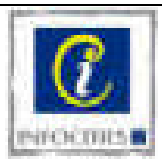


Date: 1998-june 30

Document id: MO.PROSI- 98018 V6

InfoCities project
Reference Model presented by the WP2

A contribution of the *City of Liège* with the sponsoring of the ASBL. ***TITAN***

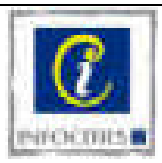


Table of contents

1. The TEAM

The Reference Model proposed for use in the *InfoCities project* has been prepared by:

Guy MARECHAL

Project manager of the part of the City of Liège (called the Win® project) in the InfoCities project, has prepared the kick-off document and its first revision after the meeting in Berlin.

It is a contribution of the **TITAN** non-profit association.

TITAN asbl
Av. Brand Whitlock, 127
B-1200 Bruxelles
Tel: +32 2 736 89 86 or +32 2 734 97 24
Fax: +32 2 732 18 43
e-mail: titan.asbl@skynet.be
URL: http://www.titan.be

PROSI (Guy Maréchal as Senior adviser)
Av. De Béco, 46
B-1050 Brussels (Belgium)
Tel/Fax +32 2 6489828
E-mail g.marechal@skynet.be

Corinne LEIBOWICZ,

Who contributed during a meeting at Paris on Nov. 7th.

Office: **Compagnie Générale de Video**

Mail address: Quai du Point du Jour, 42
F-92659 Boulogne (France)

Tel **+33 1 46 94 7900**
Fax **+33 1 46 94 7919**
E-mail corinnel@teleriviera.fr

The Work Package leader of the WP2 of the InfoCities project is:

Thomas KEMMERE,

Who is in charge of the management of the filled questionnaires and of the synthesis report.

Office: **Telematics Support Center**
Mail address: **Van Bylandtstraat 115**
NL-2562 GA Den Haag (The Netherlands)

Tel **+31 70 362 50 08** **Mobile: +31 6 5433 66 12**
Private: +31 70 362 50 08
Fax **please call first**
E-mail tkemmere@bart.nl
Site http://www.bart.nl/~tkemmere

The minimal Taxonomy for the Content of the Applications has been designed by:

Claude PIAGET

PHILIPS, Eindhoven NL
Manager Digital Cities Europe
tel: +31 40 27 87 192
fax: +31 40 27 85 382
mobile: +31.653.78.29.60
E-mail: claude.piaget@nl.cis.philips.com

Mailing address:

PHILIPS NEDERLAND
Building VB4-04
P.O.Box 90050,
NL-5600 PB EINDHOVEN
The Netherlands

****

To send a message to all the members of the WP2 team you can use the following address:

infocities-wp2@mcc.ac.uk

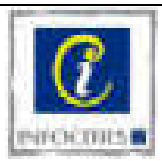
That mailing list address is managed by:

John Heaton, G1YYH <john@manchester.ac.uk>
G-MING Applications Programme, Manchester Computing,
The University, Oxford Road, Manchester, M13-9PL, UK
[+44 161 | 0161] 275 [6011 Phone | 6040 FAX]
http://www.mcc.ac.uk/John/

To unsubscribe, send a message with
unsubscribe infocities-wp2 <your email address>
as the ONLY TEXT (no signatures, please) to <majordomo@mcc.ac.uk>

On April 20, the list was:

kschofae@casema.net; tkemmere@bart.nl;
martinr@mcr1.poptel.org.uk; jsmits@prize.nl; Andreccn@euronet.nl;
m.h.blom@ptt-telecom.nl; g.marechal@skynet.be; Tauno.hovatta@hpy.fi;
Kimmo.ikonen@hpy.fi; corinnel@teleriviera.fr; cardijm@sofreavia.fr;
sigma@worldnet.fr; john@manchester.ac.uk; p.mills@mcc.ac.uk;
j.strom@doc.mmu.ac.uk; guy.bruyneel@telepolis.antwerpen.be;
ronald.calje@electrabel.be; phnet@interbusiness.it;
lovisari@comune.bologna.it; tserra@mail.bcn.es; Francesc@bcn.es;
claude.piaget@nl.cis.philips.com; Valentina.Bortolazzi@comune.bologna.it;
heikki.sundquist@hpy.fi; dave.carter@manchester.gov.uk; p.diveris@mmu.ac.uk;
Eric.mino@enter.org; sarah.green@man.ac.uk;
ludo.hoste@telepolis.antwerpen.be



2. Introduction

During the Nice meeting of the InfoCities project, it has been decided that a small team will prepare a proposal document as base for the work of the cross Work Package:

WP2 (Technical co-ordination & Standards).

That document has been presented at the WP2 meeting in Berlin on 1997 November 30 and in Amarousion on 1998 march 5.
This final version (V6) is the version as presented for release at the Manchester meeting in June 1998 after revision to cope with the last received comments and suggestions. This document is intended to be included in the deliverable of July 1998.

This document is to be found at http://www.casema.net/~tkemmere/wp2

After having presented the **team** (chapter 1) and having made an **introduction** (this chapter 2), the **reference model** (chapter 3) proposes an organisation for the analysis of the emerging Information Society.

The **coding** is then introduced (chapter 4).

The **functional profiles** (chapter 5) propose a list of typical "conduct" , "content" and "application" configurations for the services.

The **taxonomy of the compatibility** (chapter 6) proposes to organise the compatibility in 3 classes.

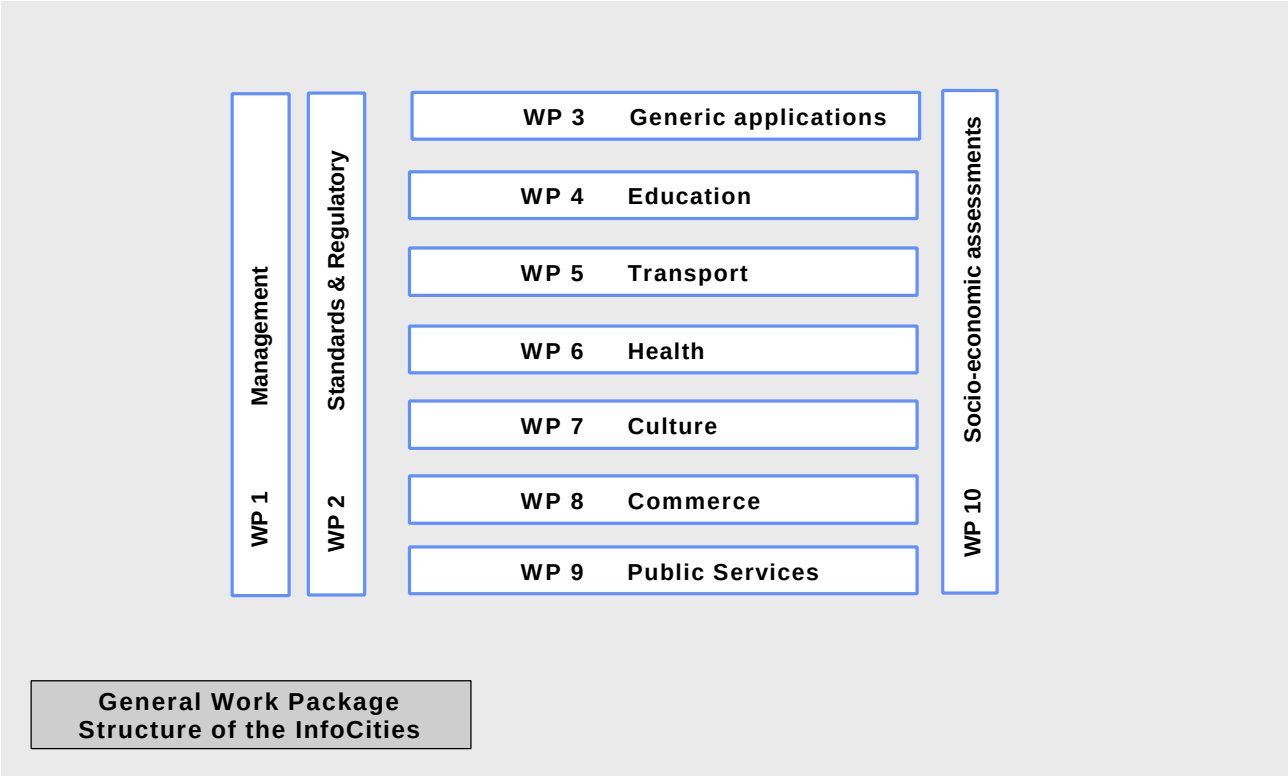
The recommendation for the **interoperability** is further handled (chapter 7).

The **explanations** for the **questionnaire** to be filled for each service is then proposed (chapter 8).

The three last chapters are appendices**:**

- Appendix A (chapter 9) gives the **illustrations** for the configurations;
- Appendix B (chapter 10) presents a **glossary**;
- Appendix C Prim (chapter 11) gives an **example** of filled questionnaire:
  - for the Enhanced Internet service mode.
- Appendix C Bis (chapter 12) gives annother **example** of filled questionnaire:
  - for the Basic Internet mode

The structure of the InfoCities project is as follows.



Note: the present document, although prepared for WP2, has direct hooks to the activities of the WP1 (management), of the WP 9 (public services) and of WP10 (Co-ordination & socio-economic assessments) and has indirect hooks to the activities of the other WP's (3-8). This is due to the "vertical" nature of WP2 !

This document covers the Regulatory & Supply plane **(TECHNICAL)** of the model described here after, while the document of WP10 covers the Operations dimension **(APPLICATION)** seen from the point of view of the

- Sociology
- Economy
- Cultural
- Political

points of view.

3. REFERENCE MODEL

3.1. The context

The **Information Society**, which is emerging, represents a major change of the context in which individual persons live, interact and organise their culture, politics, social and economic society.
The management of the society (in particular the information in the cities, **InfoCities**) implies a good understanding of the frame in which **collective & private interests** could be promoted, controlled & balanced whenever required.

3.1.1. The assets

The revolution is now fundamental.
Indeed, it is the first significant change in the nature of the human assets since the start of the human activity. From Stone Age to now, the human societies have based their organisation on material goods. With the Information Society, the human will have to organise the proper handling of a world where the main asset is **Information**. Now, even the notions of enterprise and of entrepreneur-ship are changing, as it occurred at the end of the 18th century, with the emergence of the **Industrial Society**.

