jesper Thestrup (In-JET)	23-03-2006	
Javier Cámara Melgosa (SAG)	27-03-2006	
Jesper Thestrup (In-JET)	11-04-2006	
Franco Chiarugi	13-04-2006	

Index:

Figures:

1. Executive Summary

1.1. The purpose of this document

This deliverable describes the communication architecture to be adopted by eu-DOMAIN prototypes. It presents different technologies and decides the ones to be used in the platform. The purpose of the work has been to establish the overall communication structure and the constraints of the platform in order to have a solid foundation for the implementation work.

The communication infrastructure is the basis of the communication patterns illustrated in the combined deliverable D3.1 and D4.1 that provides a complete overview of the software architecture of eu-DOMAIN.

1.2. Contents of this deliverable

The deliverable presents an overview of the software architecture as ground to build the communication architecture infrastructure. It also identifies the requirements from WP2 related to communication issues, and tries to identify solutions for those requirements. This is not a validation of the requirements but an analysis.

Then, the communication architecture is discussed, regarding high level protocols and communication patterns and physical links.

Finally, security issues are presented. Although security architecture is further discussed in other deliverable, in here, high-level security issues regarding communications are shown.

An appendix with a review of communication technologies is also provided.

1.3. Reader prerequisites

The reader is assumed to be familiar with the referenced deliverables of eu-DOMAIN and UML notation.

2. eu-DOMAIN Software Architecture Overview

This chapter is included so as to identify the communication requirements and patterns which are derived from eu-DOMAIN software architecture defined during the project. The content of D3.1+4.1 is taken as basis.

The communication architecture is based on the client and server software architecture, which is also supported by the functional and security requirements as outlined in D2.1 ("User validation framework plan") [eu-DOMAIN D2.1, 2005], D2.3 ("Functional user requirements") [eu-DOMAIN D2.3, 2005], and D2.4 ("Trust and security user requirements") [eu-DOMAIN D2.4, 2004] of the eu-DOMAIN project. It is assumed that the readers of this document are familiar with these deliverables.

Figure 1 shows the most high-level overview of the eu-DOMAIN platform. The notation used is UML deployment diagrams. Here, main nodes of the architecture infrastructure are shown as well as the links established among each one by means of software links.

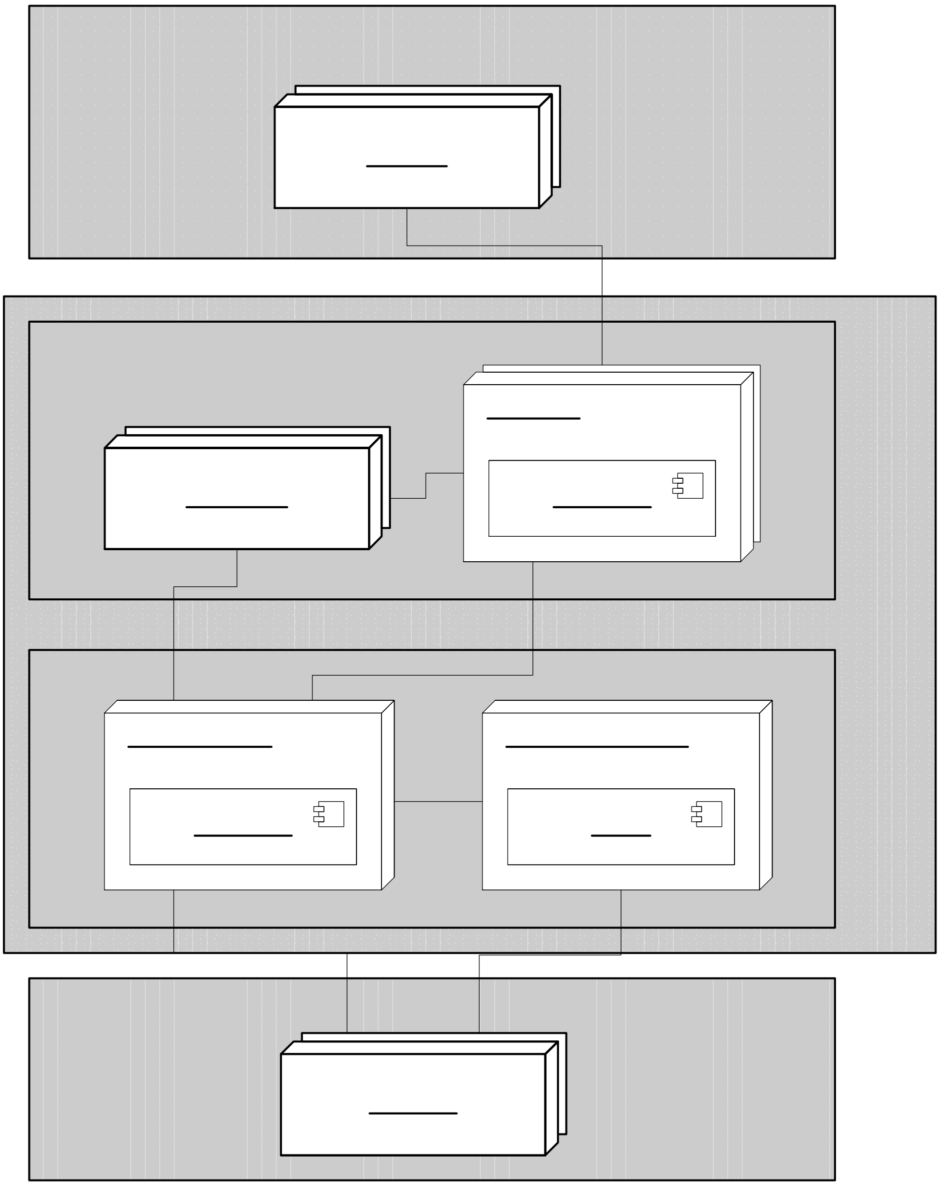


Figure 1: eu-DOMAIN Platform Overview

From Figure 1, communication paths which are needed so as to deploy eu-DOMAIN software architecture can be derived. Based on this knowledge, a description of the communication architecture is provided in following sections. In order to fulfil this task, the entire layout of communication infrastructure will be analysed and the following routes will be established:

- Between Client Gateway and Server Park
- Between Terminals and Server Park
- Between Terminals and Client Gateways, taking into account mobile terminals (using the Client Gateway as proxy/router to acquire connection with the Server Park)
- Between Devices and Client Gateways
- Between Server Park and External Content Providers
- Among software agents in the Server Park

All of these routes are mandatory to allow a correct performance of eu-DOMAIN platform. This means that network connectivity is crucial. Basically, fixed and mobile networks will be used in order to provide communication issues among the components of eu-DOMAIN platform. Depending on the situation of the element to communicate, one type of network, and no other one will be chosen to allow communication in eu-DOMAIN. It is needed to identify the potential and benefits of each approach with respect to eu-DOMAIN needs. Moreover, communication infrastructure specification will take into account constraints derived from hardware component features. For instance, client gateways will have to manage different communication protocols as eu-DOMAIN does not assume any specific protocols on behalf of devices. This means, for example that if a device uses Bluetooth as communication channel, the Client Gateway has to include a Bluetooth adaptor to perform that communication.

Each of the needed communication routes are shown in detail in Figure 2 and Figure 3**Error! Reference source not found.**, which depict an overview of the eu-DOMAIN Server and Client Tier respectively.

In following sections, technologies to be used to fulfil communication requirements are studied and detailed and the eu-DOMAIN communication infrastructure is provided.

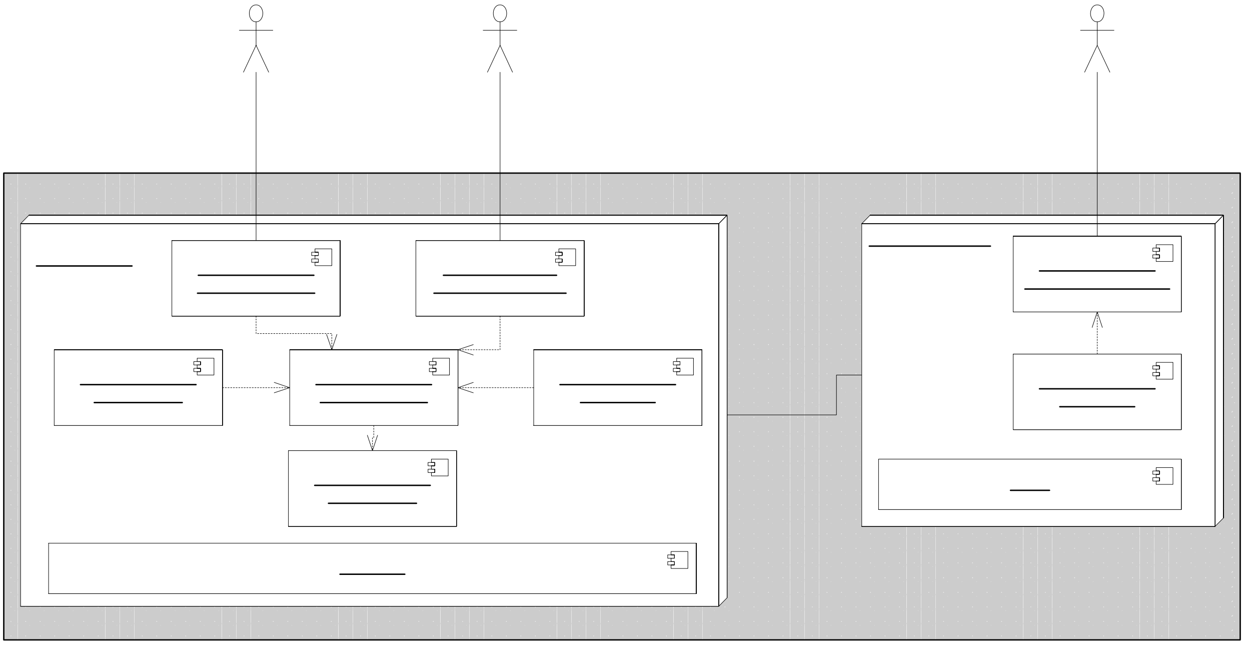


Figure 2: Overview of the Eu-DOMAIN Server Tier

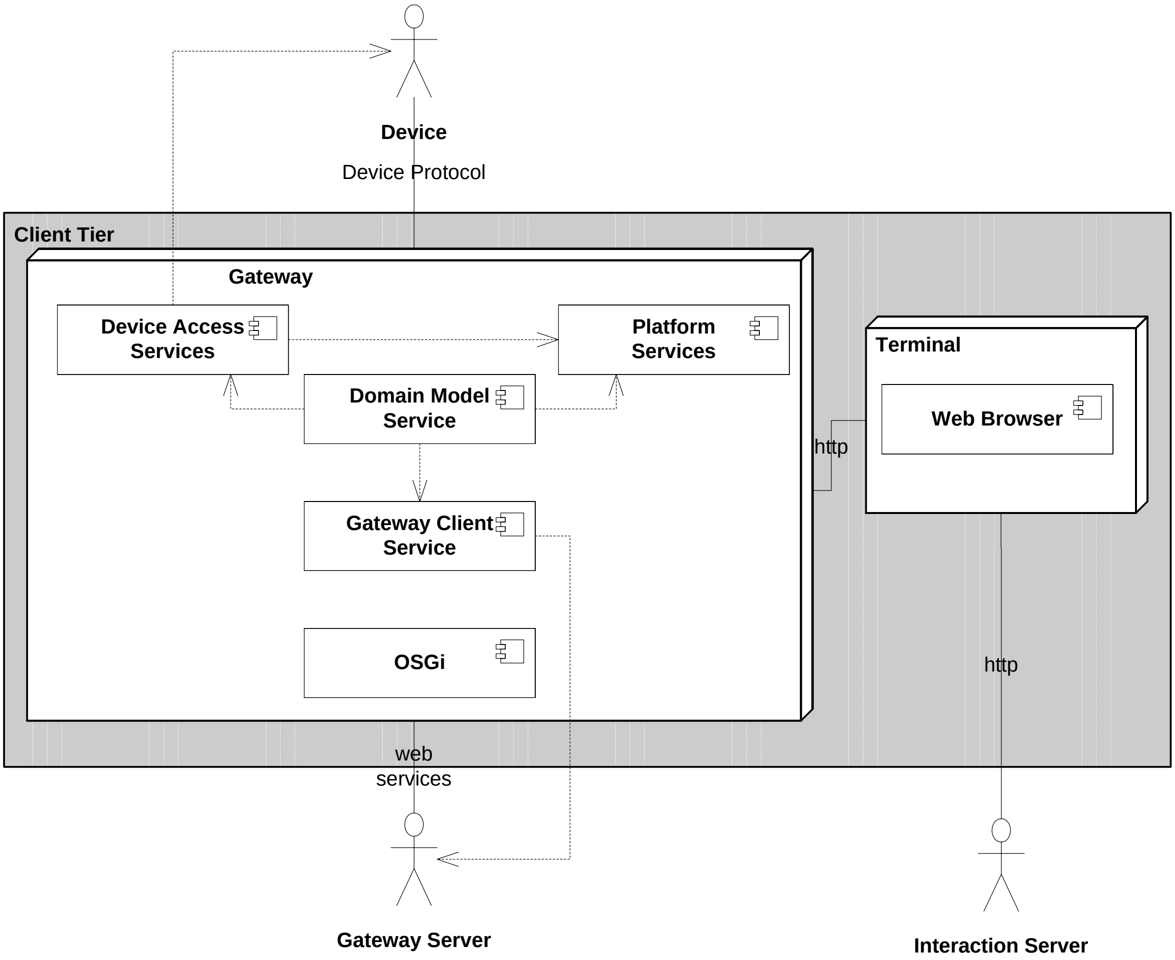


Figure 3: Overview of Eu-DOMAIN Client Tier

3. Requirements

Figure 4 shows the overall process of communication architecture design in eu-DOMAIN in simplified form. In reality this process is iterative, incremental, and artefacts are worked on in parallel. Functional requirements have been described in D2.1 ("User Validation Framework Plan") [eu-DOMAIN D2.1, 2005] as scenarios and in D2.3 ("Functional User Requirements") [eu-DOMAIN D2.3, 2005] as use cases

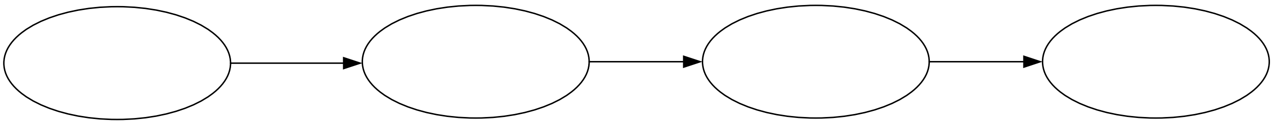


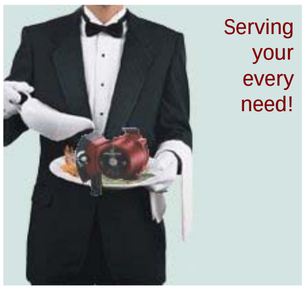
Figure 4: Simplified flow of architectural design process.

The significant functional requirements form the communication architectural requirements for eu-DOMAIN upon which the software architecture has been designed. These are described in Section 3.1.

3.1. Functional Requirements

Of the eu-DOMAIN scenarios, two have been chosen as central to the implementation of the eu-DOMAIN platform. These are the European Service Network scenario "Serving your every needs!" (D2.1 [eu-DOMAIN D2.1, 2005], pp. 29-30: henceforth the "ESN" scenario):

In a world where customers are the primary driving force in shaping product characteristics, features and use of pumps, combined with the existence of a sophisticated communication infrastructure, i.e. the eu-DOMAIN, the basic product function of a pump will shift from simply moving water (or fluids) to be an integral, maybe even a crucial part, of the customers solution. The value created by the "ambient intelligence" functionality of the pump becomes a major part of the customers overall value creation. The pumps are "serving you – wherever you are – whatever you do – whenever you want it".
We call this scenario: "Serving your every need!"



and the Healthcare for Tomorrow scenario "Patients as customers!" (D2.1 [eu-DOMAIN D2.1, 2005], pp. 48-49; henceforth the "PaC" scenario):

The healthcare system is multi-faceted. A large amount of new methods, devices and medication are available from various service providers, each of them offering their services to an informed patient - sometimes in competition; sometimes in cooperation. The patient chooses the providers that are most suited to her/his needs. We call this scenario: "Patients as customers!"

Patients as
customers!

Functional Requirements

From these, use cases have been derived. The subset of these use cases shown in Table 1 are termed communicational significant in the sense that they have implications for the overall structure of the eu-DOMAIN communication platform.

Use Case	Name	Actors	Implications
ESN.1.1	Monitor 24 hours a day the effectiveness and the performance of a technical installation in a commercial building	Maintenance company responsible, Servizio Provinzia operator, Technician, Grundfos	Remote monitoring and data storage and analysis capabilities
ESN.2.1	Monitor 24 hours a day the effectiveness and performances of a technical installation in the commercial building of several customers	Servizio Provinzia operator	Monitoring, control, information filtering
ESN.2.3	Receive notifications/alerts in case of ineffective operating conditions or failures of the equipments	Servizio Provinzia operator, technician	Notification/Alert
ESN.2.5	Be alerted when updates of system software are available	Servizio Provinzia operator	Connection, updating
ESN.2.6	Establish connection with the domain service provider to ask for explanation on issues related to the technical equipment functionalities	Servizio Provinzia operator, Grundfos	Connection, matchmaking service
ESN.3.1	Record and communicate the data and the ID of the installed equipment to Grundfos and to Servizio Provinzia	Technician, Servizio Provinzia, Grundfos	Communication, identification, archive creation
ESN.3.2	Access the commercial building, obtaining identification and authorization	Technician	Access, identification, authorization, information download
ESN.3.3	Receive the information relevant to his profile and task	Technician	Information filtering
ESN.3.4	To receive on the PDA all data history and service records for the installed equipments	Technician	Information filtering
ESN.3.5	To download from Grundfos product database all the product information and tutorials	Technician	Information filtering
ESN.3.6	Negotiate technical support directly from Grundfos	Technician, Grundfos	Matchmaker service
ESN.3.7	To establish a virtual workgroup with Grundfos	Technician, Grundfos	group communication, matchmaker service
ESN.3.9	Make an update of the activities accomplished, sending this information both to Servizio Provinzia database and to that of Grundfos	Technician, Servizio Provinzia, Grundfos	Updating, Information, communication
ESN.3.10	Receive alerts over the coming days in case of similar malfunctions	Technician, Servizio Provinzia	Notification/Alert

ESN.4.1	Remotely access every single product enabled with the eu-DOMAIN service	Grundfos	Monitoring, control, information filtering
ESN.4.2	Remotely update the software in the installed equipments	Grundfos	Updating, monitoring, control
ESN.4.3	Negotiate technical support directly with the technician of Servizio Provinzia	Grundfos	Matchmaker service, communication
ESN.4.4	Establish a virtual workgroup with the technician	Grundfos, technician	Group communication, matchmaker service
HC.1.1	To send e-mail to the PALS outreach service	Patient or informal carers, PALS coordinator	e-mail, matchmaker service, group communication
HC.1.3	To have its blood pressure remotely monitored 24 hours a day	Patient, medical devices, formal carers	Remote monitoring, control
HC.1.5	The patient has to be monitored (by means of several house sensors) in case of critical situations when he is alone in the house	Patient, sensors, ambient intelligence environment	Surveillance, monitoring, alert
HC.1.6	To rely on a range of communication and feed back options for its self-manage program	Patient, formal carers	Group communication, matchmaker service, e-mail, messaging
HC.1.8	To be enrolled on the “new to diabetes course” provided by the MHDSS	Patient, MHDSS/formal carers	On-line course, group communication, matchmaker service
HC.1.9	To have its first diabetic eye screen and have this information uploaded in its PEHSCR	Patient, the GP/formal carers	Medical data collecting and transferring
HC.2.1	The patient’s immediate family has to be notified by the eu-DOMAIN system in case of minor critical situations by mobile phones	Informal carers, medical devices	Notification, alert
HC.2.2	The patient’s neighbours have to be notified by the eu-DOMAIN system in case the patient’s immediate family is unreachable during minor critical situations	Informal carers, medical devices	Notification, alert
HC2.3	The patient’s immediate family would like to access the data about the patient and to receive regular detailed status reports by e-mail	Informal carers	Notification, e-mail, information filtering, access, control, monitoring
HC2.4	The patient’s immediate family has to receive a text message when there is a suspected deviation from the patient’s norm profile	Informal carers, medical devices	Notification, alert, e-mail, information filtering, control, monitoring
HC.3.1	the PALS coordinator has to pass the EPR details to the MHDSS	PALS coordinator, MHDSS	Matchmaker service, messaging, mail
HC.3.2	The GP has to be informed electronically when the patient’s blood pressure device is operating	GP, blood pressure device	Notification, control

HC.3.3	The GP has to receive an alert in case the patient's mean blood pressure is outside preset limits for more than 3 consecutive days	GP or other formal carers, blood pressure device	Alert
HC.3.6	The GP and the case manager from MHDSS have to perform an on-line electronic discussion	Different formal carers (GP, case manager from the MHDSS, the diabetes consultant, the pharmacist, etc)	Group communication, matchmaker service
HC.3.8	The nurse practitioner has to switch the patient's blood pressure device to "compliance mode" from her PC	Nurse practitioner	Remote access and action on a device
HC.3.9	The nurse practitioner has to remotely monitor the patient's blood pressure profile uploaded on the PEHSCR and to set up a "Suspected Abnormal Behaviour" monitoring scheme	Nurse practitioner, blood pressure device	Access, monitoring scheme setting up

Table 1: eu-DOMAIN Communication use cases

3.2. Functional requirements analysis from communication perspective

We here outline how these functional requirements can be addressed from a communication view. Next section will offer a communication architecture description based on this preliminary analysis, i.e. which technologies can be used to handle the significant use cases regarding communication in the scope of eu-DOMAIN identified in Section 3.1.

3.2.1. ESN functional requirements

3.2.1.1. ESN.1.1: Monitor 24 hours a day the effectiveness and the performance of a technical installation in a commercial building

Different devices may be connected to a eu-DOMAIN service gateway and thus connected to a eu-DOMAIN server-side installation. If the device supports exchange of relevant data, such data may be either processed locally on the gateway or transmitted to the eu-DOMAIN server-side for processing using asynchronous web service calls (events).

Connection among Client Gateways and the Server Park can be addressed by means of mobile and fixed networks using DSL or Cable, allowing monitoring 24 hours a day the performance of a device. Here, it is envisaged the need of 24 hours availability of the eu-DOMAIN communication connection. Ideally, fixed network solutions are better to accomplish this requirement. Depending on the data transfer, bandwidth needs should be studied.

3.2.1.2. ESN.2.1: Monitor 24 hours a day the effectiveness and performances of a technical installation in the commercial building of several customers

Communication issues will be solved in the same way as ESN.1.1 requirement. The Network Intelligence Manager will control the gateways (installations) connected to eu-DOMAIN at any time.

3.2.1.3. ESN.2.3: Receive notifications/alerts in case of ineffective operating conditions or failures of the equipments

Servizio Provinzia operator has to be able to receive the alert anywhere and anytime. If the operator is in his office he might receive these alerts as e-mails on his personal computer or mobile handset, which has to be connected to the Internet. However, if he is out of the office he must also be properly informed. In this case, the operator would have at his disposal a mobile terminal (e.g. PDA, mobile phone) where he might be notified, for instance, by means of a SMS. The main constraint in this situation will be the need of being in an area with GSM coverage.

3.2.1.4. ESN.2.5: Be alerted when updates of system software are available

This means that the operator must be notified when new software versions are available at locations. This underlines the need for being constantly connected in order to receive these alerts and be able to maintain the system updated. So, the operator will receive these messages through his mobile terminal using the WLAN coverage provided by Client Gateways or using a fixed connection ((A)DSL or cable) when he is at a determined location. Therefore, the operator might manage the updating of the system without worrying about looking for new versions. Then, the operator will be able to download the suitable software from the Server side (maybe from external content providers) due to the Client Gateways internet-connection.

3.2.1.5. ESN.2.6: Establish connection with the domain service provider to ask for explanation on issues related to the technical equipment functionalities

If the Servizio Provinzia operator needs information about any technical equipment functionalities, he will be able to make use of his mobile terminal connectivity capabilities. This means that he will be able to send request and receive responses about concrete issues if the operator is under commercial WLAN coverage, uses the one provided by Client Gateways or uses DSL or cable connection he could connect with the domain Service Provider to ask for those explanations too. The Service Provider has to offer its services via Internet.

3.2.1.6. ESN.3.1: Record and communicate the data and the ID of the installed equipment to Grundfos and to Servizio Provinzia

The technician has to record and communicate the data and the ID of the installed equipment from his PDA to Grundfos and to Servizio Provinzia in order to enable Grundfos to remotely upload the software and populate the historical database related to the equipment.

This issue might be easily tackled using PDA connectivity capabilities. It is assumed that the PDA will allow GSM, GPRS or UMTS connectivity. In case the user terminal has WiFi capabilities, it could ideally connect to the wireless access point in the Client Gateway to acquire connection. In the ESN scenario, the technician's PDA acquires connection using the WiFi Access Point provided by the Client Gateway in the location.

3.2.1.7. ESN.3.2: Access the commercial building, obtaining identification and authorization

The platform supports mobility of persons through e.g. mobility of terminals. So, the technician has to be able to send his virtual identity from his PDA to the eu-DOMAIN service. Once the technician is authenticated he can receive information related to the commercial building where he is via the same wireless network that he uses in order to be authenticated in the eu-DOMAIN system.

3.2.1.8. ESN.3.3: Receive the information relevant to his profile and task

Once the technician is authenticated in the eu-DOMAIN system (ESN.3.2), he will receive information relevant to perform his tasks through his PDA using its connectivity capabilities available.

3.2.1.9. ESN.3.4: To receive on the PDA all data history and service records for the installed equipments

This requirement involves that the technician's PDA is connected to the WLAN at the location, and in this way he is able to receive all data history and service records in the installation.

3.2.1.10. ESN.3.5: To download from Grundfos product database all the product information and tutorials

The technician has to be able to remotely connect to Grundfos database, find and download relevant information to perform his tasks. Here, Grundfos is regarded as Content Provider which has a service (providing access to a product database) that the eu-DOMAIN server should be able to access via fixed network infrastructures.

3.2.1.11. ESN.3.6: Negotiate technical support directly from Grundfos

The technician has to be able to contact Grundfos (External Content Provider) from his PDA in order to directly negotiate technical support and complementary services. In the scenario, the PDA will use the WLAN at the location to acquire connectivity with the Server Park of eu-DOMAIN. External Content Provider will provide a mean to support technicians

3.2.1.12. ESN.3.7: To establish a virtual workgroup with Grundfos

The technician has to be able to receive support online being in direct communication with Grundfos. This communication must be performed interactively. WLAN infrastructure described above will be used in the ESN scenario to provide communication to the PDA.

3.2.1.13. ESN.3.9: Make an update of the activities accomplished, sending this information both to Servizio Provinzia database and to that of Grundfos

After finishing his tasks, the technician has to make an update of the activities accomplished, sending this information both to the Servizio Provinzia database and to that of Grundfos, in order to update the historical data of the installed equipment. Then, communication will be established between the Server Park and the technician's PDA using WLAN coverage at the location

Communication with External Content Providers is inherent in the architecture. The services from the External Content Providers are available as web services that are contacted from the Server Park..

3.2.1.14. ESN.3.10: Receive alerts over the coming days in case of similar malfunctions

To ascertain that the equipment has been repaired appropriately, the technician has to be able to receive alerts over the coming days in case of similar malfunctions. This is done automatically by the system by sending SMS (using GSM networks) to the technician's mobile phone or emails to his PDA or laptop. The terminal has to be connected to the Internet. The decision about the type of notification to be sent is taken regarding the technician profile.

3.2.1.15. ESN.4.1: Remotely access every single product enabled with the eu-DOMAIN service

Grundfos has to be able to remotely access every single product enabled with the eu-DOMAIN service and installed in any kind of commercial building worldwide.

Devices communicate with the rest of the world through Client Gateways, which have to support the communication technology of the device in question, and gateways will communicate via fixed or mobile networks with the Server Park. Thanks to that, Grundfos can perform their remote tasks, as the different services from the devices as web services.

3.2.1.16. ESN.4.2: Remotely update the software in the installed equipments

Grundfos has to be able to remotely update the software in the installed equipments to adjust their performance to the actual load conditions. It suggests the same communication constraints exposed in the previous use case (ESN.4.1). In this case, a Manager in the Server Park will be in charge of updating the software bundles in the different locations.

3.2.1.17. ESN.4.3: Negotiate technical support directly with the technician of Servizio Provinzia

The technician has to be able to contact Servizio Provinzia (External Content Provider) from his PDA in order to directly negotiate technical support and complementary services. In the scenario, the PDA will use the WLAN at the location to acquire connectivity with the Server Park of eu-DOMAIN. External Content Provider will provide a mean to support technicians.

3.2.1.18. ESN.4.4: Establish a virtual workgroup with the technician

This use case will require the same communication solution as ESN.3.7.

3.2.2. PaC functional requirements

3.2.2.1. HC.1.1: To send e-mail to the PALS outreach service

The patient or the informal carers have to send an e-mail to the coordinator of the PCT's Patient Advisory and Liaison Service (PALS) outreach service to ask for help in accessing primary care services. In order to address this issue, patient might have a computer connected to the Internet.

3.2.2.2. HC.1.3: To have its blood pressure remotely monitored 24 hours a day

This means that the device will be 24/7 accessible from and to the Server Park. Data measured is not continuously sent to the Server Park, just when an alarm exists or an alert is created, but the data is always available from the Client Gateways, as every device will publish their services as web services in the Client Gateway.

3.2.2.3. HC.1.5: The patient has to be monitored (by means of several house sensors) in case of critical situations when he is alone in the house

The eu-DOMAIN system has to be able to monitor the patient when he/she is alone in the house in order to alert the formal or informal carers in case of critical situations. When a critical situation occurs, eu-DOMAIN system has to notify informal careers about it by sending an alert. An event will be received in the Server Park and the Notification Manager will send an alert to the proper career.

3.2.2.4. HC.1.6: To rely on a range of communication and feed back options for its self-manage program

The patient has to be provided with several tools to communicate and give/receive feed back from the formal carers as regards her health situation and her performance in dealing with her self-management program. At least, the patient will have at his disposal a PDA with wireless connectivity (WLAN coverage at home) to receive information related to its self-manage program.

3.2.2.5. HC.1.8: To be enrolled on the "new to diabetes course" provided by the MHDSS

The patient has to be enrolled in a "new to diabetes course" provided by the MHDSS, an External Content Provider that uses the eu-DOMAIN network to enhance the feedback information to patients by collecting additional electronic diabetes information, often cases and things that have been discussed in class sessions. The Content Compiler in the Server Park will make the course available in the Interaction Server, which is accessible using internet connection from patient terminals.

3.2.2.6. HC.1.9: To have its first diabetic eye screen and have this information uploaded in its PEHSCR

The patient has to have a detailed diabetes clinical review in which an eye screen is performed by the GP in order to ascertain the level of diabetes. This information should be uploaded in the patient's PEHSCR.

From GP office, an internet connection will make possible that this measurement is uploaded to the Patient Record System.

3.2.2.7. HC.2.1: The patient's immediate family has to be notified by the eu-DOMAIN system in case of minor critical situations by mobile phones

As result of minor critical situations described in HC.1.5, patient's family will received alert messages by mobile phones via SMS (using GSM networks) or email (internet connection).

3.2.2.8. HC.2.2: The patient's neighbours have to be notified by the eu-DOMAIN system in case the patient's immediate family is unreachable during minor critical situations

It will be solved in a similar way as in HC2.1.

3.2.2.9. HC2.3: The patient's immediate family would like to access the data about the patient and to receive regular detailed status reports by e-mail

In order to address this issue, patient must have a computer connected to the Internet so that they can access the data available in the Interaction Server (web based interaction).

3.2.2.10. HC2.4: The patient's immediate family has to receive a text message when there is a suspected deviation from the patient's norm profile

An email or SMS will be sent (see HC2.1)

3.2.2.11. HC.3.1: the PALS coordinator has to pass the EPR details to the MHDSS

The PALS coordinator has to receive the electronically signed e-mail by the patient, authorizing him to release the patients records (EPR) to the MHDSS, which is in charge to create the PEHSCR for the patient.

The PALS coordinator will have at his disposal a computer or a mobile terminal with internet connectivity so as to receive patient's e-mails.

3.2.2.12. HC.3.2: The GP has to be informed electronically when the patient's blood pressure device is operating

When the first measurement is taken with a new blood pressure device, the Rule Engine will send a notification (using the Notification Manager) to the GP, who authorise the measurement to be uploaded to the EPR, interacting with the Interaction Server.

3.2.2.13. HC.3.3: The GP has to receive an alert in case the patient's mean blood pressure is outside preset limits for more than 3 consecutive days

The GP has to be alerted immediately in case the patient's mean blood pressure is outside preset limits for more than 3 consecutive days. The eu-DOMAIN system will notify the formal carers by several means, such as e-mail or SMS regarding his profile.

3.2.2.14. HC.3.6: The GP and the case manager from MHDSS have to perform an on-line electronic discussion

Different formal carers need to have access to the patient's information contained in the PEHSCR. On the basis of this data they need to exchange opinions, feedback and suggestions on how to implement the patient's treatment. An Internet connection is needed for each of the formal carers in order to start the on-line discussion.

3.2.2.15. HC.3.8: The nurse practitioner has to switch the patient's blood pressure device to "compliance mode" from her PC

The nurse practitioner has to be enabled to remotely act on the patient's blood pressure device, establishing to which mode it should be switched. It is possible since the Client Gateway will be connected to eu-DOMAIN server-side via DSL or Cable at the patient's location where the services provided by the software bundles that control the devices are published as web services.

3.2.2.16. HC.3.9: The nurse practitioner has to remotely monitor the patient's blood pressure profile uploaded on the PEHSCR and to set up a "Suspected Abnormal Behaviour" monitoring scheme

The nurse practitioner has to have remote access to the patient's PEHSCR and she has to monitor the blood pressure profile, setting up a "Suspected Abnormal Behaviour" monitoring scheme.

The nurse will use an internet connection to monitor the patient's blood pressure profile.

4. eu-DOMAIN Communication Infrastructure

The overview of the software architecture in eu-DOMAIN presented in the previous chapter shows us the physical links to be solved regarding communication channels.

We can identify four different types of communications needed in eu-DOMAIN:

- TCP/IP based communications, which is the main communication technology used in eu-DOMAIN and that appears when communicating:
    - Terminals with the server side (Interaction Server).
    - Managers with other managers in the server side.
    - Client gateways with managers in the server side.
    - External content providers with managers in the server side (Web Service Server).
- SMS communication, when the users receive alerts in the shape of SMS messages, which go through GSM networks.
- Device communication, which appears when we want to control a device from the client gateways and thus we plug it physically to the OSGi gateway in a location. Client Gateways need to support the communication technology implemented in the device (sensor/actuator) with which the communication has to be established.
- Localisation information, based on the actual GPS system. The GPS system is an American technology. Russia operates an independent system called GLONASS. Moreover, the European Union is developing Galileo as an alternative to GPS, planned to be in operation by 2010.

eu-DOMAIN platform provides service interoperability using web services, which implements a Service Oriented Architecture (SOA). This means that every service in the architecture is published providing a web service interface. It does not matter the technology that is behind the service (Java, .NET, PHP, etc.), because the interface provided is technology independent. In this way, the eu-DOMAIN infrastructure is a system designed to support interoperable machine-to-machine interaction over a network. The interfaces presented before are described in a machine-processable format. This is done using WSDL language. Web service interaction (and thus communication) is performed in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP (HTTPS) with an XML serialization in conjunction with other Web-related standards.