The "**Content"** of information consists, on one hand, of the meaningful **data** represented according to conventions on **formats** and, on the other hand, of the **services** pertaining to the exploitation of information. In the Information Society, the "content" will represent a major part of the human activities and initiatives.
The **"Conduct"** of information consists of all means used to process, store, transmit and make accessible (vision, audio, typing and other modes of human interaction) those data, formats and services. The Content of Information is carried by the Conduct.
It is fundamental to pinpoint that, in the Information Society, the *Content* is the essence and the *Conduct* is the mean: both are required! The first emerge through its intellectual value; the second, through its industrial value.

It is well known that the *Intellectual property* is of another nature than *property of physical goods*. However, until now the associated domains and businesses were fundamentally disjoint.
In the Information Society, the actions on Information and the actions on material goods become **merged**.
Persons (physical or moral) could perform them although being not physically present and, possibly, through equipment performing on their behalf, under their supervision. Notice that, when the data represents a program and is activated on a conduct, it becomes an integral part of the reality, i.e. it gives a specific functional behaviour to the material world. That means that, in that case, the rights associated with the *Intellectual property* become tightly bind with the rights associated with the *property for physical goods.*
Sharing information is radically different than sharing material goods; in the first case all authorised users can exploit the information simultaneously without damage, while for goods only one user can be involved at a time and with a wear out.

3.1.2. From Vertical to Horizontal

The major trigger for entering a new era called "Information Society" is the emergence, at an affordable price, of the means to create and process information independently of its nature. The key being the full digitalisation of the information, be it textual, audio, speech, video, still pictures, movements, …and with its structure (expressing essential semantic, syntactical and lexical properties).
The consequence is a technology **convergence,** which leads to the **interoperability** of the means.

The technological convergence stemming from digitalisation is triggering the convergence of industries (telecommunications, broadcasting, information techniques, publishing,…) that have, until recently, been

largely separate.

Convergence and interoperability offer massive opportunities for the development of new services and the expansion of consumer choice, and is making possible changes in the way to work, play, trade, learn, and socialise. The outlook for new interactive services –such as selling via the Internet or interactive TV- is the subject of intense investments.
The many new, cross-sector alliances resulting from convergence and interoperability are leading to pressures for the adaptation of the regulatory framework. Moreover, serious concerns have been raised about how, or even whether, to govern the nature of the content disseminated, and over publishing and access rights to the new forms of media.
The old disjoint situation was **simple** to manage because it was possible to separate the domains.

The management of the new situation of convergence becomes **complex**. Any network can manage any data. Any service can be accessed through any network. Any media can be served by any service.

In consequence, the regulatory framework that is today organised in a vertical way (for instance, in many countries the regulatory frames for the TV and the cable are bind) has to progressively become organised in a horizontal way.
Examples of the horizontal approach are:

- harmonisation of the rules for the cable, the satellite, the terrestrial, the fibres, …;
- building the contractual relation between a (pay) TV program provider and the watchers;
- harmonisation of the framework for managing the media (transported by telecom or physically on CD-ROM);
- harmonisation of the intellectual property rights for the full content (service and media data);
- harmonisation of the rules for the service and program providers.

3.1.3. Information

In the Information Society not only the humans have access to the meaning of information but, to some extend, also the machines. The variety of forms in which information appears also changes the ways in which intelligence has to be understood and conducted.

Information can be considered at various levels: at the level of **intelligence**, it is a cultural and political asset or challenge; at the level of **organisation**, it has a social impact; at the level of **creation/innovation** it has entrepreneurship value; at the level of **representation** it enables semiotic.

The information can be passive, active or adaptative.

The handling of the rights (private & publics) is confronted with new challenges

- The three main intellectual property rights systems **(**the copyright © , the trade mark ™ , the wordmark **WM** and the patent **PT)** are not any longer fitting.
- The export-control rules become ineffective on the world span networks.
- The automatic fee mechanisms (like the VAT on sold goods) are loosing their grounds.

Improvements are on the way!
The European Union has adopted an innovative directive which already harmonise horizontally the protection of the intellectual rights: the media data, the service and their structure (say data base) are governed by a single framework (including the controversial *sui generis* aspects).
A very interesting and complete analysis of he problematic can be found in "*Le droit d'auteur, du logiciel au multimédia*" by A. Strowel and J.P. Traille (Ed. Bruylant).

The Information Society has a fundamental influence on human rights and democratic values. The European Union and the OECD have made significant efforts to identify and propose directives on that matter.

The "electronic democracy" is a new lifestyle with its own risks and opportunities. The protection of human image rights, the competition and pluralism of information, the protection of data, privacy and consumers, the freedom of association, the rights to access to and express information, the protection of the infants and of the human dignity are, among others, important topics for which a fundamental revision of the framework has been made or is ongoing. For more visit: http://www.oecd.org/dsti/iccp/legal

The ways of ensuring the public services and the relations between the citizen and the administration will also be significantly changed.
The expropriation rights, for superior public interest, will cover not only the grounds but will be extended to the intellectual rights. This is a not- trivial extension of Law.

3.1.4. From procedural rules to functional rules

The current society is organised around many **procedural** rules, ... and laws assuming the physical appearance of persons (physical or moral), objects and original documents.
The Information Society requires **functional** rules, ... and laws in which the *places, moments, formats and other context definition* are parameters and not any longer implicit parts of the formal context.
The essence is the set of properties required to be obtained, not the way to reach the goal, if it is a pertinent way for the specific intended context.
We are going into a world in which the **intentions** (information not yet represented) become **reality** (a compound of operations, goods and data) in many ways which should each have the same social value. All the intentions currently available in the current regulatory frame have to remain, but their formal expression should be enlarged to cover other ways of expression than the ones expressed in the current procedural frame. New associated public services and context should emerge.

Two examples:

1. **The signature:** Under the current formal law of most of the democratic countries, the movement of the body of a person setting his/her seal (usually a handwriting of his or her name) with a pen on a sheet of paper is called "signature". The three functional properties associated with that formalism are:
   - the un-forgeable binding of that person to the meaning of the content written on that sheet of paper,
   - the un-forgeable expression of the existence of a living person at the moment of signature and
   - the creation of an unforgeable unique object (each signature is a distinct act represented by a distinct support with unique instance of the written seal),

   In many cases however, only the two first of those three properties are required! Indeed in most commercial letters, the number of copies is not significant or can be solved by other means. Each banknote should have the first and the last properties: however, since long, the Governor of the National Bank is not any longer signing each of them! The integrity, the authenticity and the unique instance are now warranted by other means. Providing that context conditions are met, the electronic signature could be accepted for the cases were only the first property has to be met or when the unique instance is warranted within the content.
   Many European Government plan to recognise ***the electronic signature*** *in a useful, but limited, context: physical persons, for commercial use and providing the involvement (through* certificates *and signed* cross-interchange agreements*) of accredited Certification Authorities. The case of the persons signing on behalf (role) has also to be solved similarly (currently by use of official stamps; trade marks; word marks; estampilles; multiple signature with roles; and other ways).*
   Various levels of security are required depending of the application. In some cases, more than one signature will be required. In the context of the ***authentic bills****, such a single digital signature cannot now be accepted by law: indeed, the functional property requires the physical presence of the parties and of a certifying and authentifying party, representative of the public authorities (the notary). It is another context.*

   The cryptographic technique used for expressing the digital signature is a parameter (RSA or Zero-

Knowledge or ..) of the format definition.

2. ***The identity and existence:*** *In most of the European Countries and, under the current law, the proof of identity of a person occurs through the use of his/her Identity Card, issued by a Public Authority close to the citizen. The issue is made under the responsibility of a person representing the Public Authority (typically the Burgomaster). The intention is to register every citizen from birth to death in an unforgeable way and to bind that identity to the person through his/her photo, biometric characters and signature. The role of the public authorities is obvious in this case. In the long term, the public authorities have to organise and control the Certification Authorities! However, in the limited context of the digital signature for commercial transactions, they will have simply to accredit them! Indeed the parties mutually accept the identities, existence and integrity of contents through the "Cross-interchange agreements" and the "Certificates". Therefore, the public authorities are not involved parties in possible conflicts. However in larger contexts, the public authorities will not escape to accepting to empower the specific public empowered facilities to become "Certification Authorities".*

   Note: *The issue of an "Identity card" by a public authority is a procedural way to organise the possibility to authentify the identity and attributes of a person. The card based on a rugged carrier. It is signed on behalf of the public authority by one of its agent and an official stamp is added. On could say that the identity card plays, for the current operations, the role of the public key certificates, issued by a TTP, for the digital signature. In that sense, the two examples are here combined.*
   In the future, one could imagine *that the public authorities, jointly and in agreement with the involved person, will give a unique name to each citizen registered in their authority level: for instance:*
   My (the author of this WP2 document) unique name as citizen: guy.noel.leon.marechal@foret.be
   Unique name of the public certifying authority: bourgmestre@bruxelles.be
   *The public authorities will communicate with me through that E-mail address, while as a entrepreneur (*id est, *with the role of economic actor) I could be identified and I could sign digitally with the name and associated token guy.marechal@prosi.bruxelles.be**.***
   Similarly, as voluntary member of the Belgian French speaking Community, I could be identified and touched through guy.noel.leon.joseph.minou.marechal@communauté-francaise-de-belgique.be.

   To ensure proper functioning, cross-certificates are required between all the public authorities.

   The role is implicit in the name.

3.1.5. Remarks

- The word "**service**" covers all types of multimedia services and programmes, whatever medium they use: CD-ROM, etc. (in non-real time), Satellite, Cable, Fibre Optic, terrestrial radio, etc. (in real-time); whatever the mode: broadcast, addressed, with interaction, client-server, client-server-client, etc.
- The word "**application**" covers the service with its content of information.
- The word "**formats**" cover all ways in which "sense" can be expressed: i.e. the semiotic, syntactical and semantic elements of documents or messages, as well as the interaction types between people through such documents or messages possibly exchanged via telecommunication.

  In particular, the encoding and representation techniques used within a specific format cover the languages used and the interface protocols for the various layers of the tri-axes analysis model proposed below.
  In particular, the analysis of the content of a message and legal monitoring could be based on these formats.

3.2. The principles

- **The open human action** Society should be organised in such a way that people can carry out their actions that can be realised via information processing, storage and telecommunication networks, with the same social value as if they had directly carried out the action in the current formal material frame or with a new social value for actions that do not have equivalent in the material world.

- **The context for open human action** Society should be organised in such a way that the regulatory framework is no more restrictive than necessary for the correct operations of the society and sufficiently open to permit the values, rights and obligations of everyone to be respected and promoted.

Note: These principles imply that the equipment and infrastructures should be organised in such a way that the right information handling should be obtained "***a priori***" and "**by construction**".

3.3. The Information Society Space, the Roles & the Actors

The preceding sections have introduced the nature and principles for the Information Society.
This section intends to structure the way to progressively **organise the management and governance** of the Information Society.

The analysis of the activities and assets in the Information Society could be based on the organisation of **roles**. An **actor** can play one or several roles. The roles are interacting according to "peer-to-peer" protocols through the interfaces and functionality's of a layered framework.

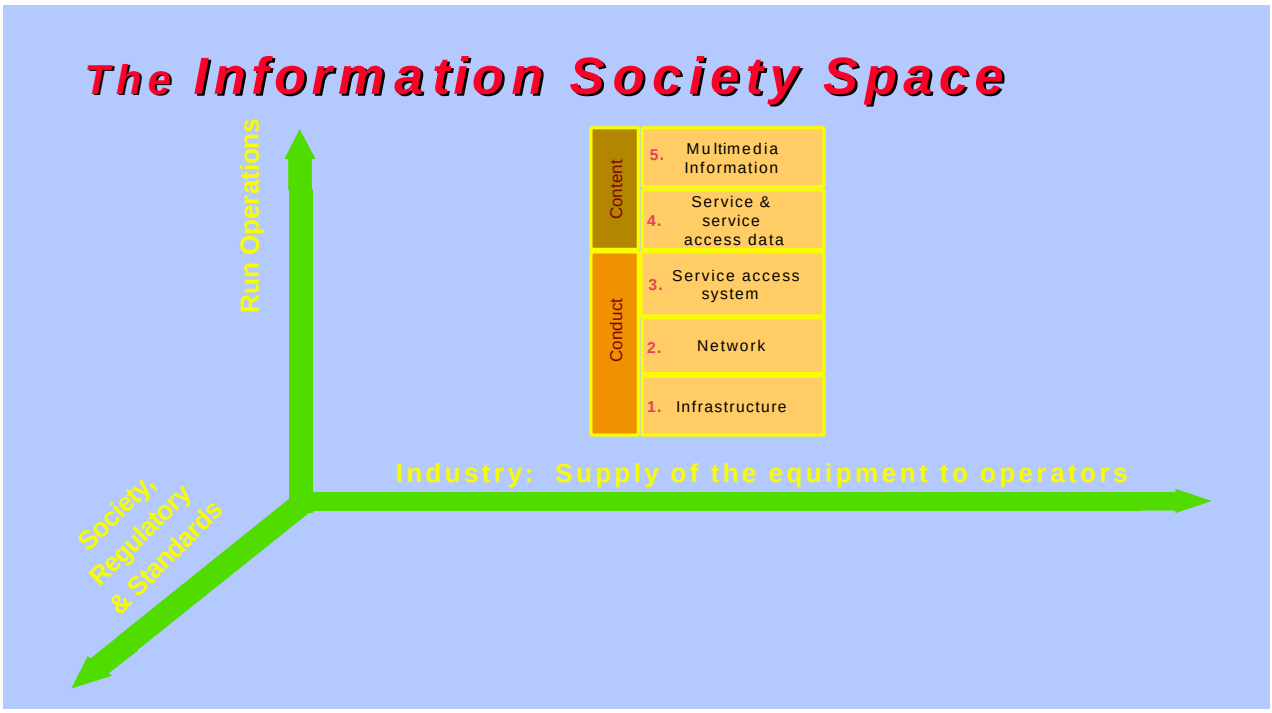
The concept of **layering** is directly answering the problems issued from the convergence and interoperability. It simplifies also the integration of the technical standards in the regulatory frame.

The concept of **Information Society Space**, with roles and actors, is directly answering the problems issued from the needs of the flexibility, responsibilities (f.i. for actors playing several roles) and independence (f.i. for open access to actors to play specific roles).

In the proposed organisation the functional laws can easily be expressed and introduced progressively. In the same way, the vertical rules can be progressively structured in layers and then assembled horizontally, which means the capability of a stepwise introduction.

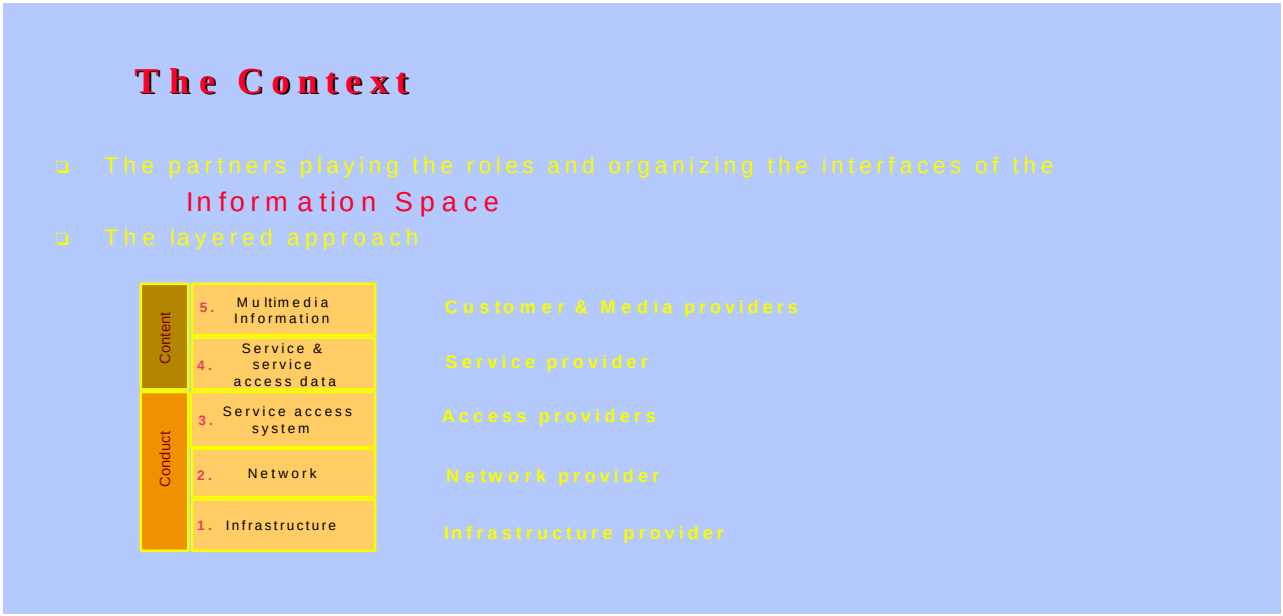
3.3.1. The Information Society Space

The roles can be structured in a three axis space: the **operations** (exploiting services and information) based on the **supply** of the equipment (with the tools and methods required to operate) and the **regulatory** frame.



3.3.2. The layered framework

The organisation of the three axes is layered as explained at the figure.



The operations can be represented according to peer-to-peer relations between parties performing roles in the layered framework. The framework has layers, based upon the roles of the players involved, where regulations are uniform for each layer. In each layer the private or public nature of the role, as well as the collective impact, should allow adaptation of the regulation. Gradual introduction of this framework is possible.

The framework has 5 layers, grouped in two blocs:

Content

5. Information
the handling, as asset, of the information represented by data

4. Service
the exploitation of the asset information and of the control of the access to the service

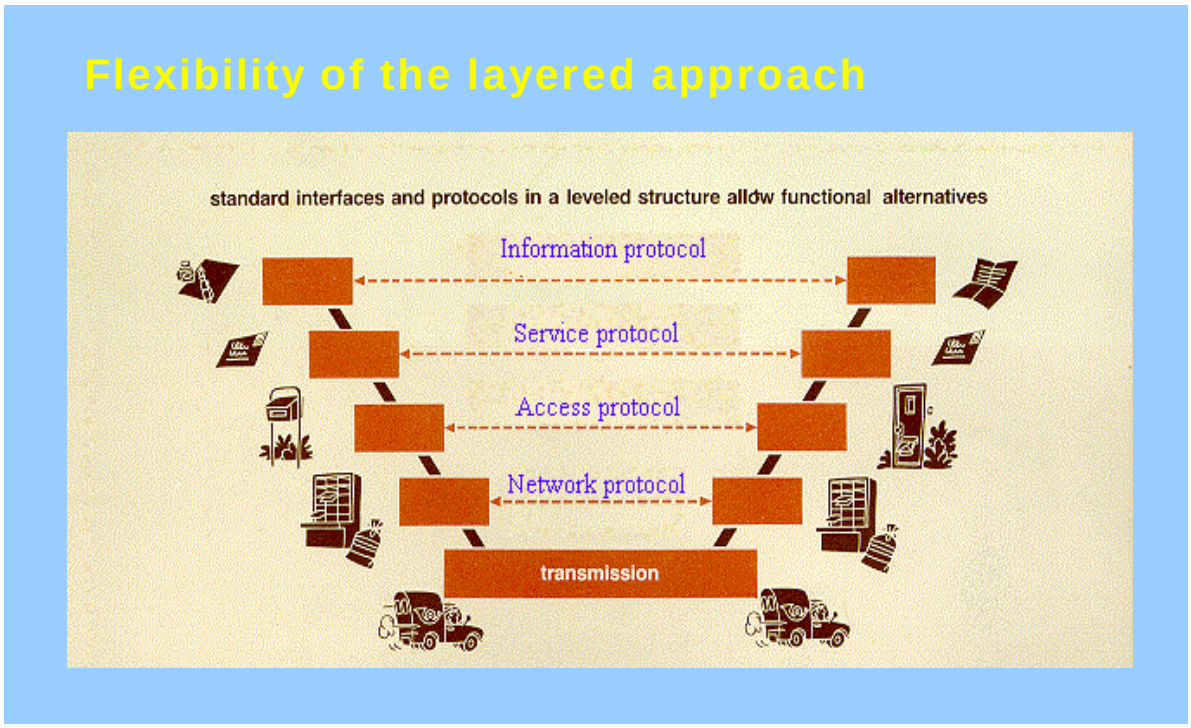
Conduct / Handling

3. Access
the service of giving to the services access to the telecommunication network

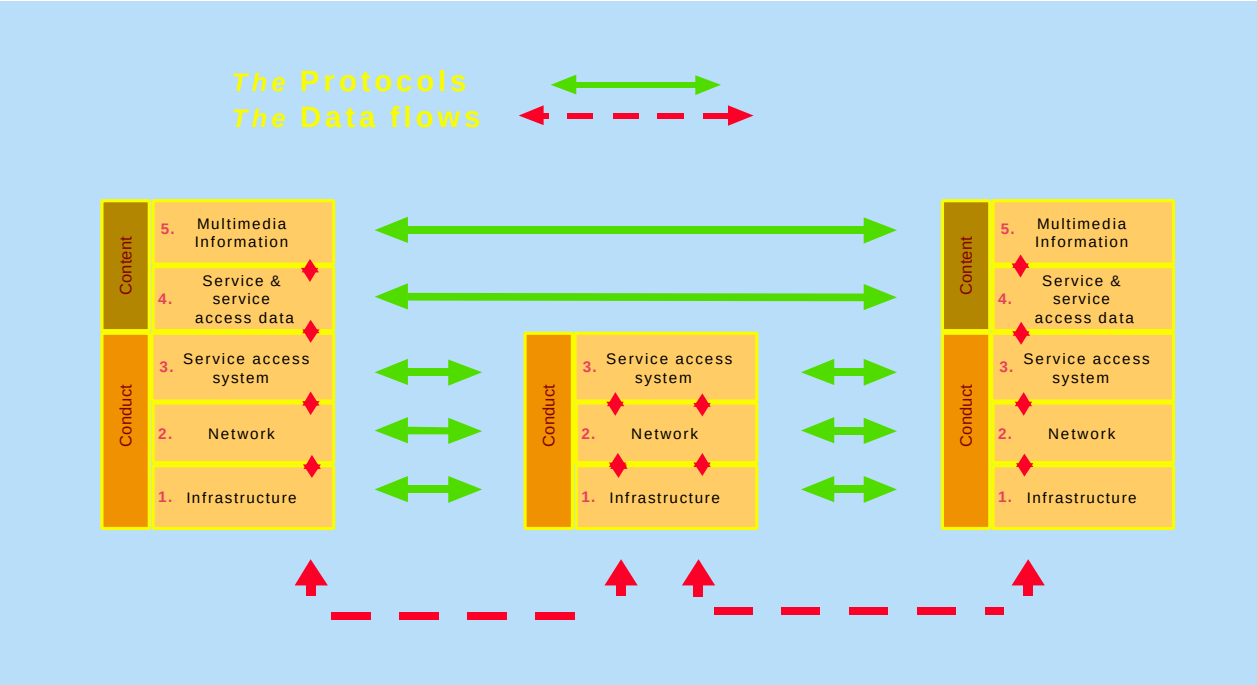
2. Network
the service of transporting the data

1. Carrier
the exploitation of the specific carrier of the data.

The layered approach can be illustrated in the case of the service offered by the Post Office.

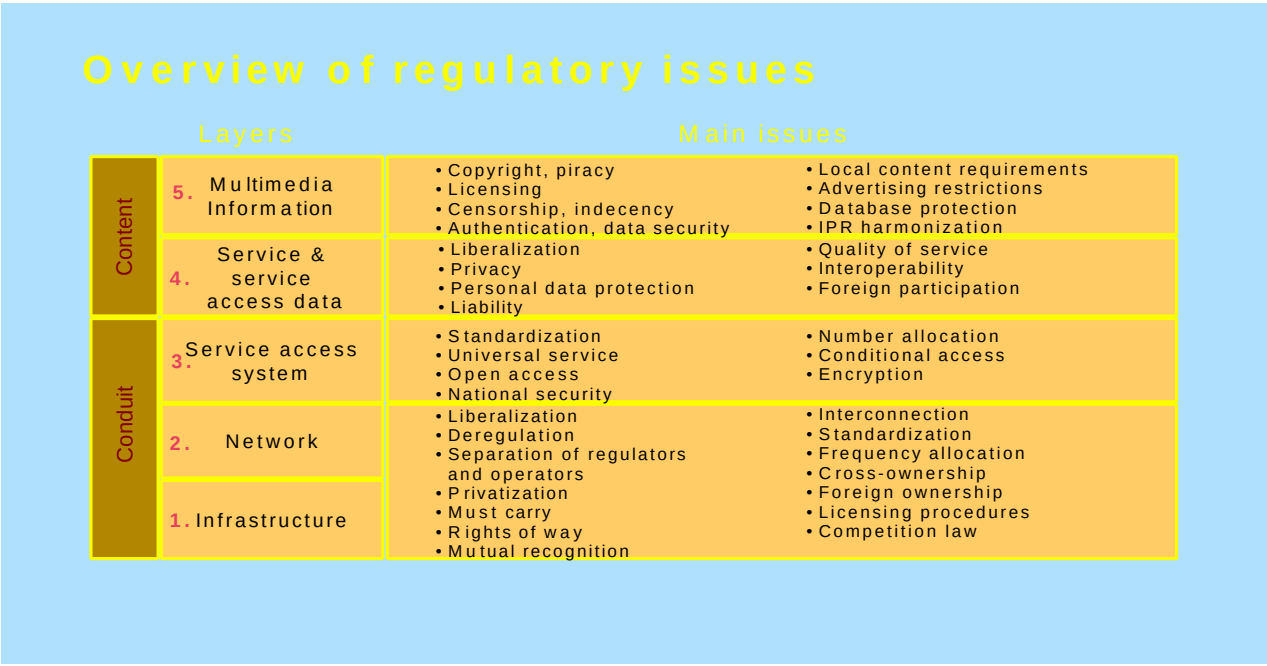


The generalisation of the layers with protocols and data flows is represented at the next figure.



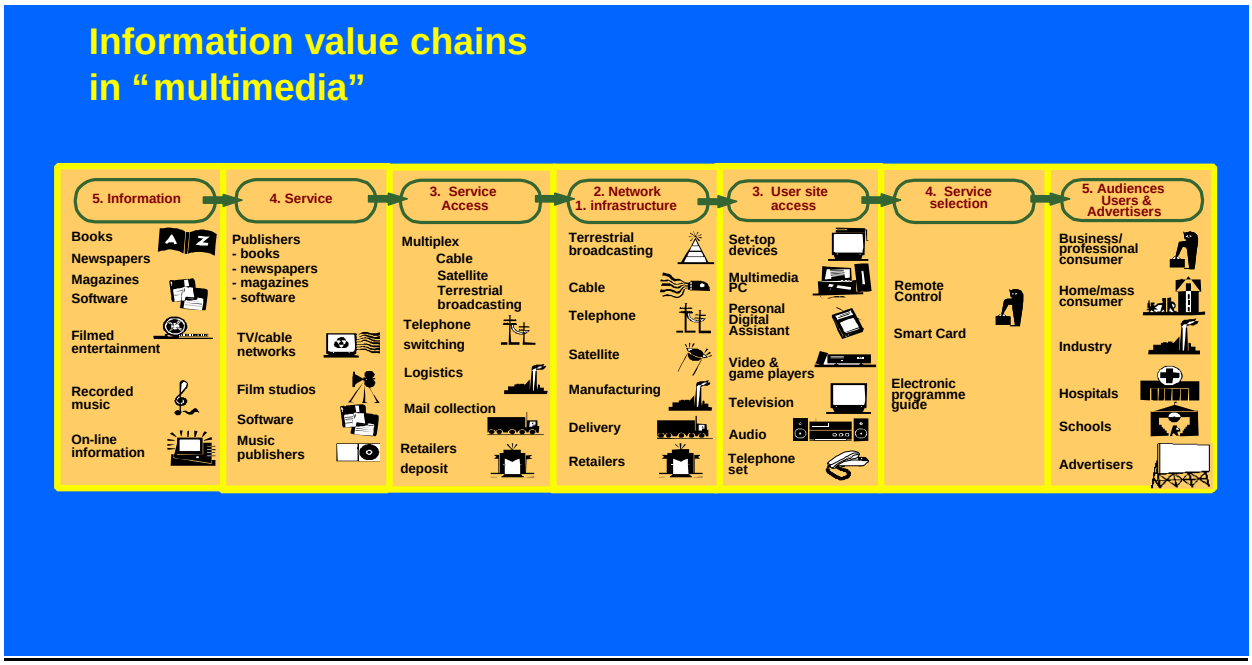
3.3.3. The regulatory axis

The frame is well suited for matching with the Information space by presenting correspondences between the operations, the supply and the regulatory axis:



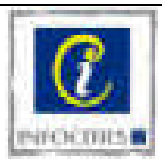
3.3.4. The Information Value chains

To that frame corresponds many **Information Value Chains** (see figure)



3.3.5. Conclusion

The organisation of the Information Society represents a significant effort. The real question is: "are the public authorities and other involved actors ready to undertake the role of organising it in a reliable and democratic way?" The technologies required are now available and at an affordable price.



3.4. The Information Security roles & services

3.4.1. Introduction

The emergence of the Information Society offers new opportunities but also new risks. The public authorities may not escape from endorsing the responsibilities attached to the new Information Society.
A new framework has to be established, in which the risks can be limited to the needs of the specific contexts.

In that framework, the functional properties are seen in a positive way: how to assure to everyone that things will be good *a priori.*

3.4.1.1. Functional properties

The main functional properties for the security goals and the security primitives are:

- Document reliability (digital signature)
  - Integrity
  - Authenticated Identity
  - Authenticated Existence
- Equipment reliability (digital signature)
  - Integrity
  - Authenticated Identity
  - Authenticated ability of valid operations
- Service availability
- Confidentiality (roles, actors, documents, equipment's, services)
  - Of existence
  - Of content
- Accountability
- Conformity
- Quality & vulnerability

3.4.1.2. The regulatory framework

General recommendations for issuing a regulatory framework have been presented in two key documents:
- *The* Green Paper *of the Commission of the European Union on the Security of Information Systems;*
- *The* OECD guidelines *for Cryptography policy.*

The major issues, which are involved, are introduced in the next sections.