The eu-DOMAIN SOA is a distributed system, first of all because a number of distributed locations are connected to the Server Park. Each location is governed by an OSGi residential gateway where services are deployed in the shape of Web Services. For example, if there is a blood pressure monitor plugged to a gateway, there will be a bundle that will publish a web service with the services provided by the blood pressure monitor, let's say, for instance, last systolic, last diastolic and last pulse measurement taken. These services will be contacted from the Server Park using SOAP messages, which relies in HTTP(S) mainly and in TCP/IP protocol. The TCP/IP protocol is concerned primarily with passing data across the wire in packets. As a protocol that guarantees transmission across public networks, TCP/IP emphasizes reliability of data transport and physical connectivity. It has to be pointed that although it is generally assumed that SOAP messages need HTTP, some implementations admit MSMQ, series MQ, SMTP or TCP/IP directly. Anyway, HTTP is the most widely used protocol for interchanging SOAP messages, and thus, this will be the technology used in eu-DOMAIN, at least for the ESN and PaC prototypes. Secondly, eu-DOMAIN SOA architecture is distributed because the Server Park itself is a distributed system where different services are located in different machines that interact among them seamlessly interchanging SOAP messages.

The distributed system is composed by a discrete number of software agents that work together. These agents do not operate in the same processing environment, so they must communicate by hardware/software protocol stacks over a network. The first implication of this architectural election is that communications in a distributed system are intrinsically slower and less reliable than those using direct code invocation and shared memory. This has important architectural implications because distributed systems require that developers (of infrastructure and applications) consider the unpredictable latency of remote access, and take into account issues of concurrency and the possibility of partial failure. This problem (and other not directly related to communication issues but to SOA ones) appears whether the distributed object system is implemented using COM/CORBA or Web services technologies (or other distributed architecture or technology). It is a problem inherent of distributed system, where the communication channels play a very important role. Nevertheless, eu-DOMAIN platform is mainly concerned about interoperability and extensibility and these requirements are clearly met by using web services communications (SOAP over HTTP(S), over TCP/IP) as the benefits they offer in terms of platform/vendor neutrality offset the performance and implementation immaturity issues they may introduce.

When working with web services as the interaction patterns among software agents, it is important to differentiate between the two principal architectures for Web service interfaces: synchronous Web services and asynchronous Web services. These two architectures are distinguished by their request-response handling. With synchronous services, clients invoke a request on a service and then suspend their processing while they wait for a response. With asynchronous services, clients initiate a request to a service and then resume their processing without waiting for a response. The service handles the client request and returns a response at some later point, at which time the client retrieves the response and proceeds with its processing. These different architectures have implications in the communication model, as in the first one, the communication is maintained until the response is received by the client that performs the call while when working with asynchronous web services, once you performed the request, the communication ends, and a new communication is started by the service side when the request is ready to be sent. Eu-DOMAIN Service Oriented Architecture will adopt both architectures, although asynchronous calls will be more usual, as a very important number of calls will appear in terms of events (asynchronous web service calls), where no response is needed (a sub-group in the asynchronous communication architecture model).

Synchronous services are characterized by the client invoking a service and then waiting for a response to the request. Because the client suspends its own processing after making its service request, synchronous services are best when the service can process the request in a small amount of time. Synchronous services are also best when applications require a more immediate response to a request. Web services that rely on synchronous communication are usually RPC-oriented, although this is not mandatory.

In asynchronous services, the client invokes the service but does not (or cannot) wait for the response. Often, with these services, the client does not want to wait for the response because it may take a significant amount of time for the service to process the request. The client can continue with some other processing rather than wait for the response. Later, when it does receive the response, it resumes whatever processing initiated the service request. Generally, a document-oriented approach is used for asynchronous class of services.

As explained above, when trying to provide interoperability and flexibility to the eu-DOMAIN platform, which is a distributed one, and taking into account pros and cons of the different solutions, we decide to use web services as the interaction pattern between software agents in the infrastructure instead of other distributed solutions such as CORBA. With this solution, we cover the communications between managers in the server side, between gateway clients and the Server Park and we provide an easy and widespread solution and platform for external content providers to offer their services and to be plugged into the eu-DOMAIN infrastructure. It has to be said at this point that some communication between managers in the Server Park is not SOAP based but using direct code invocation and shared memory (this solutions is used for those managers that interact directly with the domain model), which is a faster and more reliable solution than the web services solution, but less flexible.

The only interaction that is not based on SOAP messages interchange (let's say, web services) is the one performed by terminals accessing the Interaction Server. The eu-DOMAIN platform will provide web based interaction for terminals. This means that terminals need internet connection (using fixed or mobile networks) to access the services and applications provided by the Interaction Server. If there is no connection, there is no interaction for end users. The interaction will be based on HTTP(S) transfer protocol over TCP/IP. The decision of using web-based interaction for user terminals is based on a supposed always connected user terminal and in trying to include the less processing tasks and applications as possible in those terminals. User terminals in eu-DOMAIN are dummy interfaces to access the functionality provided by the infrastructure.

Once this distributed solution is chosen, the main concern is to maintain “on” the communication channels. The infrastructure to run needs that all the services are reachable 24/7. Different physical connection can be used to support TCP/IP communication, which includes fixed and mobile networks such as (A)DSL, cable, GPRS, UMTS, etc. We can identify four TCP/IP types of communication channels to handle in eu-DOMAIN:

1) Communication channels among managers in the Server Park: the Server Park will consist on a number of machines allocated in a physical location. It can be assumed that the communication channels between these machines and thus, between the services published are always on (reachable) in the LAN of the location. There is also a possibility that the Server Park is distributed in different locations and although it is supported by the eu-DOMAIN SOA, this is not implemented in the prototypes. The Server Park will offer an entrance point for gateways clients to contact and another one for terminals. It is assumed then that the Server Park is a communication controlled area within the eu-DOMAIN platform

2) Communication channels between Client Gateways and the Server Park: a number of gateways will contact the Server Park. The entrance point to the Server Park is the Gateway Manager. In addition, there is a component in the architecture, the Network Intelligence Manager in charge of controlling the different gateways that are registered in the eu-DOMAIN infrastructure. This kind of infrastructure creates an ad-hoc organised network of well known elements. Ad-hoc networks differ considerably from the fixed communications networks, as nodes and connections are inherently unreliable. Nevertheless, this ad-hoc network is based on a number of Client Gateways that enter and leave the network in a controlled fashion (except for occasional fall-out and non-connectivity). The networks are created on demand but with the support from fixed commercial infrastructure. Security in this environment is managed with the help of certification authorities (CAs), certificates and security associations. The communication channel could be based in fixed and mobile networks, as we can have gateways in fixed locations or in mobility. The usual situation of a client gateway is to be set in a fixed location where different devices (sensors and actuators) can be controlled within its area of influence (this depends on the communication links provided by the gateway itself). Nevertheless, a car, an ambulance or a van could have a gateway installed in (for example using the one provided by LIWAS), and even PDAs and Smart Phone could act as gateways, as efforts has been done to include OSGi residential gateway in mobile environments. In these cases mobile networks will be used to acquire connectivity with the Server Park. In any case, eu-DOMAIN cannot control whether these gateways will be always reachable or not. They rely on commercial communication infrastructure and thus it is not a controlled communication channel. Anyway, always on communication channel is not needed, as the communication is based on events and no continuously data interchange is needed.

3) Communication channel between external content providers and the Server Park. The services provided by these external content providers should be reachable at any time. They will offer a web service interface to be contacted by the eu-DOMAIN platform. As an external content provider, it is up to them to provide an always connected link. Again, we are in a non-controlled communication channel. This channel is also based in commercial infrastructure communication.

4) Communication channel between terminals and the Server Park: this communication channel allows end-users interact with the platform and access the services provided by eu-DOMAIN. The interaction is web based and the user uses a browser in the terminal (PC, laptop, PDA) to access the functionality provided. We are again using HTTP transfer protocol over TCP/IP. In fact, eu-DOMAIN will provide the ciphered version of HTTP, HTTPS, based on SSL to protect the communication between the end-users and the Server Park. Behind these protocols the terminals can use fixed o mobile commercial networks. Terminals do not need to be always connected to the Server Park, just when they need to interact with the Interaction Server.

Terminals can acquire this connection by themselves or using a gateway client as a proxy if they are within the area of influence of the gateway and this gateway offers that possibility.

This entire four TCP/IP communication channels are summarised in Figure 5:

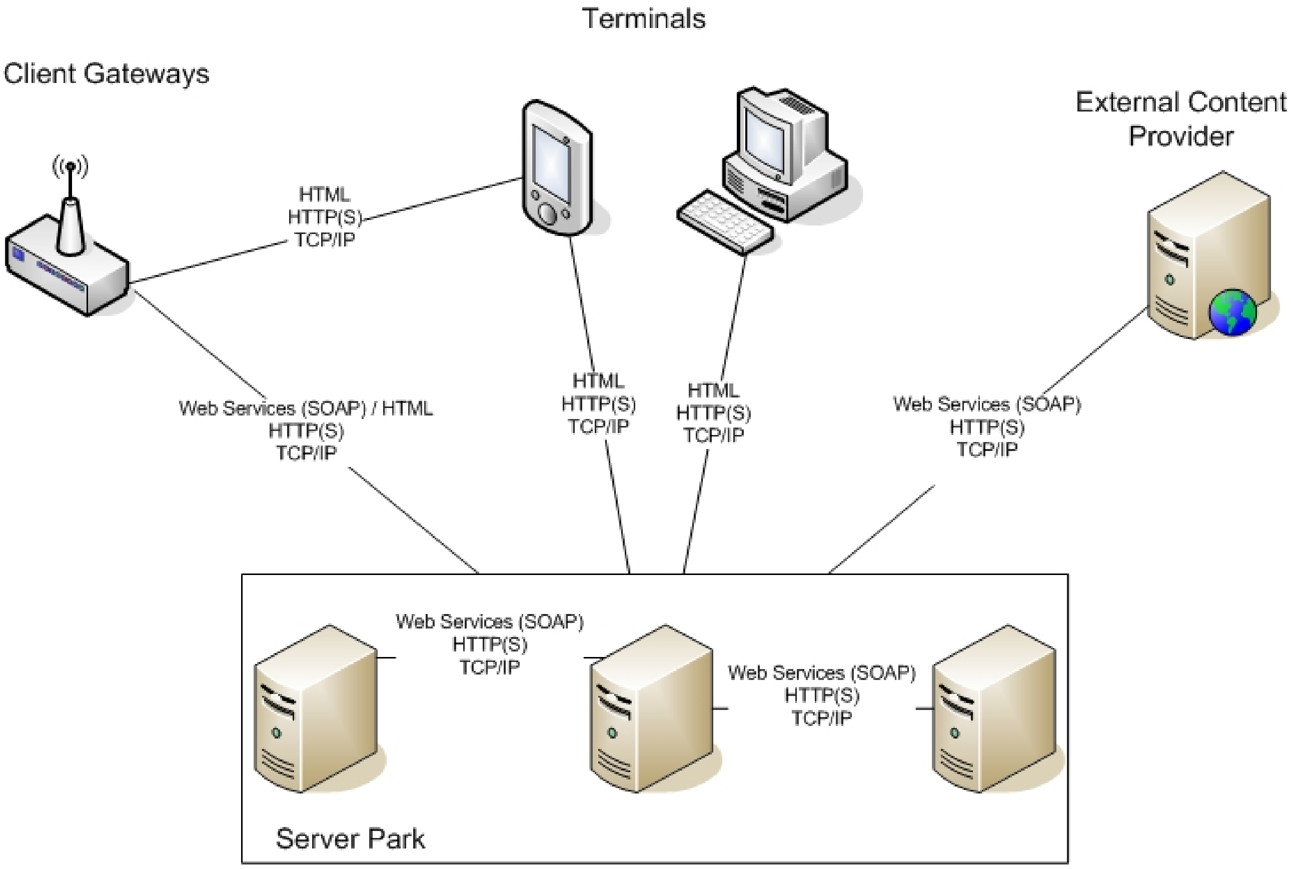


Figure 5: TCP/IP communication channels in eu-DOMAIN

Apart from the communication channels described before, there is a special one that includes terminals and that concerns the SMS messages sent by the Notification Manager to mobile phones when a special event occurs. SMS is supported by GSM networks. Figure 6 shows this interaction channel.

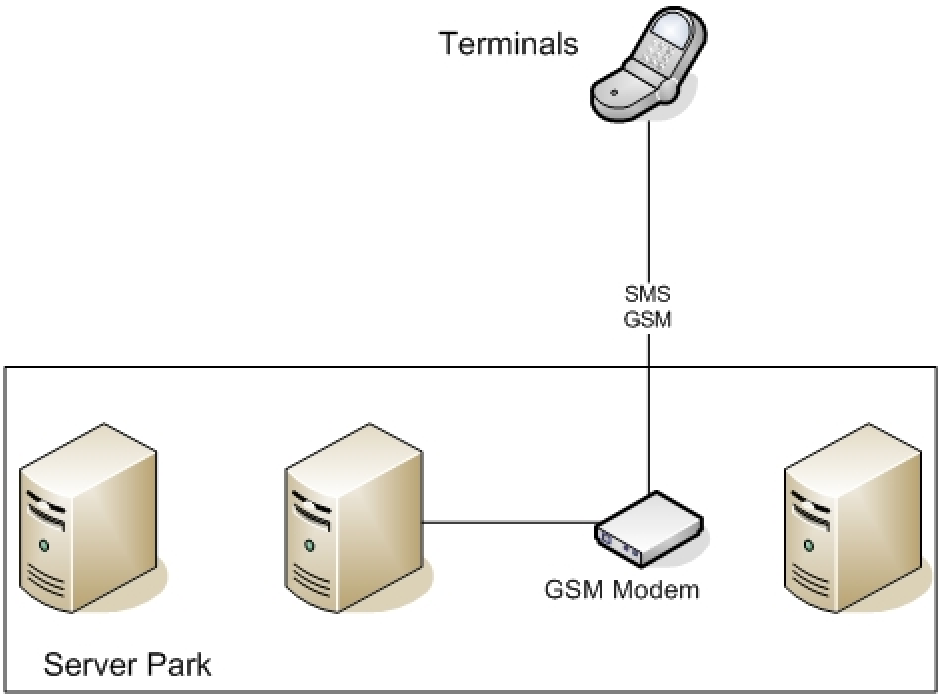


Figure 6: SMS interaction in eu-DOMAIN

Finally, although it is not envisioned to include this feature in PaC scenario (and it was not incorporated to the ESN one), GPS technology can be used to control and localise users (such as mobile workers or nurses) so that it is possible to determine which is the resource that is closer to where a technician or a nurse is required. The user has to carry a GPS module (included in his terminal or in the vehicle he uses). This module allows the system to determine his position using trilateration techniques as the following image shows.

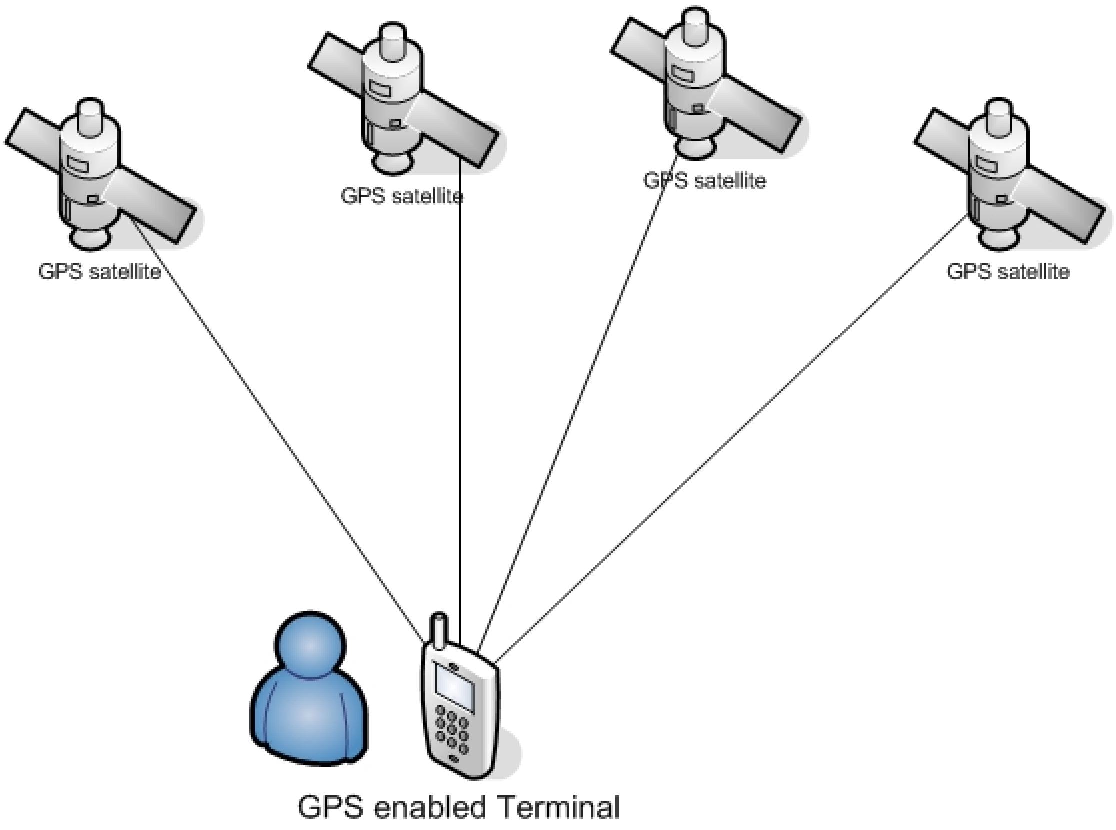


Figure 7: GPS Localisation System

There are other issues concerning communication links in eu-DOMAIN. One important concern is security. Although security aspects are well treated in other deliverables, a special chapter can be found below, where the principal problems are addressed. Apart from securing the communication channels, the eu-DOMAIN platform has to deal with the problem of dynamic IP addresses for gateways. We can suppose that the Server Park will have fixed IP addresses, and the same assumption could be taken regarding external content providers (although this is not mandatory). Terminals are not affected by using fixed or dynamic IP addresses. The problem could arise with Client Gateways being plugged and unplugged from the platform. The Network Intelligence Manager in the Server Park is suppose to handle this situation, although, at least for the ESN and PaC scenario prototypes, we will assume that fixed IP addresses are used in the entire infrastructure. As a general comment we can say that we need an fixed IP address when we run one or more Web servers directly on a site that require external access (from the Internet, or Extranet but not typically an Intranet). This is the case of the Server Park, the external content providers and, in some way, the Client Gateways. On the other hand, if we browse the Internet, send and receive e-mail, download or upload files, it is enough to have a dynamic IP address. This is the case of the terminals.