3.4.1.3. Parties, roles and actors

The concept of roles and actors implies that the parties are clearly identified and typed.

The parties can be:
- Physical persons, which are individuals acting as private persons or as representatives of a moral person or acting as supervisor of an equipment;
- Moral persons, which are represented by physical persons, possibly for a specific role;
- Equipment, under the supervision of one physical person, possibly indirectly through a moral person.
  The equipment considered is any physical device having means to receive an identification and means

to interact with other parties in a sufficiently reliable way (depending upon the requirements of the current context or domain).
Typical types of equipment considered here are the smart-cards, Tamper Resistant Devices, User PCs and also servers or client equipment used in Telecommunication, Electronic Commerce, Internet and similar.

3.4.1.4. The unconditional chain of trust

The concept of chain of trust pertains to the principle that the overall trust is the same as the weakest link of the chain.

The concept of unconditional chain of trust intents to obtain the trust by disjoining the responsibilities of the roles and actors performing them; each step has its own reliability and responsibility in such a way that the identification of a breach or of the place of an attempt to breach can be done easily and that the repair can be made by restoring, improving the weak elementary link; all those links are assembled according to controlled architectural scheme. All steps of the procedures can be realised by parties acting in remote from each others, through telecommunication, except in special cases.

3.4.1.5. Level of trust

Several "quality" profiles could pertain to named parties or services.

3.4.1.6. Named or anonymous parties

The transaction flows could pertain to named parties.
The case of anonymous parties has to be seen in two parts:

- a named party that wants or has to be anonymous for certain transactions (hidden named case);
- an application in which the availability of the token (possibly with corresponding password) gives the right to perform transactions (real anonymous case).

3.4.2. Trusted third parties

Trusted **T**hird **P**arties should be organised by the public authorities (States and Federation of States). At minimum, they have to organise an accreditation of the TTP's.
Some of those TTP's should be under direct control of the public authorities: in particular the means ensuring the authentication of the existence and of the identity of persons (locally or remotely on telecommunication networks).
For other TTPs, the public authorities should organise that they exist, specify democratically their specific rules of operations and accredit actors to perform specific TTP roles: the public authorities can monitor the correctness of the execution of the operations but do not control the content of the TTP service performed.

In democratic societies, physical persons should always select themselves and independently of any authorities or Trusted Third Parties the cryptographic secret key(s) required for their identification and for the authentication of their identity, as well as their cryptographic secret key(s) required for ensuring their privacy; they should always decide themselves and independently of any authorities or Trusted Third Parties the moment of key change and of the creation of aliases, if any. Authorised physical persons should do the same for representing the actions made on behalf of an enterprise (moral persons). Authorised physical persons should do the same for enabling equipment to act on their behalf or on behalf of an enterprise (moral persons), under their control. In other words, ultimately the responsibilities always lie on physical persons (for them selves or as actors empowered to play role(s)!). Hence, the fundamental place of the authentication of the existence and identity of persons.

The fact that the Information Society operates and interacts in independence of **the places, moments and formats** implies that the interacting agents do not have means equivalent to the case when they physically meet. Tools and organisations have to be available to **create the confidence required** for these target operations and interactions.

- As known, it includes confidence on the existence, identity, unity (when required), integrity and privacy of the
  - Physical persons
  - Moral Persons
  - Equipment, documents, and messages under the control of these persons.

  The relations between those persons, equipment, document and messages have to be secured as well: the signature of a document by a physical person is one of the best examples of such relations.

These basic Trusted Third Party services imply the organisation of:

- Registration authorities for these physical & moral persons and these equipment documents and messages
- Token issue authorities
- Certification authorities for the association of "Public Keys" with these physical & moral persons and these equipment, documents and messages.

- Furthermore, extra services should be added to enhance the confidence or to assist in the operations and interactions. The most important of those services are:

  - Directory
  - Affiliation for democratic monitoring & safeguarding
  - Reliable
  - Archiving
  - Registration of formats
  - Stamping of moments, places and/or formats
  - Certification of dematerialised data
  - Certification of rematerialised data
  - Certification of content
  - Certification of non repudiation
  - Certification of the quality (availability, reliability, fitness for purpose, adherence to standards, ..) of equipment
  - Accreditation of a moral or physical person for performing a role
  - Brokerage, Arbitration, Clearing and similar.

3.4.3. The evaluation of the value of the services and of Information

This problem is very complex because the evaluation of their value cannot be restricted to the "merchant economic value". The replication of information cost only the price of the support: the copyrights reflects only one face of the "intellectual rights".
The structure and taxonomy of a data base has also to be correctly protected as intellectual rights. Cultural and educational information do not fully proceed of the economic value chains.
The global social value of Information and Services should be evaluated according to new and well established criteria.

3.4.4. The standardisation of formats

The standardisation of format is essential for resolving the problems of ambiguity of meaning (sense) in all the possible application including the monitoring (see below)

3.4.5. The qualification of contents and services

Creating contents and operating services gives rights (intellectual; copy; ...) and duties (accuracy; fitness; protection of young persons; ...).

3.4.6. The privacy protection

3.4.6.1. Guaranteed identity and privacy

The Public Authorities ensure (by implementing or ordering implementation under their control) that the various levels of authority set up a delivery system for "electronic identity cards" which respect individual privacy. The system should be non-obligatory and non-requisitionable. The necessary techniques exist. Acts carried out remotely could be attributed beyond doubt and their author would assume the obligations and benefit from the associated rights. A state that has recognised another state should set up a cross-verification system.
Without a guarantee of identity there is no way of ensuring that rights and obligations are respected. For example, it is mandatory to mention the publisher responsible for a publication and, in some countries, there is an obligation to deposit copies in order to verify the truth of the information.

3.4.6.2. Private data

The concept of private data is very general! It covers all forms of representation of information (data; data base; attached to private physical or moral persons.
The basic rule, to be guarantied by law, is that information and its representations are confidential against anyone else except when

- explicitly agreed otherwise by the person and only for the "need to know part" without authorisation of cross-exploitation of individually disclosed parts.
- in the special/limited/listed cases where law authorises (as an exception to the normal case) and with the explicit formal issue, recording and democratic monitoring of such abnormal events.

In consequence, the use of cryptography for all uses should be liberalised, except in the case of usage for confidentiality which would be guaranteed under the normal regime but lifted in cases where the law permits or requires. This means that all current usage of cryptography would be liberalised such as access control, bank transfers, digital signatures, time, place and format stamping, and other cases where cryptography protects information and authorises or refuses access to resources.

<u>The monitorability of private archives is also covered by the general case</u>

In practice the implementation of monitoring (monitorability) would take place in the "conduct". However, responsibility for monitorability is transmitted from the owner of the content (layer 5) to the service owner (layer 4) then to the owner of the service access system (layer 3), who transmits it to the network owner (layer 2) and finally to the transporter (layer 1). At each transfer point, the contract must explicitly provide (where there is no law to make it explicit) that the messages (and documents included therein) should use formats and implementation methods for these formats which can be monitored.

3.4.6.3. The legal monitoring of the existence of private relationships, identity of the parties & of the content of the relation.

Using the TTPs organisation, correct democratic approaches to the legal monitoring of the content of private relationships can be obtained. Idem for the knowledge of existence & identity of the parties. Such monitoring is one of the most sensitive problem: the privacy right is the rule in democratic societies; however, in well defined exceptional cases the public authorities have to monitor the information content of private relationships. A

democratic monitoring system should be such as, by construction, the system could not be used outside the cases where the law authorise it.
If the legal monitoring may or cannot access to the plain content, the monitored person should disclose the information (*a posteriori*). If it can be demonstrated, at charge of the public authorities, that the reason for the impossibility to monitor is due to the responsibility or lack of good will of the monitored person, he/she will become guilty of a severe fault. If the public authorities cannot demonstrate that, the monitored person will be considered as innocent.
Several good approaches exist: the *escrow or key extraction* of the keys and the *virtual addressing* are the most interesting ones.

- In the monitoring, the *escrow approach* and also the *key extraction are* always questionable. A **fair a priori scheme**, i.e. such as fulfilling the requirement of being unable, by construction, to be used outside of the allowed (by law) cases, is very difficult to remain under strict democratic control.
  However, even in that case, the identity secret key(s) should never be escrowed or extracted! Only privacy key(s) should be escrowed or extracted.

- The *virtual addressing schema* is one example of apparently good, long-term approach for solving the monitoring problem. The presentation of one good case, in a sound context could help in the identification of possible remaining problems and show paths for solving other problems.
  In the **virtual addressing schema** (see figure) none of the keys are escrowed nor extracted. It is simply to allow, *a posteriori*, that one of the addressee could recover the content of messages or document, providing that it receive, a mandate (electronically signed) to do so from persons duly empowered by law.

3.4.6.4. The defence and state protection

The public authorities are confronted with new challenges. The new Information Intelligence requires new method, tools and power.

3.4.7. The reliable de-materialisation and re-materialisation

The need and the purpose are for fulfilling the needs of justice, in particular when no cross-interchange agreement exists between the parties. The technical solution exists, but requires the presence of a TTP. In those processes, the digital signature of the TTP recognised by the Justice is mandatory.

The purpose of **re-materialisation** is to issue of a document, printed on a surface conform with the requirements of the justice (proof of evidence and autoconclusive), which is a reliable certificate of the content of a document or a reliable materialisation of the content of a dematerialised document. Reliable means for which the integrity can easily be verified and that the moment, place and format can easily be authenticated.

The purpose of **de-materialisation** is to generate an electronic document, for which it could be demonstrated that it is a reliable representation of a document fitting with the requirements of the justice. Reliable means again, for which the integrity can easily be verified and that the moment, place and format can easily be authenticated.

The figure illustrate one example of materialised document which fulfils the two basic functional requirements required for being a proof at the court:

- being **autoconclusive**: the document includes the means to control its validity
- being **proof of evidence**: the understanding of the meaning of the document can be obtained without using tools (except obviously genuine, like lenses or spectacles. In this context, the control of the document is not any longer an art but becomes a technique.

3.4.8. The public security services

The public authorities should organise the availability, at reasonable and affordable cost, to every citizen of universal security services.
Like the Post-Office service, including the “Registered Mail”, equivalent services should be made available on the Information networks. Registered and certified archiving a new possible service.