Another problem that should be taken into account is how to handle unreliable communications in eu-DOMAIN. There are small chances that a link is broken during a communication (for instance, when uploading a measurement). This situation cannot be handled at communication level, so it is up to the software agents involved in the communication to include some mechanism to avoid data loss. This problem is more critical when an asynchronous communication is performed, which is the communication pattern used for events (widely used in the eu-DOMAIN infrastructure), as no response is waited and thus there is no easy way to determine whether a data transfer over the communication channels took place or not. One solution suggested is to use unique identification for every event communication between client gateways and the Server Park.

We have introduced until this moment all the communication channels from client gateways, external content providers and terminals to the Server Park and among software agents inside the Server Park.

The communication channels that are still to be defined are those that appear between devices (sensors and actuators) and a Client Gateway. Each device defines the communication link to use and in case we want to include it in the eu-DOMAIN infrastructure, we will need to provide that kind of communication support in the Gateway Client in question. For example, if a device uses Bluetooth to communicate its data, a Bluetooth access point will be needed in the Gateway Client to handle this communication channel. Theoretically, any protocol could be supported by the eu-DOMAIN infrastructure. A bundle will control the real communication with the device and will publish a service in the form of a web service, so that interoperability is acquired in terms of service level. The OSGi framework provides mechanisms to discover devices within the range of the gateway. This can be done for those devices that use protocols that allow discovering, such as Bluetooth or USB. In other cases, if the device uses RS-232, for example, this cannot be done and the device has to be manually plugged into the gateway. Figure 8 shows a number of devices (sensors and actuators) connected to a client gateway. They all use device protocols, where we can integrate communication solutions such as RS-232, USB, X-10, ZigBee, Bluetooth, etc.

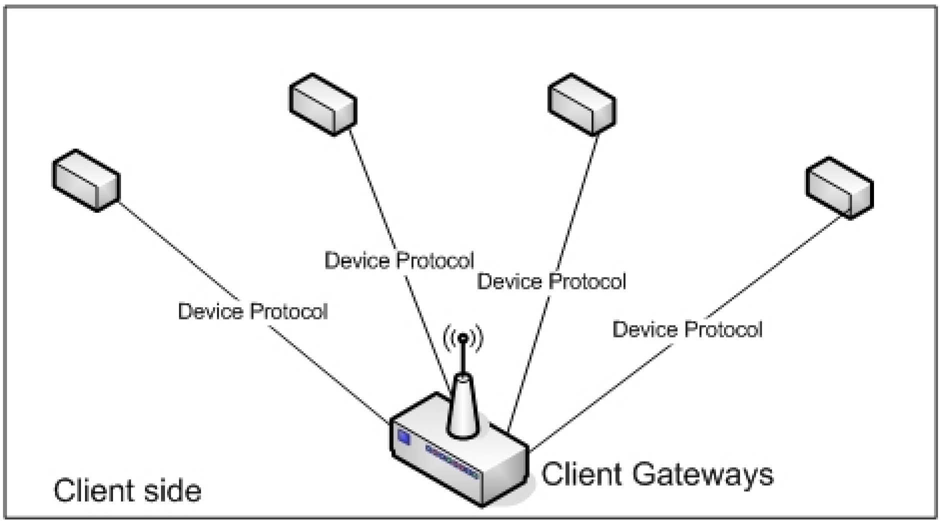


Figure 8: Device communication in eu-DOMAIN

4.1. Communication Technologies

We have discussed and presented the communication infrastructure needed in eu-DOMAIN in terms of protocols and interaction patterns. One of the first conclusions that we can derive is that network connectivity is crucial in a SOA solution and in the web-browser based terminal solution. This means that there is an underlying assumption that network connectivity is pervasive in the eu-DOMAIN scenarios. This is explained from the moment that any service in eu-DOMAIN will be contacted via web services from other software agents located in different physical locations and thus the only way of interacting is by using network communication channels. This pattern is used among software agents in the Server Park, between External Content Providers and between Client Gateways and the Server Park. Moreover, user terminals need to have network connectivity if they want to access the functionality provided by the platform.

In this section we will discuss most of the communication technologies that can be used to provide elements in the architecture with network connectivity. Finally, the communication prototype platform will be presented.

As a general assumption, fixed and mobile networks will be used to provide communication links among the components of the eu-DOMAIN platform. Users can access the eu-DOMAIN platform via different terminals; such as, computers, laptops, mobile phones, PDA, etc. Each of these devices shows several constraints with respect to communication capabilities.

We will maintain in this section the classification of communication routes identified in previous sections of the chapter:

- Among software agent in the Server Park
- Between Client Gateways and the Server Park
- Between the Server Park and External Content Providers
- Between Devices and Client Gateways
- Between Terminals and Server Park
    - Web-based interaction
    - SMS interaction
- Between Terminals and Client Gateways (using the latter as proxies)

4.1.1. Client Gateways – Server Park communication

The Gateway Server in the Server Park is the entrance point for client-side Gateways to the server-side of eu-DOMAIN. Its main function is to direct traffic (and filter it) to and from such gateways to the different software agents in the Server Park. The Network Intelligence Manager controls the actual Gateways connected to the platform, controlling whether the gateway is on-line or not..

Client Gateways act as mediators among devices and the eu-DOMAIN server-side, and thus communication links are needed. Client Gateways belong to a location, which can be a mobile one, in case of embedding Client Gateways in mobile handsets (there are efforts at the moment embedding OSGi frameworks in such gadgets). Gateways run an OSGi service platform, i.e., a Java VM, an OSGi Framework, and a set of bundles.

As explained in the previous section, this information interchange between Client Gateways and the Server Park is based on SOAP messages (web services) over TCP/IP networks. If we go one step down in the stack of protocols we can find several different physical protocols that provide this kind of connectivity needed in eu-DOMAIN. We will try to explain this links in detail regarding the physical technologies that fits better into the eu-DOMAIN architecture framework. We will be centred then on (A)DSL, cable, GPRS and UMTS networks,

(A)DSL and cable modem network access are two alternative ways to connect to a network service provider using fixed networks. DSL and cable modem networks achieve the same result of providing dedicated access to a network service; often the Internet, but each one does it using different technologies. ADSL is the traditional DSL communication technology used for residential purposes, so that we have chosen it as one of the suitable ones to connect Client Gateways with the Server Park in eu-DOMAIN.

A typical ADSL service architecture as Figure 9 illustrates consists of Customer Premise Equipment (CPE), the Network Access Provider (NAP) and the Network Service Provider (NSP).

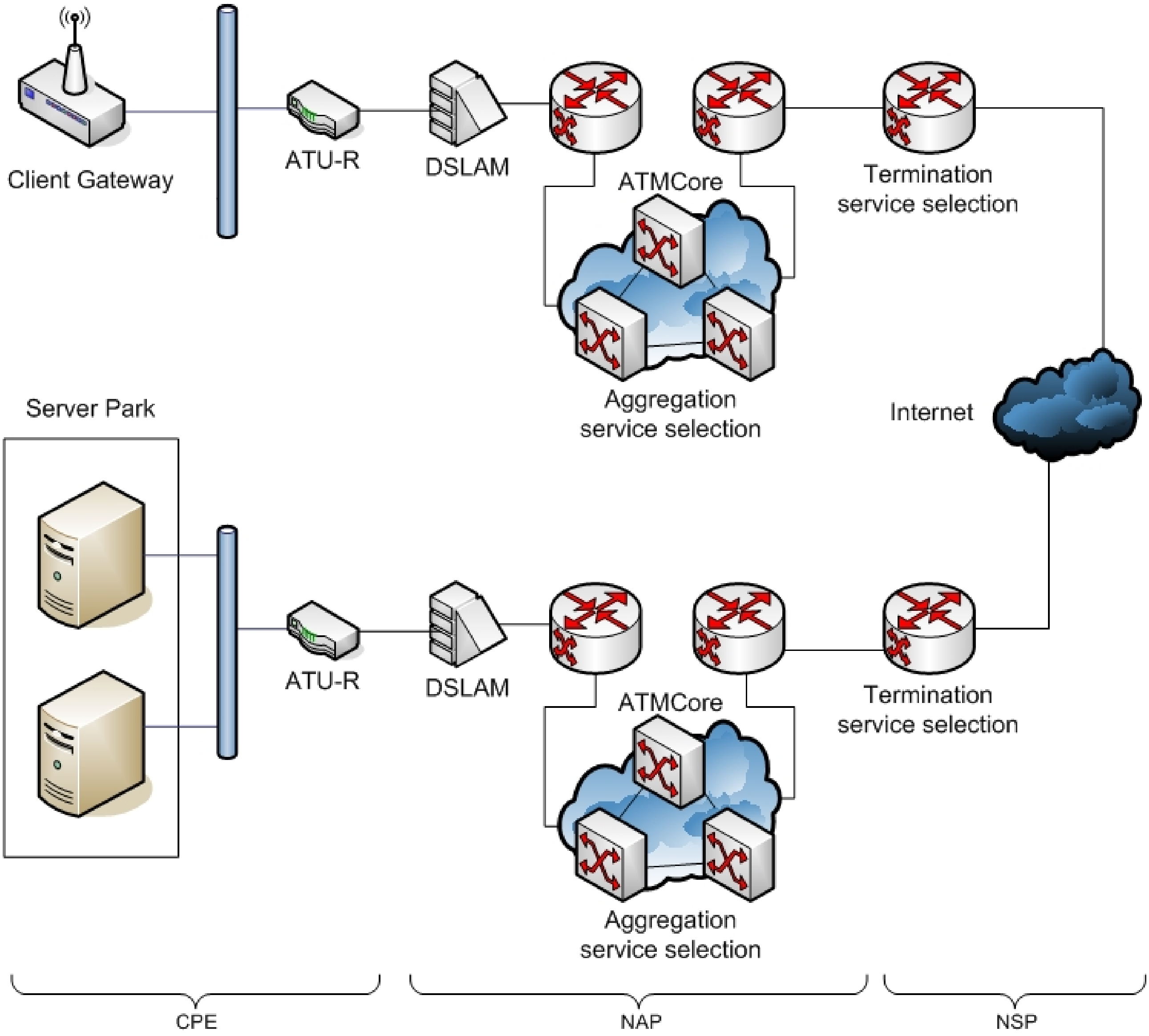


Figure 9: (A)DSL architecture

On the other hand, cable access technologies can be also used to connect the Client Gateways with the Server Park. If the Client Gateway is to use this technology, connection to fibre nodes is gained by coaxial cables. Nowadays, commercial cable networks have moved from coaxial cable networks to hybrid networks (HFC), using both optic fibre and coaxial cable. Figure 10 shows this typical architecture applied to eu-DOMAIN.

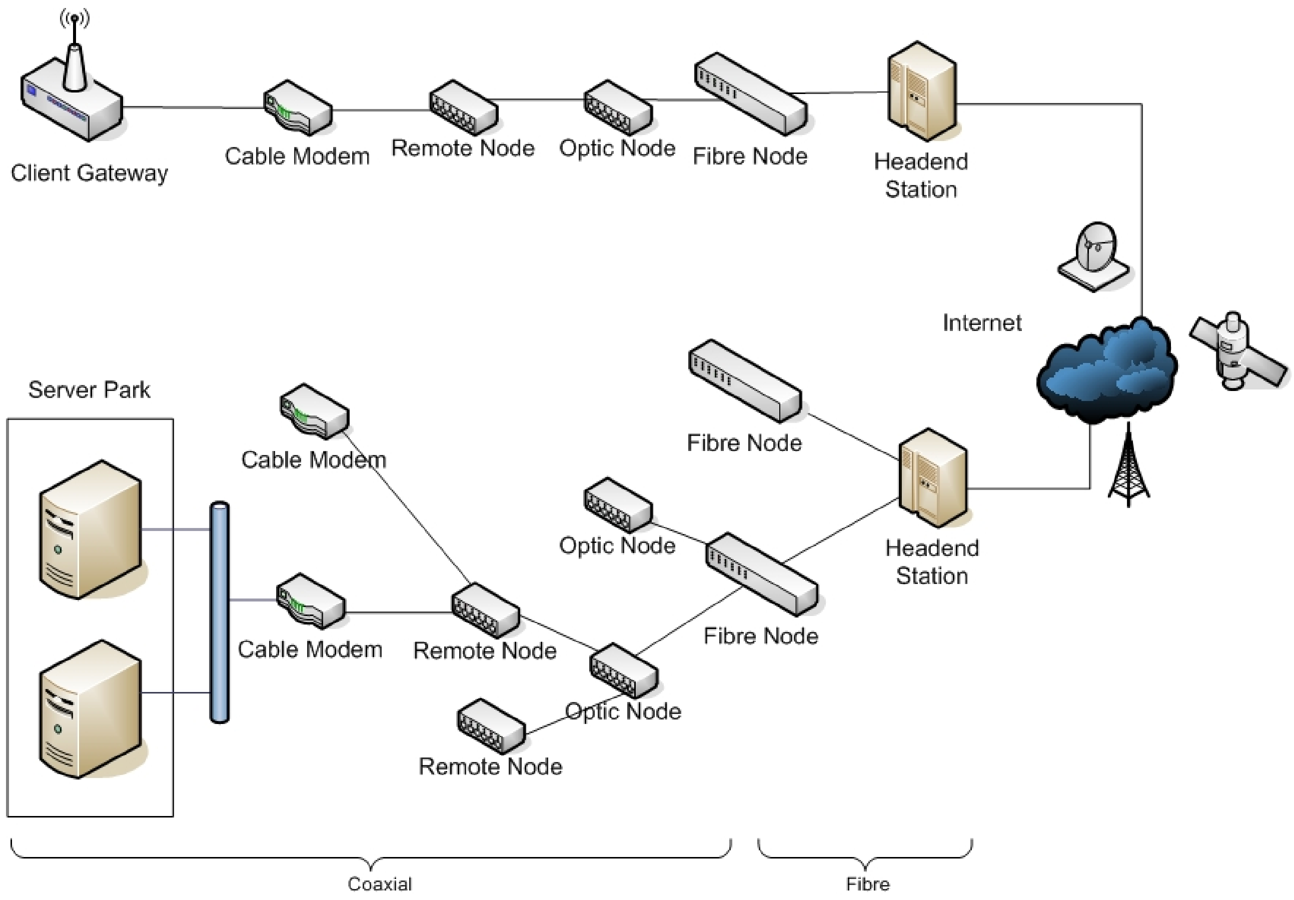


Figure 10: Cable architecture

Until this moment we have presented two examples of fixed mobile network that could be used in order to connect a Client Gateway with the Server Park. Both of them are feasible for the communication requirements in eu-DOMAIN. It is up to Client Gateways to acquire Internet connection by using one of these technologies. Nevertheless, there is the possibility that a Client Gateway in not fixed but in movement. This can occur is cases in which the gateway is embedded in a mobile handset (PDA, smart phone) or in a vehicle (ambulance, van, car, etc.). In these situations, the networks explained above are not useful. They could still be useful if the gateways could connect to them using wireless access points (WiFi) (see Figure 11) to gain internet connection through a fixed network. This is not the usual scenario, and thus, mobile networks have to be presented in here too.

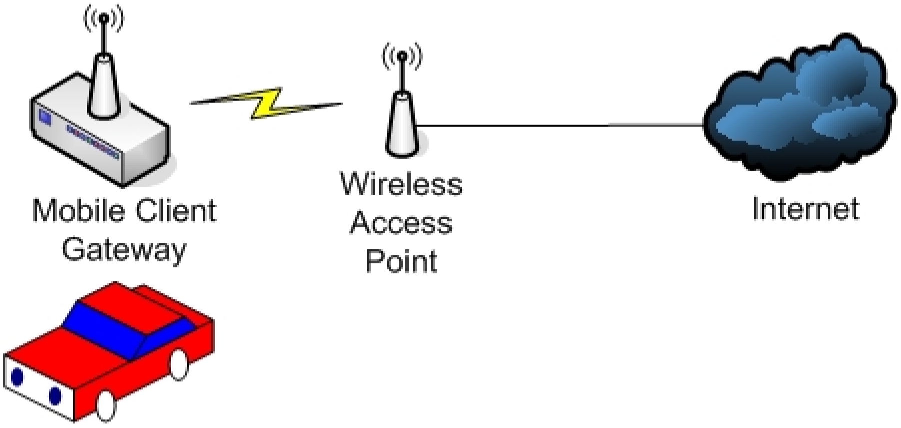


Figure 11: Wireless Access Point

In case Client Gateways are not in the area of influence of a wireless access point, they have to gain their internet access using any of the mobile communication networks available in the market. The technology to be use at this very moment is GPRS or UMTS where available. We will explain these technologies applied to the eu-DOMAIN case in the following lines.

GPRS networks are an evolution of the GSM network that is explained below. Figure 12 shows the different elements of the GPRS architecture and how a mobile Client Gateway in eu-DOMAIN will acquire access to Internet to connect to the Server Park in mobility, where the gateway GPRS support node (GGSN) acts as interface between the GPRS backbone and the external packet data network, while the serving GPRS support node (SGSN) is responsible for routing the packet switched data to and from the mobile stations within its area of responsibility. The Home Location Register (HLR) stores all the subscriber data. In the architecture, the Base Station Controller (BSC) manages the radio resources allocated for circuit switched use while the packet Control Unit (PCU) manages radio resources for the GPRS traffic itself.

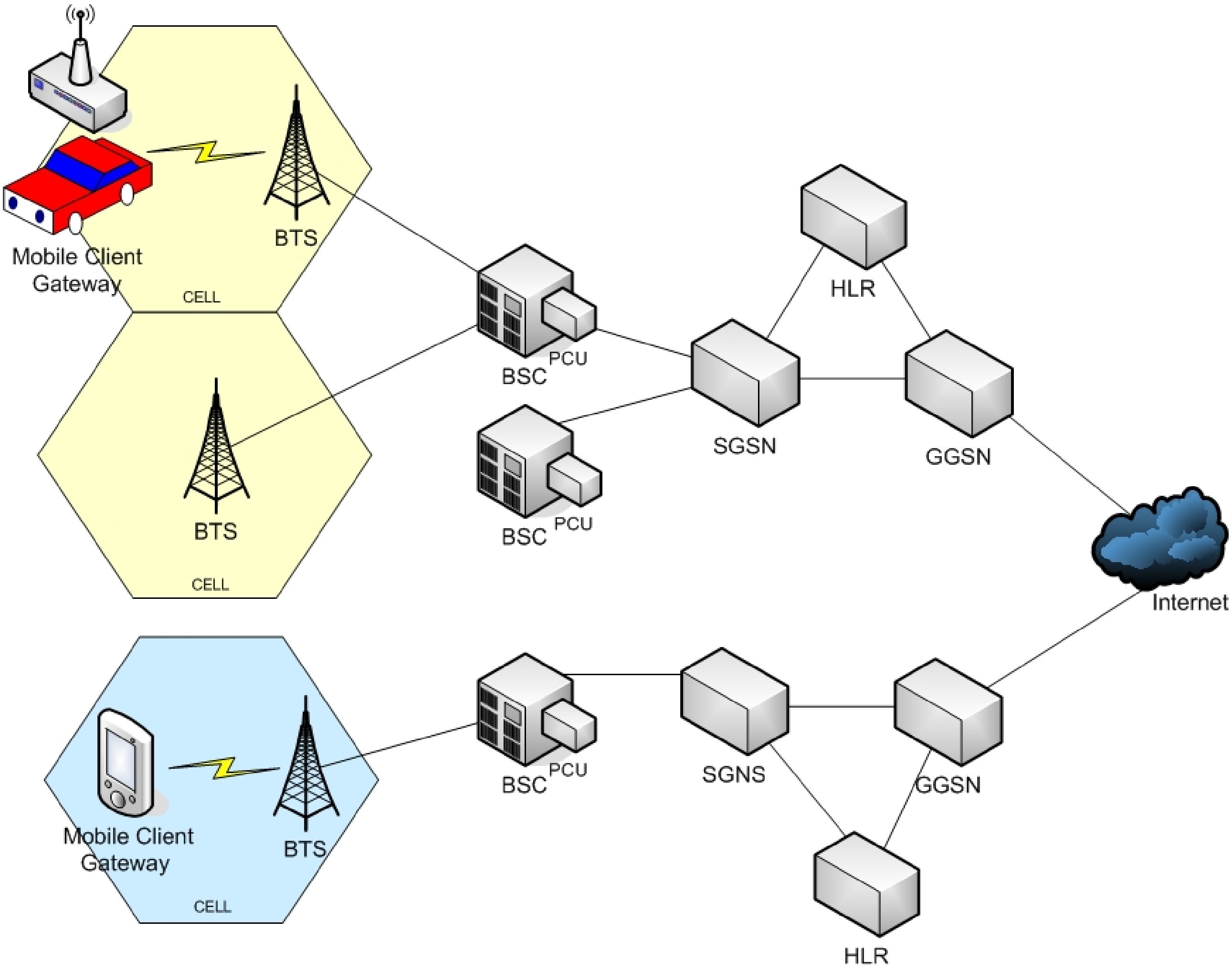


Figure 12: GPRS architecture

Moreover, UMTS technology (3G technology) can be used for this purpose. UMTS is another mobile network technology which becoming more and more popular as new mobile services that requires high data rates appear. UMTS system uses the same core network as the GPRS and uses entirely new radio interface. A Radio Network Controller (RNC) plays the role of the BSC in the GPRS architecture. Figure 13 shows this architecture. Client Gateways must incorporate UMTS capabilities to access this network.

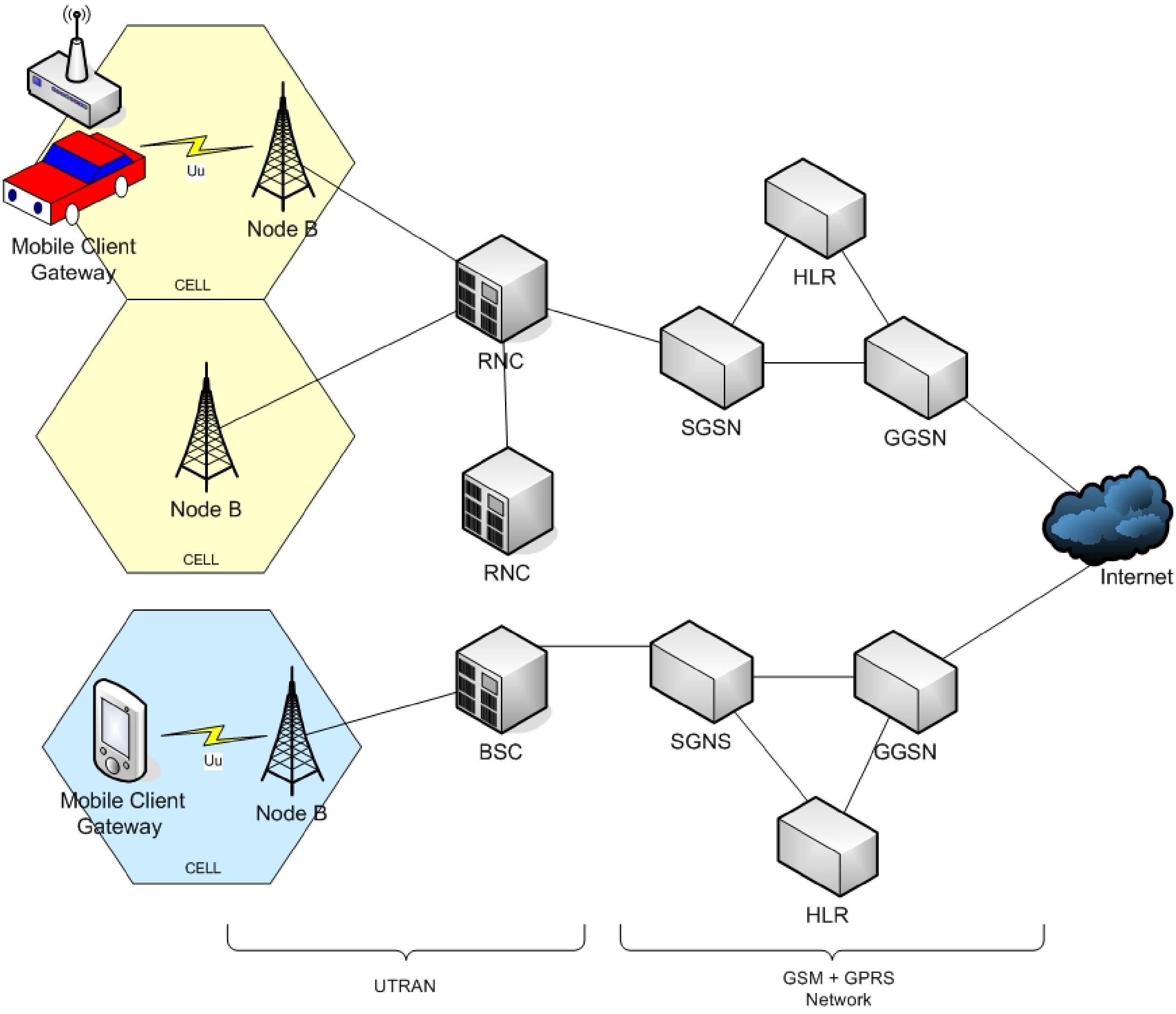


Figure 13: UMTS architecture

4.1.2. Server-Park – External Content Providers communication

The Service Tier contains services external to eu-DOMAIN provided by External Content Providers which are accessible through web services. An example of a service would be a web service-based interface to the producers of equipment for a facility management application. Again, the eu-DOMAIN platform does not make any assumptions on the type of web service interface that external services provide.

Any of the communication technologies explained in the previous section (4.1.1) can be used to publish the services of the External Content Provider in Internet. Maybe the mobile ones are not very interesting for this purpose and (A)DSL (Figure 9: (A)DSL architecture) and cable (Figure 10: Cable architecture) (the fixed ones) are the most suitable for this task. The bandwidth needed depends on the number of requests estimated at the same time and the data transferred in each of these requests. This bandwidth is not a critical issue at least for the prototypes in eu-DOMAIN, but it is an issue to be studied in case of exploitation of the eu-DOMAIN infrastructure.

4.1.3. Server Park components communication

The Server Park, as its name says, is composed by a number of servers running software agents that interchange information with the others by code calls in the same machine (in the case of accessing the Domain Model) or using SOAP messages (web service calls). In order to make the whole system work, these machines have to be interconnected. Once possibility is that the different machines that create the Server Park are allocated in the same facility and thus are interconnected using an intranet or an ad-ho network with one of the machine offering access to Internet. Anyway, this is not mandatory, and a Server Park composed by machines allocated in different facilities, even in different countries is possible thanks to the SOA architecture chosen for the eu-DOMAIN architecture.

The latter is solved using any of the commercial communication technologies explained and publishing the services of the different machines in the Server Park in Internet (which means that security policies are needed to secure the communications such as creating a VPN between server machines). Figure 14 shows the architecture needed to deploy the Server Park with machines distributed in different facilities using a VPN.

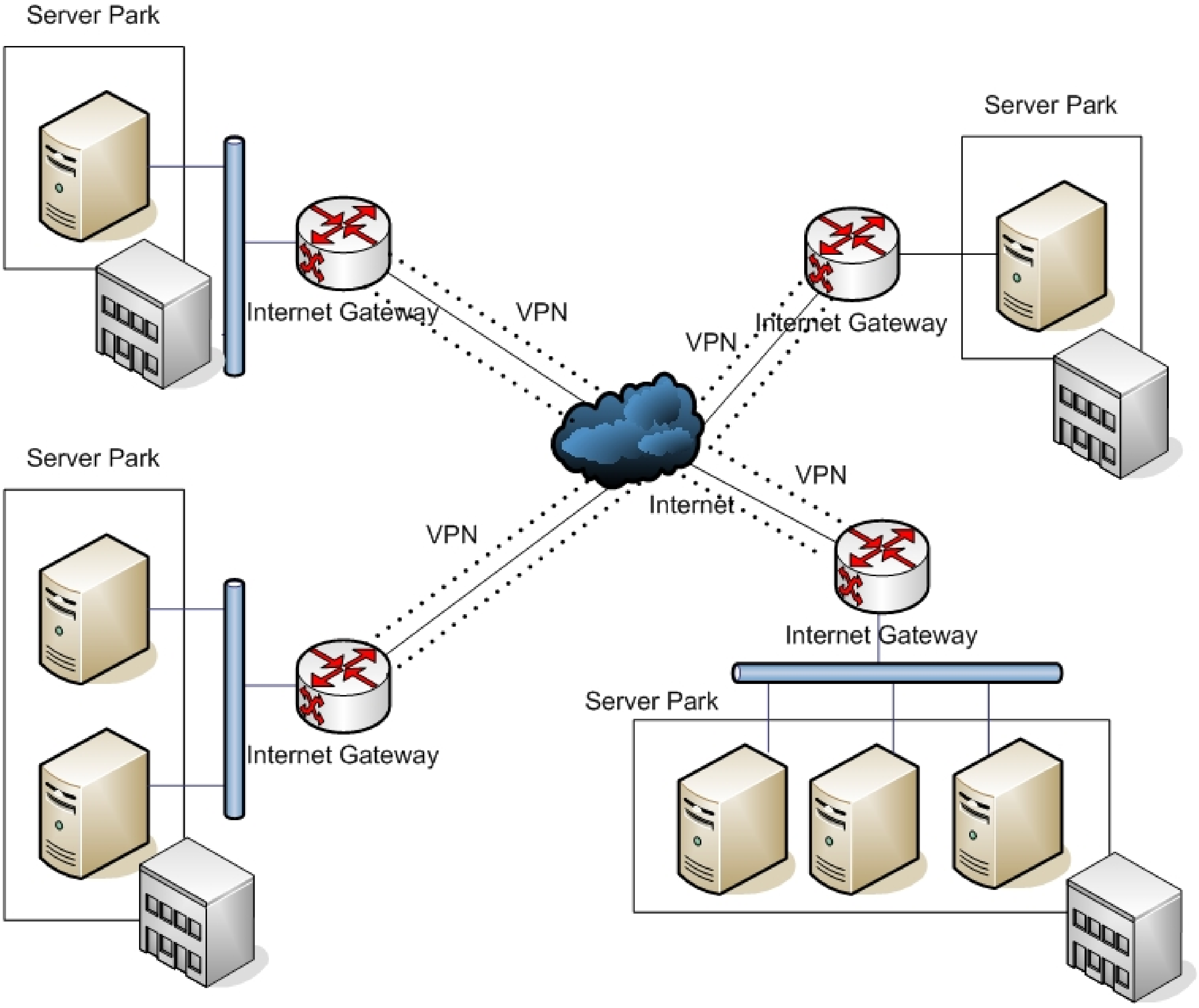


Figure 14: VPN architecture

The former, which is also the solution chosen for the ESN and PaC scenarios, is much easier to implement and is much more performing too, as all the communications take place inside the intranet of an organisation. Moreover, it is preferable also in order to achieve an easier configuration and maintenance of the Server Park. The different servers create a LAN and they use a gateway to access outside the intranet. A number of topologies can be used to create the LAN, among which the most common are Ethernet, Token Ring or FDDI. Figure 15 shows a LAN based on Ethernet, the solution chosen to implement the communications in the Server Park of eu-DOMAIN for the prototypes using the communication network within TID facilities.

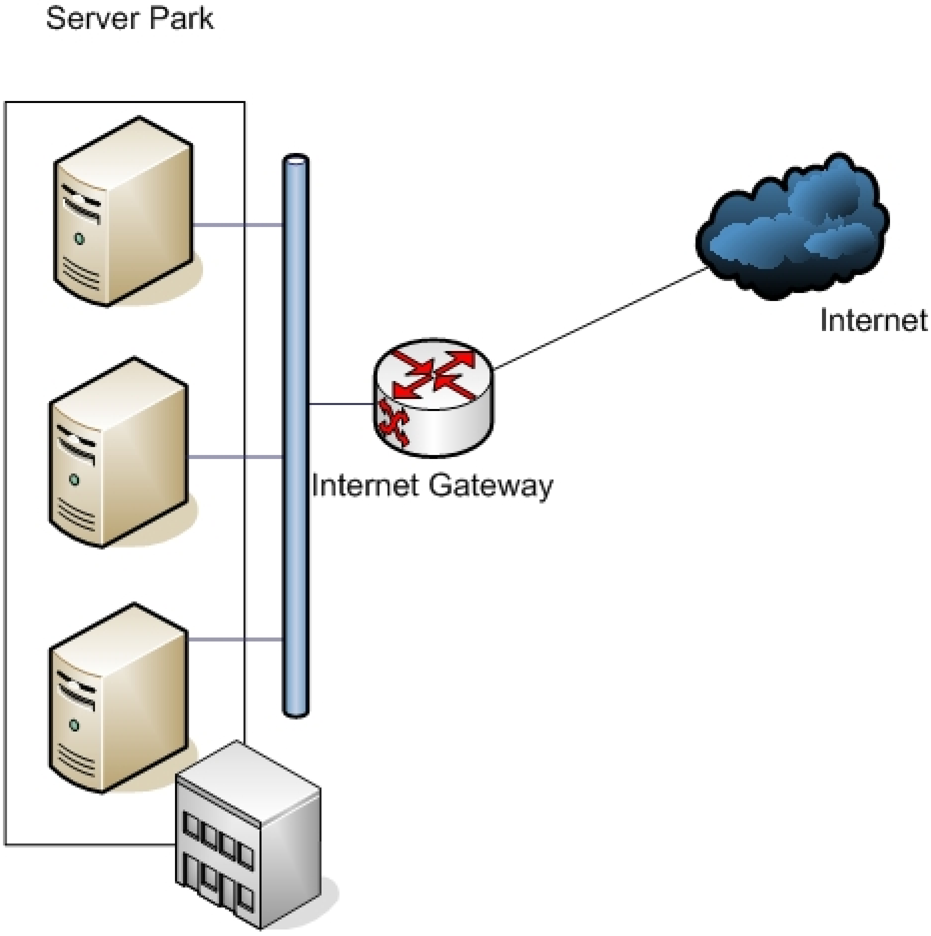


Figure 15: Ethernet LAN architecture

4.1.4. User Terminals – Server Park communication

The Interaction Server is the entrance point for end-user terminals to the functionality of the server-side of eu-DOMAIN regarding web-based interaction. The Interaction Server is accessible from multimodal terminals (e.g., laptops, PDA, mobile phones) from which requests are created and passed through the Interaction Server to other elements on the server-side. The resulting reply is rendered and shown to end-user again using the Interaction Server (displaying the information in a web browser).

Wireless Access will be used by mobile terminals (e.g. mobile phones, PDA, laptops) providing users with a high level of mobility. Outside locations this may be achieved by using WANs such as GPRS or UMTS; inside locations, mobile terminals may more conveniently access an existing wireless network (using e.g. WiFi technology…). In this case, the terminal will authenticate with the existing wireless network infrastructure in some way depending on the security of the network. In case the user uses "fixed" terminals in order to contact with the Interaction Server (PCs, laptops), DSL or Cable are the most suitable technologies to provide this connection. The architectures and interaction patterns were explained when talking about Client Gateways and Server Park communication channels (4.1.1). We have seen how a Client Gateway can connect to the Server Park using Wireless Access Points (Figure 11: Wireless Access Point), (A)DSL (Figure 9: (A)DSL architecture), cable (Figure 10: Cable architecture), GPRS (Figure 12: GPRS architecture) or UMTS (Figure 13: UMTS architecture) technologies. The same schema is applicable to terminals.

There is also another interaction pattern that appears between user mobile terminals with GSM (Global System for Mobile Communications) capabilities and the Server Park. The Rule Engine in the Server Park, for instance, triggers an event when something is happening in the system and the Notification Manager send an appropriate alarm to the suitable target to warn him about the situation. These alarms could be electronic mails or SMS, depending on the configuration of the rules and profiles. We are centring now in SMS interaction. A SMS to be sent and received needs a GSM network behind to transport the message and to communicate the terminals. Figure 16 shows the GSM communication architecture network that is used in eu-DOMAIN (commercial infrastructure), where Mobile Switching Centres (MSC) controls a number of BSC and Signal Transfer Points (STP) provide interconnection with the Short Message Centre (SMSC).