3.4.9. Rules for protection against piracy and info criminality of the infoWAR

A general framework, applicable in each country, should be installed: it is necessary that it meets correctly the principles and measures described above.
Any unauthorised try to bypass a reasonable protection (un-valid use of a password, for example) is a crime (equivalent to a housebreaking/burglary, in the example of an un-valid use of a password).

All types of attacks have to be addressed:

- attacks against the information and services (the social sense is targeted)
- attacks against the persons (the impersonnalisation of identity, ...)
- attacks against the resources (denial of service; virus; ...)
- attacks against the context of the information and services (law, standards,...)

4. CODING

4.1. The coding approaches

The **Information Society**, implies to represent the **INFORMATION** by **DATA.** Several approaches are to be used:

- Anthropic coding
- Entropic coding
  - Negentropy
  - Zero-entropy
  - Entropy
- Steganography coding

For more details, see:

URL: http://www.titan.be

4.2. The coding techniques and standards

The most important coding techniques at the various levels of the reference model are:

Layer 5:	MPEG-1	MPEG-2	MPEG-4	JPEG
Layer 4:	HTML	MHEG	MPEG-7	
Layer 3:	Internet addressing scheme		DVB-TS	
Layer 2:	TCP-IP			
Layer 1:	PSTN	ISDN	SDH	

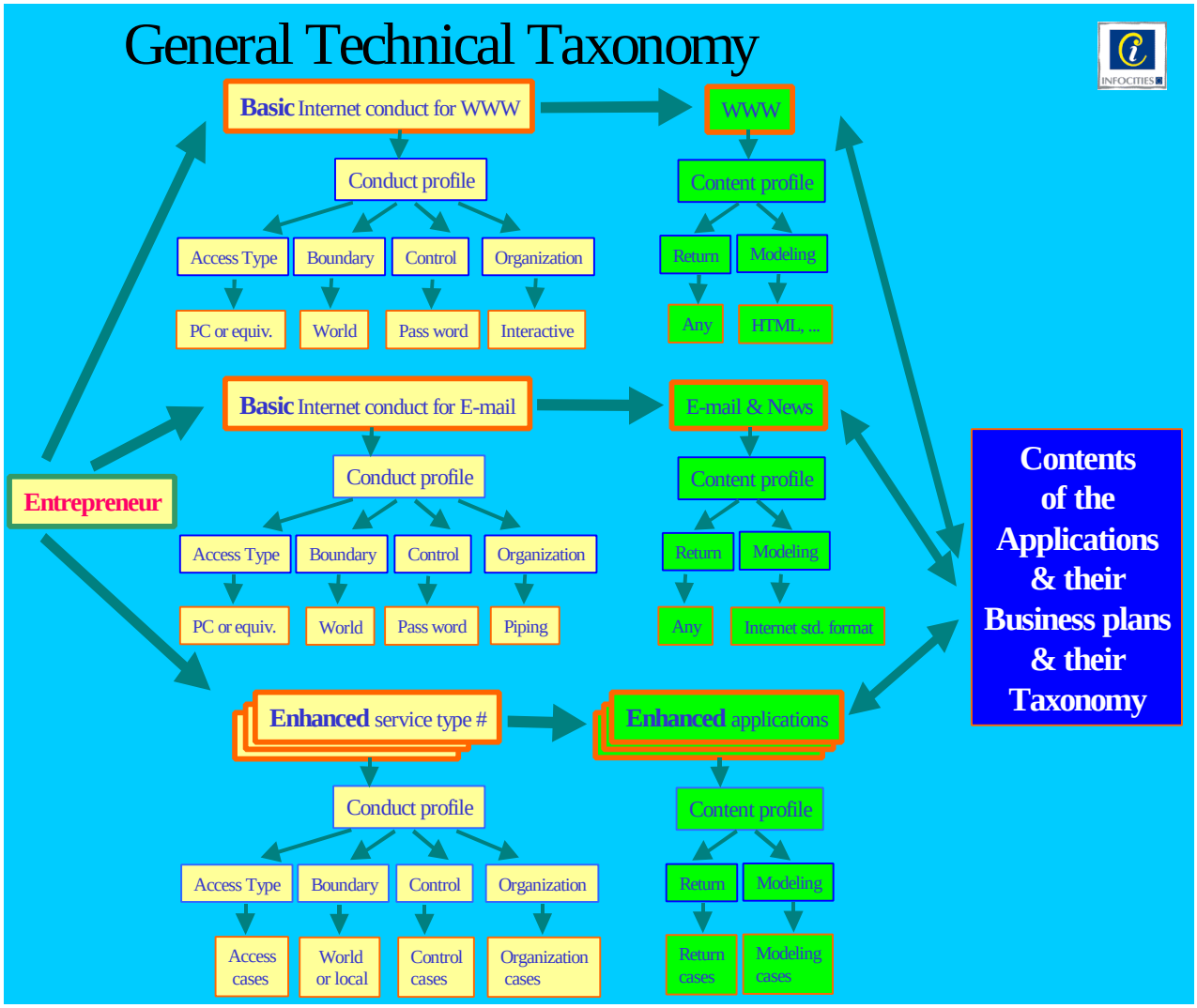
For more details, see:

URL: http://www.titan.be

5. TYPICAL PROFILES

Typical profiles can be derived from the key questions to be answered by the candidates as "Services Providers".

The general structure of the taxonomy of the technical profiles is according to the following figure, which is further detailed here after and in the two next chapters.



A. Conduct part

1. How will my customer access to my service?

Several cases could be identified: the word "mixed" is used to characterise the situation where two access systems are used; while the word "hybrid" is used when several networks have to be used to have the full service (PSTN, ISDN, Cable, Satellite, CD-ROM, …).

- **Case 1 Dedicated equipment**
  When the intention is to reach customers in a **niche**, **dedicated access equipment and networks/carriers** could be bundled with the installation, use and maintenance of the service.

- **Case 2 Personal Computer**
  When the intention is to reach customers of **Internet**, it could be assumed that they own a **Personal Computer** equipped with a Web Browser. The variant in which the PC is in reality spread on the Internet (usually called "Network-PC") can be considered as equivalent for the compatibility & interoperability.

  - **Case 2.1**
    The customer is equipped with a PC connected to the Telephone Network (PSTN) through a low speed modem.
  - **Case 2.2**
    The customer is equipped with a PC connected to the Integrated Switched Data Network (ISDN) through a medium speed modem.
  - **Case 2.3**
    The customer is equipped with a PC connected to the Cable Network through an adaptive high-speed bi-directional modem.
  - **Case 2.4 Hybrid**
    The customer is equipped with a PC connected to the Broadcast Network through a Set-Top-Box for digital TV working in (high speed) feed-through; the interaction occurs through the Case 2.1 or Case 2.2.
  - **Case 2.5 Hybrid**
    The customer is equipped with a PC connected to the Telephone Network (PSTN) and to a broadcast network through a high speed modem.

- **Case 3 Television**
  When the intention is to reach **mass customers**, **no stabilised solution** could be assumed available now.
  In all cases when interaction is required, it occurs through the Case 2.1 or the Case 2.2.
  - **Case 3.1 Hybrid**
    The customer is equipped with a "Set-Top-Box" **[STB]** (also called "Integrated Receiver Decoder" **[IRD]** for digital TV; the service is given through the dedicated Operating System and Conditional Access System
    - Case 3.1.1: OpenTV and Viaccess
    - Case 3.1.2: Mediahighway and MediaGuard
    - Case 3.1.3: XXXX and YYYY
  - **Case 3.2 Hybrid**
    The customer is equipped with a Web-Browser-TV terminal; the service is given through the dedicated Operating System and Conditional Access System
    - Case 3.2.1 WWWW and ZZZZ
  - **Case 3.3 Hybrid**
    The customer is equipped with a terminal combining the functionality's of a Set-Top-Box for digital TV and of the Web-Browser-TV; the service is given through the dedicated Operating System and Conditional Access System
    Case 3.3.1 QQQQ and RRRR

- **Case 4 Mixed**

  The customer is equipped with an Advanced-STB/IRD, which combines the functionality's of the STB/IRD for digital TV & Radio and the functionality's of a Network-PC or Web-Browser-TV.
  In February 1998, the DVB-ETSI has standardised the protocols & format to allow such a combination.
  The Hardware platform would so become Operating system independent, as the application could be written in a portable language (such as JAVA). Many European Majors has already expressed their intention to adopt that approach end 1998.
  Such a solution is ideal for reaching **mass customers! A stabilised solution** could be assumed available now, if the Smart-Card (or equivalent) interface is also implemented in the device according to an "Open" Standard (DVB-Common Interface or, better, the OSCI of DAVIC).
  In all cases when interaction is required, it occurs through the Case 2.1 or the Case 2.2.

  - **Case4.1 Full TV, Radio & Web**
  - **Case 4.2 Full TV, Radio & PC (including Web)**

    Same as previous 4.1 but the terminal has all the functions of a PC.

- **Case 5 Public**

  When the intention is to reach a priori all citizens, for a **universal service** for instance, the public or private actors could provide E-mail boxes and public access points in kiosks or similar (banks, tourism information centre, town-halls,..). In that case, all the previous modes could be selected by the actor.

The second key question to be answered by the candidates as "Services Providers" is:

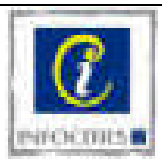
2. What are the boundaries of the access space?

- **Case §:** The whole world (Internet, X400, for example)
- **Case §§:** The limited domain (a Private Intranet, a Private Intranet for a City, a Community, a Country, for example)

The third key question to be answered by the candidates as "Services Providers" is:

3. What are the control techniques used?

- **Case A:** None
- **Case B:** Pass word
- **Case C:** Pairs of secrets
- **Case D:** Floppy disk with build-in pass word
- **Case E:** Hidden secret (SET, Swift, …)
- **Case F:** Smart Card (C-SET, Mediaguard, Viaccess, CryptoWorks, Isabel,…)
- **Case G:** Tamper resistant device (specify,…)



The fourth key question to be answered by the candidates as "Services Providers" is:

4. How shall I organise service?

The service can be organised fully in real time.
It could also be partly in real time (selection on-line and delivery off-line).
It could also be organised fully off-line.