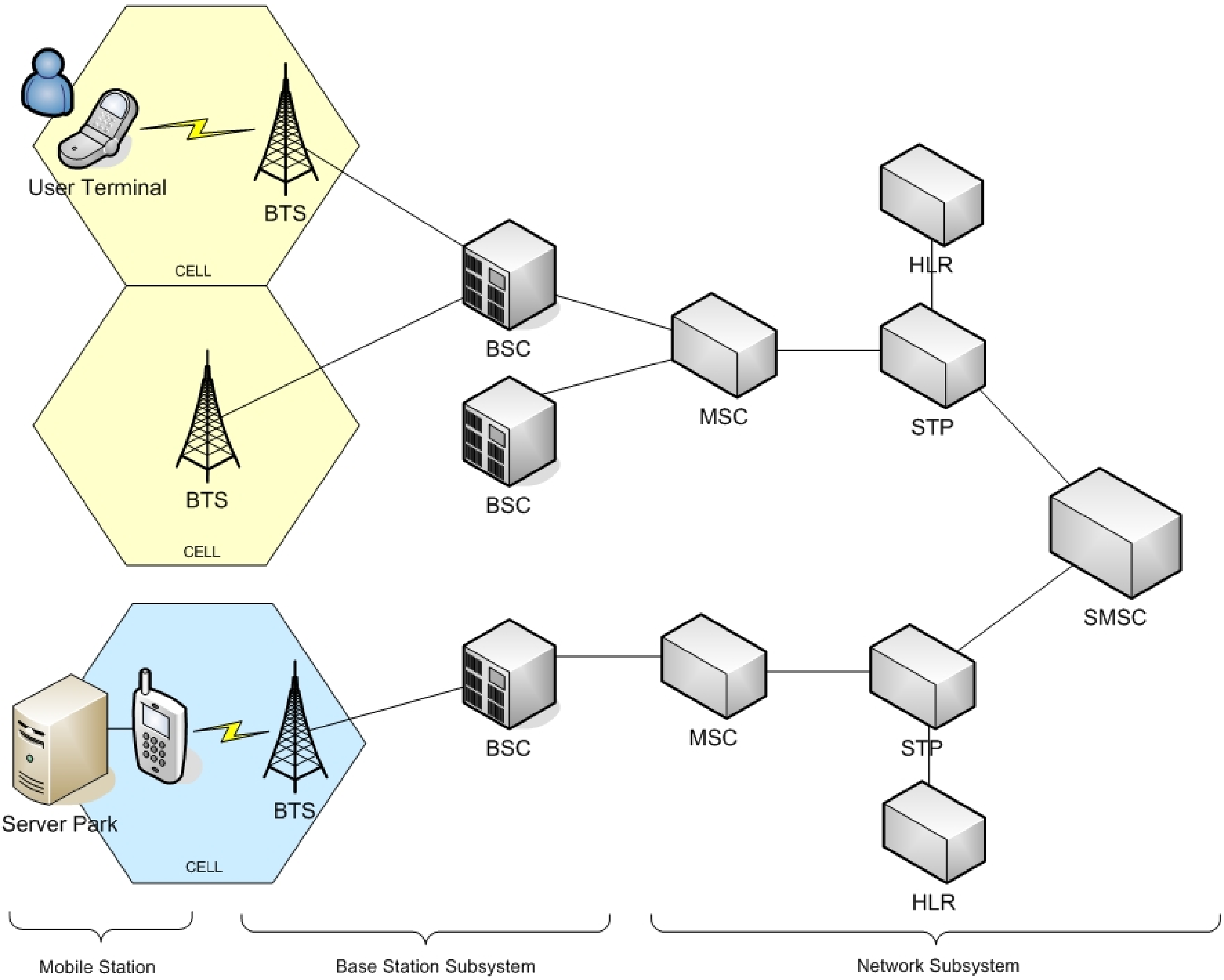


Figure 16: GSM architecture

4.1.5. User Terminals – Client Gateways communication

Terminals, as explained above, are the means for end user interaction with the eu-DOMAIN platform. The interaction with eu-DOMAIN platform will be web-browser based.

If terminals are not able to contact any of the existing commercial infrastructure to gain internet access and thus connect to the Server Park and the terminal is within the range of coverage of a Client Gateway, the eu-DOMAIN gateways at a location can be used as wireless access points and routers (proxies) providing internet access to terminals, so that, means to contact with the

Interaction Server. Figure 17 shows this situation. It has to be pointed out that Client Gateways do not provide any other services to terminals. They use them as proxies in the situation exposed.

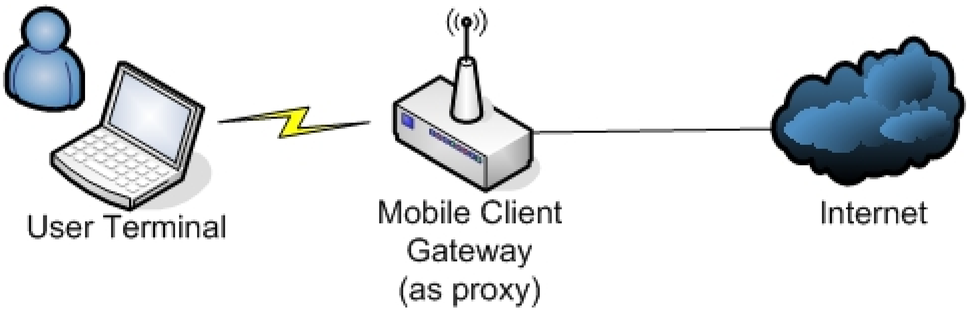


Figure 17: Terminal - Client Gateway communication

Client gateways provide a wireless access point and the access the Internet using any of the communication infrastructures explained in 4.1.1 in this deliverable.

4.1.6. Devices – Client Gateways communication

Devices are actuators, sensors, or processors that are installed and operated in a eu-DOMAIN location. At any point in time, devices are connected to one gateway.

Bundles in the Client Gateways control devices connected to them, and publish web services to allow communication from and to the Server Park. Devices are connected either wirelesses or wired with the local gateway server. This connection depends on the selected devices and can be accessible via serial communications (RS-232, USB), Bluetooth, etc. In this sense, Client Gateways should support different ways of interaction. The question in here is that each device, although it uses an standard communication protocol, uses a proprietary one for data interchanging, so it is up to manufacturers to create bundles to control devices in eu-DOMAIN (the bundles needed are standard OSGi software packages) or to open the protocol to developers. As an example, two different blood pressure monitors will be connected to Client Gateways. They both use RS-232 to be connected, but the data interchange protocols are quite different. Figure 18 shows this situation.

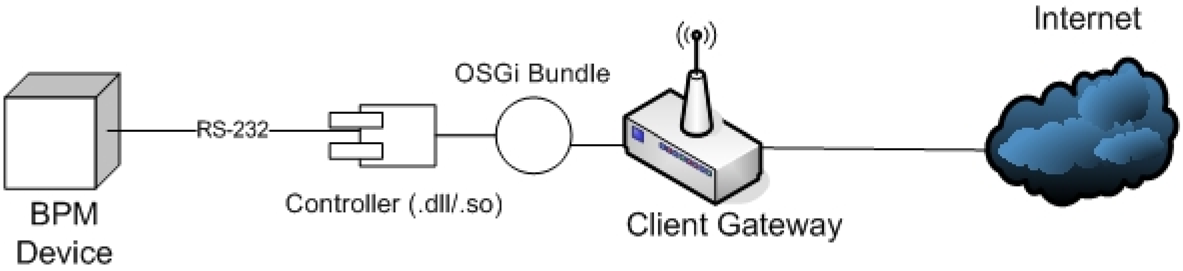


Figure 18: RS-232 communication

4.1.7. Localisation

eu-DOMAIN infrastructure tries to help workers in mobility in their daily activity. In this way, it is envisioned to include localisation technologies in eu-DOMAIN. Nevertheless, localisation techniques are not included for the moment in the ESN or PaC scenarios. The idea is to keep track of the position of technician or nurses, for example, so that when a task has to be performed the nearer resource is moved to the location where the task has to be accomplished. In order to provide this functionality, users have to carry GPS enabled terminals, or include GPS modules in their vehicles. At this moment, for civil localisation purposes, the American system is being used. Europe will have their own and improved system (Galileo) by 2010. Figure 7: GPS Localisation System indicates how localisation is perfumed.

4.1.8. TETRA Networks

At the beginning of the project, eu-DOMAIN infrastructure was going to make use of the benefits of a TETRA network. In fact, a TETRA network infrastructure was going to be provided by Motorola but they were not longer involved in the project and the budget needed to incorporate a commercial TETRA network in the project was unaffordable. Another circumstance that makes us think in other solutions was that TETRA network is supposed to be used in very specific environments, such as emergency, fire or police services, so that it is not a widely spread technology and it is not common in every domain, while eu-DOMAIN solution tries to build a general infrastructure adaptable to every domain with little changes. Moreover, the fact that Motorola was not going to support the use of the network was another factor to exclude TETRA networks from the eu-DOMAIN communication infrastructure. Nevertheless, other technologies, as the ones studied above were incorporated in the communication architecture infrastructure in order to provide similar functionality as the one provided by TETRA, at least for data interchanging, as voice transmissions are not included in the platform for the moment. GSM/GPRS/UMTS are used in order to connect workers in mobility with the Server Park along with fixed networks, and in this way data interchanging between elements in the architecture is solved. Moreover, as the communications in eu-DOMAIN are based on TCP/IP protocols and TETRA networks provide Packet Switched Data Services based on TCP/IP or X.25 protocol, depending on application, with a maximum data rate of 28.8 kbit/s, this technology could be incorporated to a specific installation in a determined domain if it is needed. Due to the cost and the low availability of the TETRA networks, it was decided that TETRA networks will not be longer used in the project. An overview of this technology is provided in 8.14 section.

4.2. Communication prototype infrastructure in eu-DOMAIN

When integrating the different components of the eu-DOMAIN prototypes, the Server Park and the Client gateway will be installed in Telefónica I+D facilities. So, TID is in charge of providing access to the eu-DOMAIN platform from outside its facilities.

We have presented the different technologies that could be used to build the entire eu-DOMAIN platform. Taking into account the communication infrastructures already available at TID facilities (where the Server Park will be installed) and the commercial infrastructure that is ready to be used, we can provide an overall vision of the communication channels and technologies that have been chosen. This vision is summarised in Figure 19.

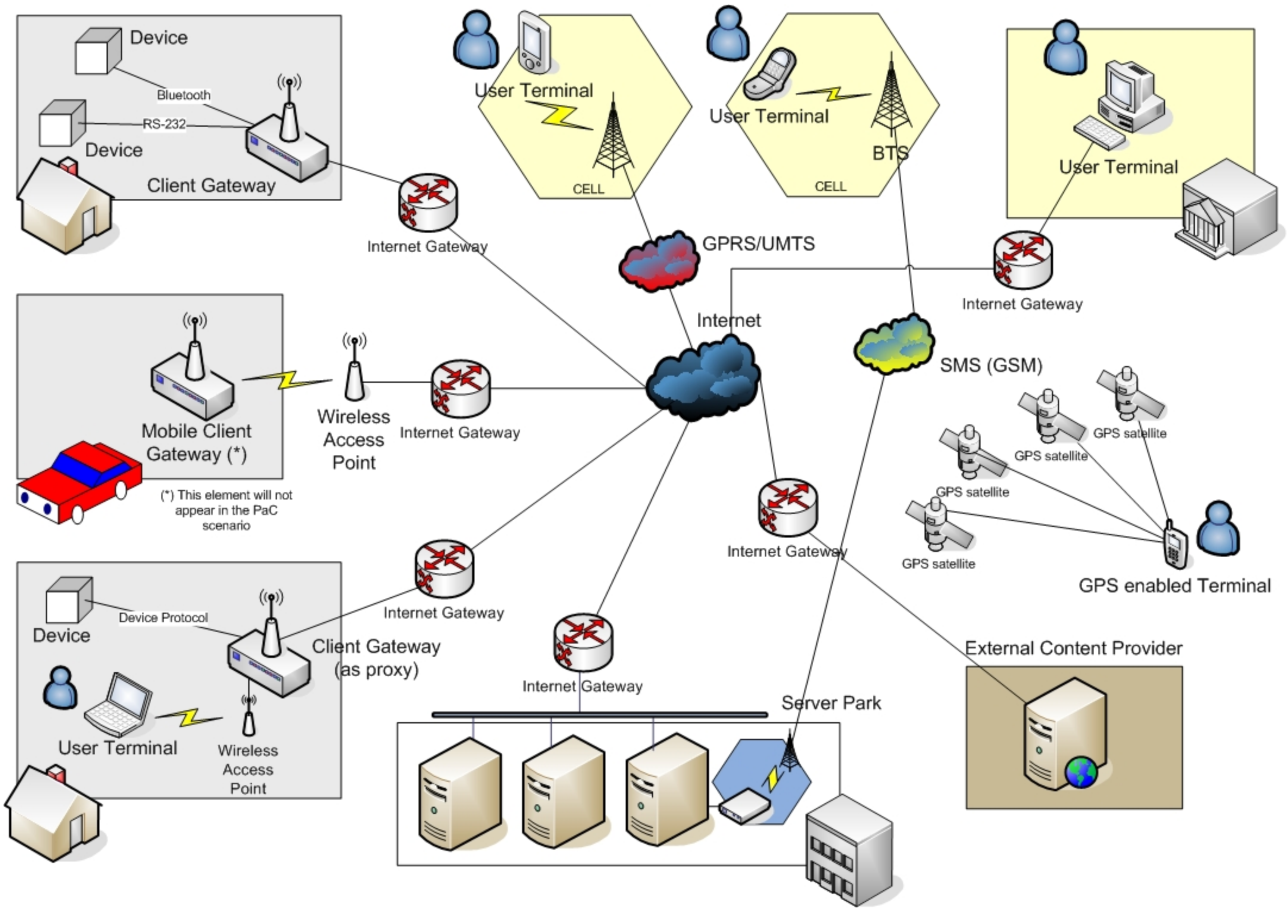


Figure 19: eu-DOMAIN communication infrastructure

The figure shows the communication infrastructure needed in eu-DOMAIN. As it was explained before, the idea is that any communication technology that supports TCP/IP connection is feasible for the infrastructure. This gives us a wide range of technologies to use. Let's see how each component is able to connect to the others:

- The Server Park, that will be located in TID facilities, provides intercommunication between software agents within the Server Park using TID intranet (Ethernet LAN). Moreover, using a NAT, we will be able to provide the services outside TID facilities. This gives eu-DOMAIN Server Park access to the Internet. Also in the Server Park, a GSM gateway will be installed and controlled by the Notification Manager to be able to send SMS to users using commercial GSM networks. Other distributed architectures using VPN for security reasons are possible but they will not be used for the prototypes.
- Client Gateways could be fixed or mobile. It is envisioned that for the first prototypes, only fixed ones will be used. They will use commercial infrastructure ((A)DSL, cable, mainly) to access the Server Park and to expose their services to it. A number of sensors and actuators, each one using their communication technology (RS-232, Bluetooth) and their proprietary protocols for communication. Anyway, Client Gateways will publish web services for each device, so that interoperability is assured at service level. The idea is to have:
    - A Client Gateway for the ESN scenario running in Aarhus (Denmark) [UAAR]
    - A Client Gateway for the Pac Scenario located in Valladolid (Spain) [TID]
    - Another Client Gateway installed in Crete (Greece) [FORTH]
- User Terminal will make use of Telco operators' networks available in the market. For the prototypes in TID facilities, terminals within TID facilities will make use of the wired and wireless Intranet to be able to access the Server Park. It is possible also in some cases that

they will be able to connect to Internet using the connection Client Gateways provide, using them as. Moreover, terminals can also use mobile networks such as GPRS or UMTS where available to have Internet access, and thus access to the services in the Server Park. This functionality is really interesting for workers in mobility. Finally, mobile terminals using GSM network can receive alerts and alarms from the system in the shape of SMS messages (the GSM gateway in the Server Park will send it, using commercial infrastructure).

- External Content Providers will expose their services as web services in Internet. It is a decision of the provider to select the communication technology to use. The only requirement for their services to be plugged and thus offered in eu-DOMAIN is that they provide a web service interface reachable from the Server Park.

As the architecture shows, a number of communication technologies can be used, which means that the eu-DOMAIN platform relies on heterogeneous commercial networks and that this is done transparently to users. They just need an Internet connection, no matter the communication technology they use to do it. All the communications, apart from the ones between devices and the Client Gateways, are based on HTTP(S) transfers (TCP/IP). Interoperability at service level is provided using web services technologies.

5. Security issues

This section tries to present the security problems identified and the solutions proposed regarding communication interactions. The overall security architecture is studied and described in [eu-DOMAIN Security, 2005] and it is not the objective of this deliverable to present it again. These security issues are not specific to any of the applications (ESN or PaC) implemented in the eu-DOMAIN platform, so that it is a general framework independent of the domain where the eu-DOMAIN platform is installed. It is important to highlight that the server is a secure environment completely under our control whereas the client side is not a controlled set of components. Hence, we can identify different components that need different security mechanisms in eu-DOMAIN:

- Server Park: communications among software agents are secured as the environment is secured. In case the Server Park is spread over different locations, the use of a VPN will be needed in order to secure the interchange of data over the network. The main concern here is access control from the outside. Anyway, the solution for the prototypes will not need a VPN, as the different servers will be located in the same facilities, for the PaC scenario, in TID facilities in Boecillo (Valladolid - Spain).
- External communication from the server, which includes communications with External Content Providers, Client Gateways and Terminals from and to the Server Park. We need to secure that communication to provide confidentiality, integrity availability and in some cases non-repudiation.
- Client Gateways: we have gateways, terminals and devices. Some of these entities might contain sensitive information that needs protection. The gateway and the devices must also perform security checks on incoming messages. Moreover, we have to provide confidentiality, integrity, availability and in some cases non-repudiation for device-Client Gateway communication in case the device offer that possibility, which is not the usual case.

The Server Park will be protected behind a set of network firewalls. These firewalls prevent certain outside connections from entering the Server Park. TID LAN uses different firewalls to protect the elements in the internal network. The first line of defence in firewall protection is the packet filter firewall which operates at the Network Layer to examine incoming and outgoing packets and apply a fixed set of rules to the packets to determine whether they will be allowed to pass. It is typically very fast because it does not examine any of the data in the packet. It simply examines the IP packet header, the source and destination IP addresses, and the port combinations, then it applies filtering rules. Then, Circuit-level Gateways are used to monitor all connections and only those connections that are found to be valid are allowed to pass through the firewall. This generally means that a client behind the firewall can initiate any type of session, but clients outside the firewall cannot see or connect to a machine protected by the firewall. Moreover, a Network Address Translation (NAT) is used to completely hide the network protected by the firewall by using many-to-one address translation. The Server Park will offer a single public IP address. All packets going outside the network have their internal IP addresses hidden for security, so any incoming packets are delivered to the network's public IP address. To handle ensuing port conflicts, a Port Address Translation (PAT) needs to be added to NAT. Finally, a demilitarized zone (DMZ) isolates the Server Park (the Interaction Server) from internal servers. The external hosts are placed in a separate network zone, on a separate adapter, connected to the firewall. Each subnetwork is also configured with its own security zone by connecting it to a separate firewall adapter. All traffic between zones, and all traffic from the Internet to all zones, is checked by the firewall. This infrastructure is shown in Figure 20: Server Firewall Security.

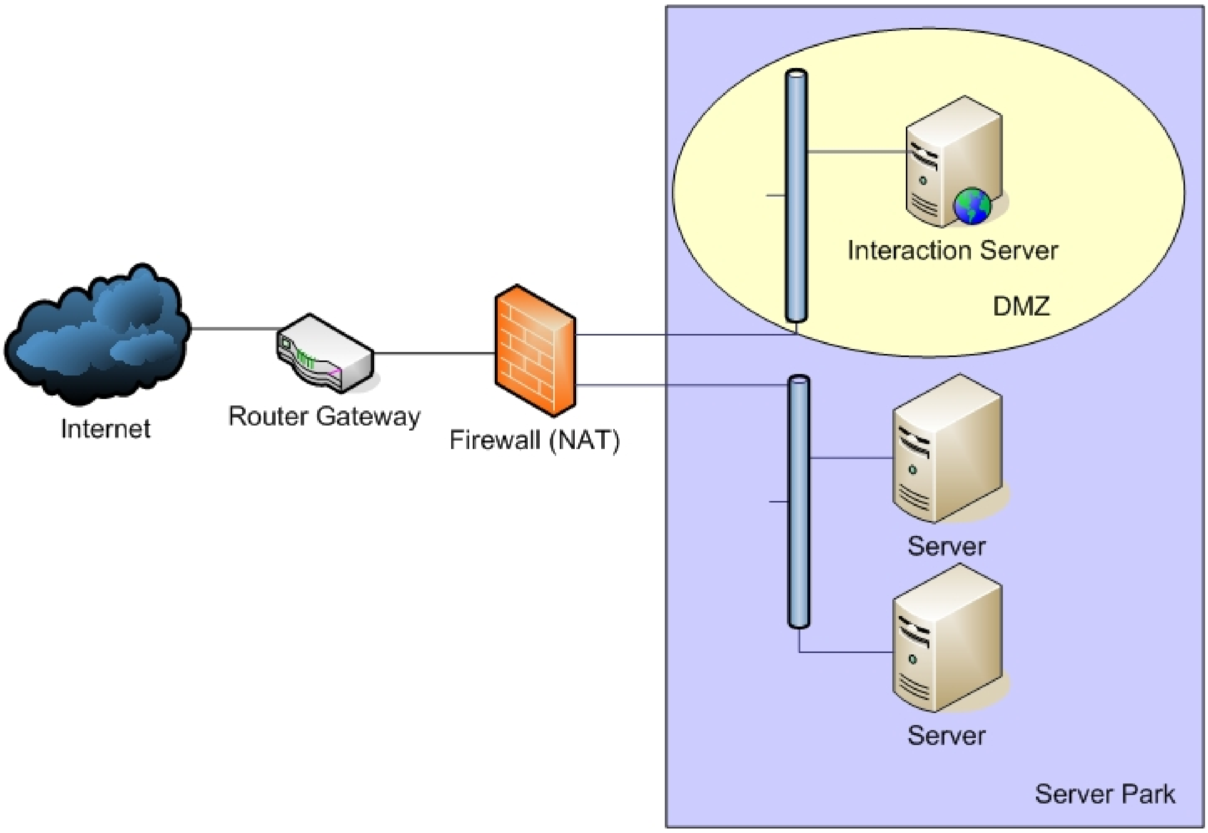


Figure 20: Server Firewall Security

The general security infrastructure envisioned to use Vordel products in order to check the access from external service providers and verifying the correctness of XML documents, and perhaps also for enforcing the security policy internally on the server side. Nevertheless, another security policy is used for the publish/subscribe architecture and other components that are not based entirely on web services. The problem is that we would need two separate security policies if we go for this hybrid solution. The decision adopted for the demonstrators (ESN & PaC) was that managers will enforce access to their services using the security manager and that this will be accomplished without Vordel. The goal of the Security Architecture is to implement object-level security (OLS) where each piece of data in the system has information about who can access that data. For example in a database that stores blood pressure measurements, there will be information about who can access these measurements. In short, Vordel provides interface security, where you define who is allowed to invoke a specific web service, but Vordel does not allow these decisions to be based upon information contained in the request, only on who made the request. So the OLS approach is not possible to implement with Vordel alone. For instance, Vordel can only enforce the policy that a given user is allowed to invoke a method called getBloodpressureMeasurement(...). It can not check whether the user is trying to invoke getBloodpressureMeasurement(Alice) or getBloodpressureMeasurement(Bob). The latter should be enforced by the manager trying to get the measurements. This of course means that the manager needs information about who is trying to get the data, but this is available in the SAML assertion in the request, and then the manager can ask the security manager about whether or not to allow the request. This means that the security infrastructure will not include Vordel products for the demonstrators, although it could be incorporated in some situations.

In order to secure the communications between External entities (Client gateways, External Content Provider and Terminals) and the Server Park (SOAP and HTML), hawse have chosen to use communications over a TLS connection established though the use of client certificates. In this way, eu-DOMAIN uses HTTPS protocol instead of HTTP when communicating elements. This provides not only confidentiality and integrity, but also establishes the identity of the entity accessing the server.

Furthermore, the client certificates can be reused in other cases for example to sign documents thereby providing non-repudiation.

The eu-DOMAIN SOA architecture is based on the interchange of SOAP messages. To secure this communication we use WS-Security to represent security attributes in SOAP headers. These attributes will be SAML documents where entities and their credentials are expressed as SAML assertions. One of the main advantages of using SAML in SOAP messages is that the same message can be passed between a number of components and the last component in the chain is still able to determine the source of the message. The decision of using WS-Security to secure communications when interchanging SOAP messages is based on the following requirements:

- The communication should not be able to be viewed by a third party as it travels on the Internet. Using HTTPS/SSL we are able to solve this problem
- The recipient must be able to determine from whom the message was coming and be able to verify that the sender was who the sender claimed to be. Digital signatures and digital certificates will be used for this purpose in eu-DOMAIN
- The recipient needs to ensure that the data being transmitted was not tampered with. Also the use of digital signatures and certificates in needed to address this requirement in eu-DOMAIN

There is a special case, when we connect External Content Providers which already have their own user database with the Server Park. In this case we need to integrate both security systems. WS-Trust can be used to exchange SAML documents between the two systems.

Client Gateway communicates with the Server Park over a TLS connection established using the gateway's certificate. This provides the necessary protection for this communication channel.

A terminal communicates with the interaction server only through a browser, so here a TLS connection with client a certificate is also used.

Devices communicate with the Client Gateways using many different protocols ranging from wired RS232 to Bluetooth and WiFi. The device bundle is responsible for handling the device protocol as well as any security features in it, but the device security gateway will provide an API that the bundle must use when communicating security related information to the gateway if the device supports it. The security architecture description in eu-DOMAIN identifies three different types of devices:

- Devices that only prove their identity to the gateway by claiming to have a specific identity. They cannot store information such as access control lists, so they will accept any request they receive.
- Devices that support symmetric cryptography for proving their identity towards the gateway and securing the communication channel.
- Devices that support public key cryptography.

6. Conclusions

We have presented and discussed the communications infrastructure architecture for the eu-DOMAIN platform in this deliverable.

We have showed an overview of the designed software architecture [eu-DOMAIN D3.1+D4.1, 2005], which is the basis for the communications architecture itself. User requirements [eu-DOMAIN D2.1, 2005], [eu-DOMAIN D2.3, 2005] regarding communication issues are selected and explained in terms of how to address them regarding the communications infrastructure. The Validation Plan in eu-DOMAIN will assure that the requirements are fulfilled.

This architecture requires that a Server Park will play the role of the central point in the architecture. A number of clients, governed by OSGi gateways will connect with the server side. The communication is performed using commercial infrastructure. Sensors and actuators are controlled in client side by bundles in the residential gateway. They are wired (USB, RS-232) or wireless (Bluetooth, ZigBee, WiFi, etc.) technologies to be connected to the OSGi gateway. Apart from these elements, we can find user terminals in the architecture. User interaction is web based and thus, connection with the server side is needed. This is acquired using commercial infrastructure (DSL, cable, GSM, GPRS, UMTS, etc.) or connecting through the connection provided by the client gateways. Moreover, external content providers can be plugged to the server side. Interoperability is performed using web services and the communication is based in commercial communication infrastructure again. Finally, SMS (over GSM networks) is used to send alarms to users whenever is needed.

The communication architecture chosen for eu-DOMAIN is based on commercial infrastructure and, in terms of the demonstrators, a Server Park will be integrated and installed in TID facilities, where we will provide external access to the services offered. Any client could connect to the server side. A client will be also installed in the TID facilities to show the overall eu-DOMAIN infrastructure. User terminals will be able to connect to the server using wireless access points inside TID facilities or any commercial infrastructure, if the terminal is outside the TID facilities. External content providers will need to provide access to their own services to be plugged into the infrastructure.

The proposed architecture covers the entire purpose of the communication architecture, where all the communication channels are explained and a solution is proposed in order to be able to communicate the different element and devices in the eu-DOMAIN architecture. The use of a commercial infrastructure makes things easier in terms of exploiting the system and making it working in the real world. Once exploitation starts, it is time to address issues like the bandwidth needed, as the number of users and data to be transmitted differs from one domain case to another.

7. References

[Answers, 2006] “RS-232”, Answers.com, 2006, http://www.answers.com/topic/rs-232

[Bass et al., 2003] Bass, L., Clements, P., and Kazman, R. (2003). *Software Architecture in Practice*. Addison-Wesley, 2nd edition.

[Bluetooth, 2006] “Learn Bluetooth”, Bluetooth, 2006, http://www.bluetooth.com/

[Cisco, 2000] “GPRS White Paper”, Cisco, 2000, http://www.cisco.com/warp/public/cc/so/neso/gprs/gprs_wp.pdf

[Digitalsmart, 2004] “Wi-Fi”, Digitalsmart, 2004, http://www.digitalsmart.net/articles/Wi-Fi

[Dodd, 2002] “Universal Advantages of USB”, Dodd J., 2002, http://www.smartcomputing.com/editorial/PrntArticle.asp?prnt=1&article=articles%2Farchive%2Fl0811%2F18l11%2F18l11.asp&guid=

[eu-DOMAIN D2.1, 2005] Thestrup J, et alli (2005), *D2.1 User Validation Framework Plan*, eu-DOMAIN deliverable

[eu-DOMAIN D2.3, 2005] Aiello I, et alli (2005), *D2.3 Functional user requirements specifications*, eu-DOMAIN deliverable

[eu-DOMAIN D2.4, 2004] Pagter J, et alli (2004), *D2.4 Trust and Security user requirements specifications*, eu-DOMAIN deliverable

[eu-DOMAIN D3.1+D4.1, 2005] UAAR, CNET (2005), *Software Architecture Specification,* eu-DOMAIN deliverable

[eu-DOMAIN Security, 2005] UAAR (2005), *Security Architecture Description,* eu-DOMAIN

[GPS, 2006] “Global Positioning System”, Wikipedia, 2006, http://en.wikipedia.org/wiki/GPS

[GSM, 2006] “Today’s GSM Platform”, GSM World, 2006, http://www.gsmworld.com

[Interworking, 2005] “Digital Subscriber Line”, Interworking Technologies Handbook (chapter 21), 2005 http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/dsl.htm

[Kinney, 2003] Kinney, P. (2003), *ZigBee Technology: Wireless Control that Simply Works*, white http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=5162

[TETRA, 2006] “TETRA – Terrestrial Trunked radio”, Will’Tek, 2006, http://www.willtek.com/english/technologies/tetra

[UMTS, 2006] “3G and UMTS Technology”, UMTS World, 1999-2006, http://www.umtsworld.com/

[Wimax, 2006] “Technical information”, WIMAX Forum, 2006, http://www.wimaxforum.org/home

8. Annex A. Communication technologies

8.1. ADSL

Asymmetric Digital Subscriber Line is a form of DSL [Interworking, 2005], a data communications technology that enables faster data transmission over copper telephone lines than a conventional modem can provide. *ADSL* converts existing twisted-pair telephone lines into access paths for multimedia and high speed data communications.

An ADSL circuit connects an ADSL modem on each end of a twisted-pair telephone line, creating three information channels -- a high speed downstream channel, a medium speed duplex channel, and a POTS (Plain Old Telephone Service) channel. The POTS channel is split off from the digital modem by filters, thus guaranteeing uninterrupted POTS, even if ADSL fails. The high speed channel ranges from 1.5 to 6.1 Mbps, while duplex rates range from 16 to 640 kbps. Each channel can be sub-multiplexed to form multiple, lower rate channels. Two separate frequency bands are used. With standard ADSL, the band from 25.875 kHz to 138 kHz is used for upstream communication, while 138 kHz - 1104 kHz is used for downstream communication. Talking about modulation methods, ADSL initially used CAP and DMT. CAP was the *de facto* standard for ADSL deployments up until 1996, deployed in 90 percent of ADSL installs at the time. However, DMT was chosen for the first ITU-T ADSL standards, G.992.1 and G.992.2. Therefore, all modern installations of ADSL are based on the DMT modulation scheme.

Data rates provided by ADSL modems are consistent with North American and European digital hierarchies and can be purchased with various speed ranges and capabilities. The minimum configuration provides 1.5 or 2.0 Mbps downstream and a 16 kbps duplex channel; others provide rates of 6.1 Mbps and 64 kbps duplex. Products with downstream rates up to 8 Mbps and duplex rates up to 640 kbps are available today. ADSL modems will accommodate ATM transport with variable rates and compensation for ATM overhead, as well as IP protocols. Other versions of ADSL, such as ADSL2 or ADSL2+ provide higher downstream rates of up to 12 Mbps for spans of less than 2.5 km and 24 Mbps for spans of less than 1.5 km, respectively thanks to higher symbol rates and more advanced noise shaping.

8.2. Cable

Cable television (CATV) (often shortened to cable) is a system of providing television, FM radio programming and other services to consumers via radio frequency signals transmitted directly to people's televisions through fixed optical fibres or coaxial cables as opposed to the over-the-air method used in traditional television broadcasting (via radio waves) in which a television antenna is required.

Both, coaxial cables and optical fibre are used to deploy a communication infrastructure based on CABLE. Coaxial cables are capable of bi-directional carriage of signals as well as the transmission of large amounts of data. Cable television signals use only a portion the bandwidth available over coaxial lines. This leaves plenty of space available for other digital services such as broadband internet and cable telephony. The optical fibre can be used as a medium for telecommunication and networking because it is flexible and can be bundled as cables. Although fibres can be made out of either transparent plastic or glass, the fibres used in long-distance telecommunications applications are always glass, because of the lower optical attenuation. Two kinds of fibre optic cables are used: Single Mode cable (carries higher bandwidth than multimode fibre, but requires a light source with a narrow spectral width) and Multimode cable (gives high bandwidth at high speeds over medium distances).

Along with DSL technology, cable modems ushered in the age of broadband Internet access in developed countries. Cable modems usually deliver speeds comparable to that of DSL; however, DSL modems generally have better upload speeds. Prior to the availability of such systems, Internet access involved slow dial-up access over a public switched telephone network.

8.3. GSM

The Global System for Mobile Communications (GSM) [GSM, 2006] is the most popular standard for mobile phones in the world. GSM phone are used by over a billion people across more than 200 countries. The ubiquity of GSM standard makes international roaming very common with “roaming agreements” between mobile phone operators. GSM differs significantly from its predecessors in that both signalling and speech channels are digital, which means that it is seen as a second generation mobile phone system. GSM is an open standard which is currently developed by the 3GPP (3rd Generation Partnership Project).

GSM standard provides recommendations, not requirements. It specifications define the functions and interface requirements in detail but do not address the hardware. The reason for this is to limit the designers as little as possible but still to make it possible for the operators to buy equipment from different suppliers.

The GSM network is divided into three major systems:

- The switching system (SS) is responsible for performing call processing and subscriber-related functions.
- The base station system (BSS) is in charge of performing all radio-related functions. BSS consist of base station controllers (BSC) and the base transceiver stations (BTS).
- The operation and support system (OSS) is connected to all equipment in the switching system and to the BSC. The implementation of OMC is called the operation and support system (OSS). The OSS is the functional entity from which the network operator monitors and controls the system. The purpose of OSS is to offer the customer cost-effective support for centralized, regional and local operational and maintenance activities that are required for a GSM network. An important function of OSS is to provide a network overview and support the maintenance activities of different operation and maintenance organizations.

There are two basic types of services offered through GSM: telephony (also referred to as teleservices) and data (also referred to as bearer services). Data services provide the capacity necessary to transmit appropriate data signals between two access points creating an interface to the network.

8.4. GPRS

General Packet Radio Service (GPRS) [Cisco, 2000] is a 2.5G mobile communications technology that enables mobile wireless service providers to offer their mobile subscribers with packet-based data services over GSM networks. GPRS involves overlaying a packet based air interface on the existing circuit switched GSM network. Information is split into separate packets and then reassembled at the receiving end.