Several typical cases could be identified:

- **Case V: Full interaction**
  For example Internet browsing on the telephone network)
- **Case W: Piping**
  For example, sending a file as a Store & forward service (E-Mail)
- **Case X: Streaming**
  For example, transmitting a program stream of an event in real time
- **Case Y: Multi-protocol encapsulation**
  For example, encapsulating TCP-IP within the private data stream of a DVB compliant Transport Stream
- **Case Z: Carousel or Carousel object**
  For example, transmitting in broadcast several times the NEWS
- **Case U: Mixed mode (a mixture of the previous cases)**

In each of the cases, the standard formats, interfaces and protocols should be defined at each level of the reference model. In most cases, it will suffice to refer to the recommended mode (see 7.2.1).
Note: The ETSI has recently standardised the cases W, X, Y and Z on broadcast networks.

B. CONTENT(technical)

The first key question, for the Content, to be answered by the candidates as "Services Providers" is:

5. How shall I have my return for the given service?

Several typical cases could be identified:

- **Case A No charge**
  For example, Universal Services or Social / Cultural / … Services are given by the Public Authorities or their mandated organisations. In reality, the return comes from our taxes.

- **Case B Subscription by period**
  The subscription could be by period (day, week, month, year)

- **Case C Subscription by events**
  The subscription could be by event (football match, opera, .)

- **Case D Prepaid**
  The use of the services is automatically debited from a reserve.

- **Case E Warranty through deposit**
  The use of the services is measured periodically

- **Case F Bonus**
  The use of the services is given as a bonus (You buy a TV and you receive one year of subscription)

- **Case G Bundling**
  The rights are included in another contract (the subscription to the cable TV includes the rights to the services).

- **Case H Cash**
  This case is typical for public kiosks of the case 5 of the first question.

For each of the case in which it applies, the modes of payment can be based on:

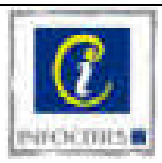
- **Option P**
  A direct link to the banking tokens and procedures (for instance, electronic purse or credit/debit card, possibly with password or other access control system) and a direct link to the service can be organised.

- **Option Q**
  An indirect link to the banking (for instance by domicialisation or drawing rights) & a direct link to the service can be organised.

- **Option R**
  An indirect link to the banking (see above) & to a service (through a broker service, a proxy server, or other) can be organised by issuing a services-related smart card, passwords or equivalent.

- **Option S**
  A direct link to the banking & an indirect link to the service (see above) can be organised.

- **Option T**
  The return is not "merchant" but the service provider has to or wants to have statistics on the use of the service. That is a typical situation for public or universal services.



6. How shall I represent the content for the given service?

6.a

Several typical cases could be identified:

- **Case A HTML**
  It is the most common and recommended representation mode. Standard for WWW sites.

  This format can be used for both online and offline viewing

- **Case B PDF**
  It is the most common way of representing documents with portability and flexibility in the physical appearance.
  Portable Document Formats make sure that documents published in this format will always look the same, independent from whatever combination of browser and PC is used. Another major benefit is that these documents cannot be changed anymore. Copyrights etc… are therefore protected.

  This format can be used for both online and offline viewing.

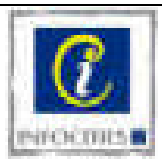
- **Case C Rich Text Format**
  It is the most useful for revisable documents.
  This format which consists of ASCII text enhanced with format codes makes it possible to port and thus view and edit documents between text editors of different origin.
  To view documents in rtf in an Internet browser, it should be converted to html. Several converters exist. However, some of the formatting will be lost when a document is converted from a specific editor to rtf.

  This format is used for offline viewing.

- **Case D Audio**
  - **D1 None-streaming audio**
    Audio in this format cannot be listened to in real-time. The audio document must be completely downloaded first and listened to afterwards. This can be done either offline with a separate application or online with a compatible plug in for the used Internet browser. Downloading and listening to it cannot happen simultaneously. This way documents often appear to be rather dull because you need a lot of time. Therefore this format is used for realising either very small sound-effects to enhance documents, or to ship larger audio-documents which do not need to be viewed immediately.

    Wav & midi formats are typical, the latter one being much more compact.

    This format can be used for online or offline viewing, but with the above mentioned restrictions.



- **D2 streaming audio**
  It is the most usual for verbal compact coding and acceptable audio.

  Downloading and listening to the audio can be done simultaneously. You therefore do not have to wait for the last sound to be captured before listening. The sound comes in as a 'stream', not as a lump.

  This format typically is 'ra' for Real Audio.

  This format can be used for both online and offline viewing, but is optimised for online viewing

- **Case E Static Pictures**
  Static Images can be included in WebPages in several formats.

  These images can be 'Interlaced'. This gives an impression of a stream of several layers gradually being uploaded. While the picture gradually becomes clear and sharps you read on and view other parts of the document.
  Also, transparent backgrounds are possible which gives enough opportunity for some special effects.

  The most traditional formats are gif and jpg or jpeg (Pictures Expert Group).

  The 'animated gifs' format makes it possible to append several images in one. These individualimages are shown one after the other in a circular repetitive mode. This is used with rather small images, such that it does not take long to download. These are often used for graphic enhancement, typically as eye-catcher.

  This format can be used for both online and offline viewing

- **Case F Motion Pictures : Video**
  - **F1 None-streaming Video**

    Video in this format cannot be viewed in real-time. The video document must be completely downloaded first and viewed at afterwards. This can be done either offline with a separate application or online with a compatible plug in for the used Internet browser. Downloading and viewing it cannot happen simultaneously. This format is used posting larger video-documents that do not need to be viewed immediately.

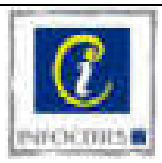
    Typical formats are 'mov' and 'avi'. This format does not give full screen

    This format can be used for both online and offline viewing but take note of the above mentioned restrictions.

  - **F2 Streaming Video**
    It is the most common for low-resolution audio-video (500 kbits/sec to 2000 kbits/sec).

    Downloading and viewing the video can be done simultaneously. You therefore do not have to wait for the last sequence to be captured before viewing. The images come in as a 'stream', not as a lump.

    Typically MPEG-1 (Moving pictures Experts Group)



This format can be used for both online and offline viewing, but is optimised for online viewing

- **CASE G HTML Embedded Scripts, objects, components.**

  HTML Embedded just means that the HTML source code is enriched with objects like scripts and components. These objects do not interfere with the code, they are just included or embedded and executed from within the HTML source code.

  These scripts control in which way the rest of the data presented in the HTML pages are retreived from databases, filtered, validated and formatted to be presented in a specific way. These objects may be visible and humanly readable within the HTML source code, but they can also be completely hidden to only be executed from the server side. Others are objects are typical 'black boxes'. Thee are visible within the HTML source code, but are not humanly readable. The results however are clearly evident at the client side. But you have no clue whatsoever is really happening internally.

  Typical examples of scripting languages are VB-script and java-scripts.
  Typical examples of component are java applets, microsoft active server pages (asp)

  These format can be used for both online and offline viewing, but is optimised for online viewing

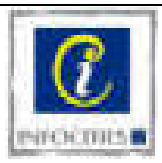
- **Case H Others**
  To be specified in the context.

6b Agents

- **What are agents**

Every day, in every job, there are recurring jobs to be done. E.g. the VCR needs to be programmed, We need to drive to work, We need to fill in our time sheets, etc. All these things are necessary, but usually tedious tasks. It would be handy if we could delegate these tasks to someone or something else.

This is where Software agents appear. One of their tasks is to automate the recurring and not so interesting things we have to do. An agent could, for example, take note of the things you do all week, and fill in your time sheet.
A Software agent does not need to wait for a message or a command from the user to start doing a task. He should be intelligent enough to make this decision autonomously. In this way, agents differ a lot from traditional software, because they are active all the time on the background, minding their own business, looking at what the user is doing, and appearing only when they decide they can help the user. Because the agent is always there, he can do much more than just sit there and wait to help us. By observing user behaviour, the agent can find out what the repetitive tasks are, which pages you browse to, etc. By using this information in an intelligent way, he can try to predict the goal of a current task and eventually help the user get to that goal faster, or more efficient.
Another way Agents can be used is to filter the information we get. This way we don't need to waist time scrolling through Junk mails and Advertisements or browse to sites that don't have the information we ask for. As this may be a very helpful application of Agent technology, it is also one of the most difficult to program. To accomplish a good information filter, the agent needs to know what the user sees as relevant documents. This can be done by simply giving a number of keywords, or can be gathered by observing which documents are read.



In a Web environment, the concept of software agents has to be rethought a little bit. Previous examples both got their information by doing some kind of user profiling. So the agent has to know who the user is in order to help him/ her in a personalised way. One of the main characteristics of the web is the anonymity of the users. A lot of people only visit a site once, in search of information concerning a specific topic, or they stumble on the site by accident. So there can be no (or at most a very limited) user-profile, or user behaviour analysis. The intelligence of the agent should therefore all be programmed, and not dependent of what the user does. This way, an agent could e.g. provide help to guide the user through a site.

There are numerous other possible applications in which Software agents can be useful. There can be reminder agents, telling you to go to a meeting, or to go to a garage on time. Agents could observe whom you usually send mail to and compose mailing lists, etc, etc.

In the end, everyone could have his own virtual self represented by a personal agent which knows everything you like or do, and interaction with the computer wouldn't go via the keyboard, but by talking to ones virtual representation.

- **Agents and Infocities**

Can Infocities applications be enhanced with Agents?
In order to know this a small questionnaire was designed to extract information about the actual application, and the nature of every organisation.

Part I determines whether the application and its user are suitable for being enhanced with Intelligent software Agents.
Part II on one hand determines whether an organisation not only has interest in being pioneer with regard to Agents and iswilling to invest in Agent resources. On the other hand it is checked if personnel with the right skills and knowledge is available or not.

Part I **Application information**

1. Do you have reoccurring tasks within the program? yes/may be/undecided/no
2. Is it possible to automate these tasks? yes/may be/undecided/no
3. Do you have mostly novice or one-time users? yes/may be/undecided/no
4. Is there a possibility to have user-feedback? yes/may be/undecided/no
5. Is there a possibility to have user-profiling? yes/may be/undecided/no

Part II **Strategic, Organisational information**

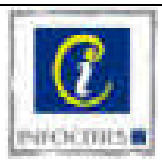
Are you willing to invest in :

6. new and unproven technology? yes/may be/undecided/no
7. extra hardware to run the agent infrastructure yes/may be/undecided/no

Do you have a programmer available with knowledge of :

8. Distributed programming? yes/no
9. Multi-threading? yes/no
10. Machine-learning techniques or user profiling techniques? yes/no
11. Component technology? yes/no

When most of the answers to the questionnaire are 'Yes' a site could probably not only start developing an agent site, but also operate one.