GPRS requires an upgrade to the GSM network. GPRS architecture consists of Gateway GPRS Support Node (GGSN) and a Serving GPRS Support Node (SGSN). The GGSN acts as the gateway to other packet data networks such as the Internet. The SGSN is the serving node that enables virtual connections to the GPRS enabled mobile device and delivery of data. GGSN provides interworking with external packet-switched networks, and is connected with SGSNs via an IP-based GPRS backbone network.

The use of the spectrum is more efficient since packet switching means that GPRS radio resources are used only when users are actually sending or receiving data. Rather than dedicating a radio channel to a mobile data user for a fixed period of time, the available radio resource can be concurrently shared between several users.

GPRS also allows faster data rates than GSM. Theoretical maximum speeds of up to 171.2 kilobits per second (kbps) are achievable with GPRS using all eight timeslots at the same time.

Regarding security functionality, GPRS security is equivalent to the existing GSM security. The SGSN performs authentication and cipher setting procedures based on the same algorithms, keys, and criteria as in existing GSM. GPRS uses a ciphering algorithm optimized for packet data transmission.

8.5. UMTS

Standing for "Universal Mobile Telecommunications System", UMTS [UMTS, 2006] represents an evolution in terms of services and data speeds from today's "second generation" mobile networks. UMTS is the natural evolutionary choice for operators of GSM networks, currently representing a customer base of more than 850 million end users in 195 countries and representing over 70% of today's digital wireless market [source: GSM Association].

UMTS network consist of three interacting domains:

- Core Network provides switching, routing and transit for user traffic. Core network also contains the databases and network management functions. The basic Core Network architecture for UMTS is based on GSM network with GPRS.
- UMTS Terrestrial Radio Access Network (UTRAN) provides the air interface access method for User Equipment. Wide band CDMA technology was selected to for UTRAN air interface. UMTS WCDMA is a Direct Sequence CDMA system where user data is multiplied with quasi-random bits derived from WCDMA Spreading codes. In UMTS, in addition to channelisation, Codes are used for synchronisation and scrambling.
- User Equipment

UMTS offers teleservices and bearer services, which provide the capability for information transfer between access points. It is possible to negotiate and renegotiate the characteristics of a bearer service at session or connection establishment and during ongoing session or connection. Both connections oriented and connectionless services are offered for Point-to-Point and Point-to-Multipoint communication

UMTS is already a reality. Japan launched the world's first commercial WCDMA network in 2001, and WCDMA networks are now operating commercially in Austria, Italy, Sweden, UK, Spain, etc.

8.6. WiMAX

It is an alternative or complement to 3G Technologies. WiMAX [Wimax, 2006], or Worldwide Interoperability of Microwave Access, is a wireless Internet service designed to cover wide geographical areas serving large numbers of users at low cost. WiMAX is the synonym given to the IEEE 802.16 standard defining wide area wireless data networking.

WiMAX is the standard being adopted worldwide by manufacturers to insure inter-operability of equipment. WiMAX is considered one of the best solutions for extending the currently limited coverage of WLAN to citywide coverage. The achievable coverage will be up to 50 km under optimal conditions and with a reduced data rate. However the typical coverage will be around 5 km with indoor equipment (no line of sight) and around 15 km with equipment connected to an external antenna (line of sight).

This technology will be particularly beneficial to many rural areas and other locations where broadband access is not currently available

The original WiMAX standard, IEEE 802.16, specifies WiMAX in the 10 to 66 GHz range and require line of sight of towers. 802.16a added support for the 2 to 11 GHz range, enabling no line of sight connections. The latest 802.16e task group is capitalizing on the new capabilities this provides by working on developing a specification to enable mobile 802.16 clients. These clients will be able to hand-off between 802.16 base stations, enabling users to roam between service areas.

Nowadays, several companies are working in order to deploy WiMAX networks around the world developed by Intel Corporation. These networks will offer wireless access to companies and residences in countries such as Germany or Guatemala (http://www.pc-news.com/detalle.asp?sid=&id=5&Ida=2217).

8.7. WiFi / IEEE 802.11

WiFi [Digitalsmart, 2004] is a set of wireless internet product compatibility standards for wireless local area networks (WLAN) based on the IEEE 802.11 specifications.

Unlike packet radio systems, WiFi uses unlicensed radio spectrum (2.4 GHz) does not require regulatory approval for individual deployers. Allows LANs to be deployed without cabling, potentially reducing the costs of network deployment and expansion. Spaces where cables cannot be run, such as outdoor areas and historical buildings, can host wireless LANs.

The typical WiFi setup contains one or more Access Points (AP's) and one or more clients. An AP broadcasts its SSID (Service Set Identifier, Network name) via packets that are called beacons, which are broadcasted every 100ms. The beacons are transmitted at 1Mbps, and are relatively short and therefore are not of influence on performance. Since 1Mbps is the lowest rate of WiFi it assures that the client who receives the beacon can communicate at least 1Mbps. based on the settings (i.e. the SSID), the client may decide whether to connect to an AP. Also the firmware running on the client WiFi card is of influence. The WiFi standard leaves connection criteria and roaming totally open to the client. This is strength of WiFi, but also means that one wireless adapter may perform substantially better than the other. In the future wireless cards will be more and more controlled by the operating system. Roaming criteria will be totally controlled by the operating system. WiFi transmits in the air; it has the same properties as a non-switched Ethernet network. Even collisions can therefore appear like in non-switched Ethernet LAN's.

WiFi networks have limited range. A typical WiFi home router using 802.11b or 802.11g might have a range of 45 m (150 ft) indoors and 90 m (300 ft) outdoors. Range also varies, as WiFi is no exception to the physics of radio wave propagation, with frequency band. WiFi in the 2.4 GHz frequency block has better range than WiFi in the 5 GHz frequency block, and less range than the oldest WiFi (and pre-WiFi) 900 MHz block. Moreover, WiFi is a global set of standards. Unlike cellular carriers, the same WiFi client works in different countries around the world.

8.8. Bluetooth

Bluetooth [Bluetooth, 2006] is an industrial specification for *Wireless Personal Area Networks* first developed by Ericsson, later formalized by the Bluetooth Special Interest Group (SIG). It was established by Sony Ericsson, IBM, Intel, Toshiba and Nokia, and later joined by many other companies as Associate or Adopter members.

It is a wireless radio standard primarily designed for low power consumption, with a short range (from 10 up to 100 meters) and with a low-cost transceiver microchip in each device.

It can be used to wirelessly connect peripherals like printers or keyboards to computers, or to have PDAs communicate with other nearby PDAs or computers.
Cell phones with integrated Bluetooth technology have also been sold in large numbers, and are able to connect to computers, PDAs and, specifically, to hands free devices.

The standard also includes support for more powerful longer-range devices suitable for constructing a wireless LAN. Every Bluetooth device can simultaneously maintain up to 7 connections, but only one active connection at the time. These groups (maximum of 8 devices: 1 host and 7 slaves) are called piconets. The Bluetooth specification also enables the possibility to connect two piconetworks together, with one master device acting as a bridge. These devices have yet to come, though are supposed to appear within the next two years. Every device can be configured to constantly announce its presence to nearby devices in order to establish a connection. It is also possible to password protect a connection between two devices so that no one can listen in.

8.9. ZigBee

ZigBee [Kinney, 2003] is a published specification set of high level communication protocols designed to use small, low power digital radios based on the IEEE 202.15.4 standard for *Wireless Personal Area Networks (WPANs)*.

The technology is designed to be simpler and cheaper than other *WPANs* such as *Bluetooth*.

ZigBee is aimed at applications with low data rates and low power consumption. *ZigBee*'s current focus is to define a general-purpose inexpensive self-organizing mesh network that can be shared by industrial controls, medical devices, home automation, etc. The network is designed to use very small amounts of power, so than individual devices might run for a year or two with a single alkaline battery.

Security and data integrity are key benefits of the ZigBee technology. ZigBee leverages the security model of the IEEE 802.15.4 MAC sublayer which specifies four security services:

- Access control: the device maintains a list of trusted devices within the network
- Data encryption, which uses symmetric key 128-bit advanced encryption standard
- Frame integrity to protect data from being modified by parties without cryptographic keys
- Sequential freshness to reject data frames that have been replayed.

Thanks to its features, ZigBee is poised to become the global control/sensor network standard

8.10. UWB

Ultra wideband (UWB) is a wireless communication technology fundamentally different from all other radio frequency communications. It is unique in that it achieves wireless communications without using an RF carrier. Instead it uses modulated high frequency low energy pulses of less than one nanosecond in duration.

Since UWB waveforms are of such short time duration, they have some rather unique properties. In communications, for example, UWB pulses can be used to provide extremely high data rate performance in multi-user network applications. For radar applications, these same pulses can provide very fine range resolution and precision distance and/or positioning measurement capabilities. In fact, multifunction architectures encompassing communications, radar and positioning applications have been developed.

These short duration waveforms are relatively immune to multipath cancellation effects as observed in mobile and in-building environments. Multipath cancellation occurs when a strong reflected wave – e.g., off of a wall, ceiling, vehicle, building, etc. – arrives partially or totally out of phase with the direct path signal, causing a reduced amplitude response in the receiver. With very short pulses, the direct path has come and gone before the reflected path arrives and no cancellation occurs. As a consequence, UWB systems are particularly well suited for high-speed, mobile wireless applications. In addition, because of the extremely short duration waveforms, packet burst and time division multiple access (TDMA) protocols for multi-user communications are readily implemented.

Among the most important advantages of UWB technology, however, are those of low system complexity and low cost. UWB systems can be made nearly "all-digital", with minimal RF or microwave electronics. Because of the inherent RF simplicity of UWB designs, these systems are highly frequency adaptive, enabling them to be positioned anywhere within the RF spectrum. This feature avoids interference to existing services, while fully utilizing the available spectrum.

8.11. RS-232

RS-232 [Answers, 2006] is a standard for serial binary data interconnection between a DTE (Data terminal equipment) and a DCE (Data Communication equipment). Communication as defined in the RS232 standard is an asynchronous serial communication method. The information is sent one bit at a time and information is not sent in predefined time slots. Data transfer can start at any given time and it is the task of the receiver to detect when a message starts and ends.

The Electronics Industry Association (EIA) has developed standards for data communication. EIA standards where originally marked with the prefix "RS". "RS" means that it is a recommended standard, but the standards are now generally indicated as "EIA" standards. RS-232 was introduced in 1962. The standard evolved over the years and had the third revision in 1969 (RS-232C). The fourth revision was in 1987(RS-232D also known as EIA-232D).

In RS-232, data is sent as a time-series of bits. Both synchronous and asynchronous transmissions are supported by the standard. Each circuit only operates in one direction, which is, signalling from a DTE to the attached DCE or the reverse. Since transmit data and receive data are separate circuits, the interface can operate in a full duplex manner, supporting concurrent data flow in both directions. The standard does not define character framing within the data stream, or character encoding. Data bits are sent with a predefined frequency, the baud rate. Both, the transmitter and receiver must be programmed to use the same bit frequency. After the first bit is received, the receiver calculates at which moments the other data bits will be received. It will check the line voltage levels at those moments. With RS232, the line voltage level can have two states. The on state is also known as marking, the off state as spacing. No other line states are possible. When the line is idle, it is kept in the marking state.

RS-232 devices may be classified as Data Terminal Equipment (DTE) or Data Communications Equipment (DCE); this defines which wires will be sending and receiving each signal. The standard recommended but did not make mandatory the common D-subminiature 25 pin connector. In general, terminals have male connectors with DTE pin functions, and modems have female connectors with DCE pin functions. Other devices may have any combination of connector gender and pin definitions.

8.12. USB

The Universal Serial Bus [Dodd, 2002] is an external bus (a hardwired connection linking two or more hardware components within a computer system) designed to provide a fast and functional means for adding external components to a PC.

Universal Serial Bus came into life when a group of 7 companies : Compaq, Digital Equipment, IBM, Intel, Microsoft and Northern Telecom decides to form a specifications to merge legacy connectivity such as RS232, Printer port, PS2 port into a single common connector to the Personal Computer. The result: Version 1.0 of the USB specifications delivered on 15 January 1996. Version 1.0 specifies 2 forms of signalling transfer rate: Low Speed (1.5Mbps) and the Full Speed (12Mbps).

Three characteristics define the USB technology: speed (maximum data transmission speed of 480 Mbps), power (a single USB interface is capable of carrying 500 milliamps of electricity to the various hardware components connected to it), and convenience (each USB port is capable of supporting chains of as many as 127 devices. Additionally, the USB ports are hot-pluggable).

USB ports come in two varieties: Type A and Type B. Type A plugs always face upstream. Type A sockets will typically find themselves on hosts and hubs. For example, Type A sockets are common on computer main boards and hubs. Type B plugs are always connected downstream and consequently type B sockets are found on devices.

USB 2.0 is the latest development of the USB technology. It is nearly identical to its predecessor, USB 1.1, except for one significant difference: speed. USB 1.1 supports a maximum throughput of 12Mbps, whereas USB 2.0 supports throughput of 480Mbps. Additionally, USB 2.0 is fully backward-compatible with USB 1.1.

USB On-The-Go it is a new supplement to the USB 2.0 specification. It addresses the need for mobile interconnectivity since many of the new peripherals now using USB are also portable devices. As these portable devices increase in popularity, there is a growing need for them to communicate directly with each other when a PC is not available.

Wireless USB is a new wireless extension to USB intended to combine the speed and security of wired technology with the ease-of-use of wireless technology. WUSB is based on ultra wideband wireless technology defined by WiMedia, which operates in the range of 3.1–10.6 GHz. WUSB offers bandwidths of 480 Mbps at three meters and 110 Mbps at 10 meters. WUSB uses a star topology with up to 127 devices. WUSB also supports so-called dual-role devices, which in addition to being a WUSB client device, can function as a host with limited capabilities.

8.13. GPS

The Global Positioning System,[GPS, 2006] usually called GPS, is the only fully-functional satellite navigation system. A constellation of more than two dozen GPS satellites broadcasts precise timing signals by radio to GPS receivers, allowing them to accurately determine their location (longitude, latitude, and altitude) in any weather, day or night, anywhere on Earth.

United States Department of Defense developed the system, officially named NAVSTAR GPS (Navigation Signal Timing and Ranging GPS), and the satellite constellation is managed by the 50th Space Wing at Schriever Air Force Base. Although the cost of maintaining the system is approximately US$400 million per year, including the replacement of aging satellites, GPS is available for free use in civilian applications as a public good.

In late 2005, the first in a series of next-generation GPS satellites was added to the constellation, offering several new capabilities, including a second civilian GPS signal called L2C for enhanced accuracy and reliability. In the coming years, additional next-generation satellites will increase coverage of L2C and add a third and fourth civilian signal to the system, as well as advanced military capabilities.

There a number of applications where GPS system is used:

- Military Applications
- Navigation
- Automotive navigation system
- Surveying
- GPS for the visually impaired
- Geocaching
- GPS on airplanes
- Precise time reference

The GPS system uses a satellite constellation of 24 satellites in intermediate circular orbits. The orbits are designed so at least four satellites are always within line of sight from almost any place on earth. Each satellite circles the Earth twice each day at an altitude of 20,200 kilometres. There are four satellites in each of six orbital planes. The constellation also includes three spare satellites in orbit. The flight paths of the satellites are measured by five monitor stations around the world (Hawaii, Kwajalein, Ascension Island, Diego Garcia, Colorado Springs). The master control station, at Schriever AFB, processes their combined observations and sends updates to the satellites through the stations at Ascension Island, Diego Garcia, Kwajalein. The updates synchronize the atomic clocks onboard each satellite to within one microsecond, and also adjust the ephemeris of the satellites' internal orbital model to match the observations of the satellites from the ground.

GPS receivers calculate their current position (latitude, longitude, elevation), and the precise time, using the process of trilateration after measuring the distance to at least four satellites by comparing the satellites' coded time signal transmissions. The receiver calculates the orbit of each satellite based on information encoded in their radio signals, and measures the distance to each satellite, called a pseudorange, based on the time delay from when the satellite signals were sent until they were received.

Russia operates an independent system called GLONASS (global navigation system), although with only twelve active satellites as of 2004, the system is of limited usefulness. There are plans to restore GLONASS to full operation by 2008. The European Union is developing Galileo as an alternative to GPS, planned to be in operation by 2010. China and France are also developing other satellite navigation systems.

8.14. TETRA

TETRA (TErrestrial Trunked RAdio) [TETRA, 2006] has been designed to fulfil the requirements of users in Private Mobile Radio (PMR), Land Mobile Radio (LMR), Public-Access Mobile Radio (PAMR) and public safety and security applications such as police, border patrol and coast guard, fire departments and ambulances.

TETRA is a TDMA standard, similar to the GSM standard. It uses four timeslots per carrier, the carrier bandwidth is 25 kHz. Similar to GSM, the first timeslot on the first carrier transmits the BCCH, a logical channel that bears synchronisation and control data. The connection between mobile radio and base station is separated into two bands for uplink and downlink (frequency division duplex).

The TETRA services are based on three major service classes with different air interfaces, all specified by ETSI:

- Voice plus Data (V+D), circuit switched speech and data transmission, (ETS 300 392)
- Packet Data Optimized (PDO), data traffic based on packet switching, (ETS 300 393)
- Direct Mode (DMO), a simplex voice transmission between two mobiles without using a network. On a physical channel two simultaneous DMO calls can be established. (ETS 300 396)

Voice and data services within TETRA were specially standardised to meet the requirements of all security administrations. The users of former PMR and public safety and security radio systems do not need to change their communication behaviour, as nearly all features of those systems are now available in TETRA, too. Moreover, many additional services are available. TETRA services are divided in tele services, bearer services and additional services. Here is an overview of the most important TETRA features:

- Tele Services:
    - Individual Call
    - Group Call
    - Broadcast Call
    - Emergency Calls
    - Direct Mode (DMO):
    - Open Channel
- Bearer Services:
    - User Status Transmission
    - Short Data Service
    - Circuit Switched Data Services in unprotected mode (7.2 kbit/s per timeslot), standard encryption (4.8 kbit/s per timeslot) and high encryption (2.4 kbit/s per timeslot)
    - Packet Switched Data Services based on TCP/IP or X.25 protocol, depending on application, with a maximum data rate of 28.8 kbit/s
- Additional Services:
    - Priority and preemption services