The questionnaire can be found in electronic form format at http://magica.dma.be/infocities/index.htm

- **Results and analysis of the collected data :**

Reactions from a few cities only have been submitted.
Barcelona, Wien, Bologna, Den Haag, and Antwerpen.
Although an entry for every work package for every city
was expected, only 11 data-records were received.

The fact that only such a small number of questionnairres were sent in also is an indication for the disintrest for Intelligent Software Agents.

The disintrest may have several reasons.

- Lack of knowledge about agents.
- Too high a work volume such that even this small form can't be sent in.
- It is too early to invest in Agents
- They never got the questionnaire or overlooked it in their mail.
- …

The listed reactions from PART I show the following trends :

1. mostly user feedback is really possible
2. but user profiling is either certainly possible while the other half of the population is doubt.

Combine this with the fact that

3. if known mostly users are either novice or first time users
4. while half the population demand tasks that are recurring tasks from the server point of view.

The listed reactions from PART II show the following trends :

5. most applications/servers show great undecidedness when considering investments in unproven technology.
6. also, investments in extra hardware to run these new services is certainly not taken for granted

When talking about the cocktail of skills needed to undertake actions in the field of agents

7. most skills are not in house, and certainly not all of them in combination in one person or organisation.

Conclusion PART I

The statements ranking from 1-4 may make us conclude that from the application/server point of view Intelligent Agents do have some potentiality, they most likely they can give added value. For a lager subset of applications this is even a fact.

Conclusion PART II

The statements ranking from 5-7 may make us conclude that most organisations are unsure to invest in Intelligent agents. The fact that the necessary skills (except one, components technology) are lacking is an extra drawback for uncertain organisations

General Conclusion

Although the applications on most servers are promising with regard to the potentiality of Intelligent Software Agents the majority of the correspondents tend to either hold back or show great uncertainty towards Agents.
The low response to the questionnaire probably is as well as the mentioned uncertainty a clear sign that most organisations are not ready yet.

The trends in the the virtual world show however that the future will undoubtedly show a lot of agents willing to proove their right to exist, to live. Huge acquisitions and investments are made by the larger companies (e.g. Microcsoft which recently bought firefly).
These companies do not want to miss out on this, they want to be sure to be active agents in the field when the rest of the world is getting ready for it.

****

The sections A. and B. covers the reference model for the Technical:

The cases could be illustrated by the figures appending (appendix A).

****

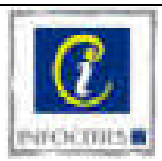
C. APPLICATION (content data)

It isn't the purpose of this *technical reference model* to organise the taxonomy of the Applications.

Such a taxonomy (planned to be covered by the WP10) will have to cover the organisations of the Web sites, Access Providers, Brokers, Proxy, Clearance, Search, Certification, Identification, Notary, Personalisation, Accreditation and other similar services.

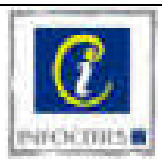
Waiting the availability of such taxonomy, the applications will be simply described according to the elementary taxonomy adopted by WP10, under a suggestion of Mr. Claude Piaget :

A few technical elements are presented to simplify the links and quick look reading.



Proposal for a Methodology to define Common Interest Applications

1. List all service descriptions.
   Descriptions should be according to a given template (see proposed template)
2. Sort and regroup services with similar functionalities.
3. In each group, find common service and technical elements.
4. Write these common elements as a “Kernel Functionality” description.
5. Check for the coherence of the content elements as an application description.
6. If needed, complete with the most common elements corresponding to the missing issue.
7. Define the differences as “options” to the “kernel functionality”.



Application description template

1. Goal of the application:

2. Generic functionality's:
   Information ☐ Communication ☐ Transaction ☐ Entertainment ☐

3. Functionality's offered to the user:
   a.
   b.
   c.

4. Users targeted *(citizens, SME's, ...)* :

5. Content providers targeted *(local administrations, commercial entities...)*:

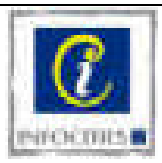
6. System(s) used to offer the service:
   a. Terminals:) *public access: kiosks,..; private (PC, Internet TV terminal,..); business (PC,...);....)* :

   b. Infrastructure *(network(s))* :

   c. Central system *(server(s), data bases, management facilities,...)* :

   d. Content providers system *(content edition, data transmission to, and communication with the central system,..)* :

   e. Nature of data *(HTML text, forms, images, audio, video)* :



6. COMPATIBILITIES

The compatibility of use between all those cases has to be analysed in three modes:

1. Could the service in one City be accessed from another City?

2. Could the service in one City be migrated and instanced in another City?

3. Could the service in one City be used in the same City through several access cases?

To answer those questions (with the forms of the chapter 8), the cases identified at the chapter 4 have to be detailed within the reference model of the chapter 3 (in reference to the applicable standards, proprietary compatible or equivalent).

7. INTEROPERABILITIES

7.1. Introduction

The first aspect of "interoperability is the release stage of the project intending to give a specific service or application. The interoperability and the compatibility will be quite different at each phase:

- if the service is only **decided** (only the intention and planning are known);
- if the service is only **specified** (the remote service provider has then limited possibilities, like informing his customers that the service is planed to be available within, say, six months);
- if the service is at **trial** (the quality of service could be limited and the problem solving is routine);
- if the service is **operational** (the quality could be better warranted and the problem solving organised in a "exception mode");
- if the service is "**end of life**" (it could be save in a museum, …).

The coding of stages could be according to:

- **M stage:** Management "go" given on the bases of a "strategy" document;
- **F stage:** Functional definition ready;
- **P stage:** Product ready and validated;
- **T stage:** Trial for evaluation before launch at large scale;
- **O stage:** Running operations and maintenance;
- **E stage:** End of life; date for end of service decided

The interoperability is the ways to obtain the compatibility's when differences exist between the equipment and protocols for the various users.
For simplicity and realism, one could say that the cases 2.1 and 2.2 of the chapter 4 are interoperable.
The InfoCities project has decided to organise the INTEROPERABILITY according to the following approach.

7.2. BASIC SERVICE mode

By default, all the services are assumed given in **BASIC SERVICE mode** corresponding to **INTERNET** at reasonable speed (on PSTN [case 2.1] or ISDN [case 2.2]). In the InfoCities, for each service, a mode of the service is always given according to Internet. It should follow a subset of the whole possibilities of Internet: only WWW, News, Chat and E-mail services are assumed always available.

The **basic service** is defined by:

Layer 5: Representation structured as HTML pages
Texts in RTF; Audio in one of the modelling mode of 5.6 (RealAudio…); Video in one of the modelling mode of 5.6 (MPEG-1…); Images in one of the modelling mode of 5.6 (JPEG…).

Layer 4: Three basic services only using the Internet.

INTERNET E-mail	INTERNET CHAT
INTERNET WWW	INTERNET NEWS

Layer 3: Access through PC equipped with Netscape 3 or MS-Explorer 3 as browsers.
If the service is not given in full warranted compatibility, without any other additions, the service will not be considered as basic but treated as "enhanced" although being in reality degraded from the basic.
Passwords (when required) can be used for access control
Based on the TCP-IP protocol and the Internet scheme for address and domains

Layer 2: Two types of networks
PSTN at 28 800 baud's max
ISDN at 64 000 baud's

Layer 1: Implicit from layer 2

Important note: the use of ancillary facilitators (see) below in a pure transparent mode do not modify the fact that the service is given in "basic mode" although the performance is higher without nevertheless changing the client maximum throughput (layer 2 of the previous paragraph.

7.3. ENHANCED SERVICE mode

When the Basic Service is considered as not powerful enough for the intended applications, in particular when the client maximum throughput of the basic mode is unable to give a realist service, when the services, although being given according to Internet, are not fully compatible, when the services remain intended to be given according to **INTERNET or NOT**, or in other situations where the basic mode is not met, the services are called given in **ENHANCED SERVICE mode. The most important intention corresponds to INTERNET at high speed** (in all other Internet cases except [case 2.1] or [case 2.2]; typically, in Intranet) or corresponding to all the remaining cases. That high speed implies, for example, the real-time video according to MPEG-2.

In that case, the InfoCities intend to facilitate **a certain level of interoperability** by installing ancillary services:

1. **Ancillary Basic Service:** As a matter of minimum, to organise the service not only in Enhanced Service mode but also in Basic Service mode (obviously with limited capabilities). That Ancillary Basic Service should describe the functionality's of the Enhanced Service and the presence or not of Ancillary Facilitators. The limited subset of functionality's of the Ancillary Basic Service could simply be one HTML page describing the service in a few sentences: "that" the service is available and requires "that" specific environment; for more details, please contact the "web master" at <name>@<domain>.
   The InfoCities consortium has noticed, at the Manchester Meeting, that all members intend to provide an ancillary basic service at deployment stage for each services they provide or will provide in enhanced mode.

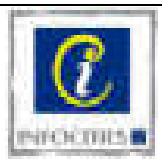
2. **Ancillary Facilitators:** Organise the diffusion of the service by ancillary facilitators, which are servers used for the adaptation to the "local" equipment and protocols to the "remote" ones. In the Enhanced Mode, it is in fact the clever ways to allow distant high speed services between two closed high speed domains, although the data-communication paths between the two domains are at low speed.

- At the layer 5: The use of "Duplicated Data" servers
- At the layer 4: The use of "Mirror" servers; of "Dynamic Cache" servers; of "off-line"
- At the layer 3: The use of "Rooming Proxy " servers
- At the layer 2: The use of "Routing Proxy" servers
- At the layer 1: The use of "Bridge" servers

For the implementation, it is advised to construct the service in such a way that the updates will have their effects in an automatic way on all the ways in which the service is given.

7.3.1. Remarks

The definition of that minimum do not preclude that the services would have prepared provisions and hooks for items that will have to be addressed later.
Typical are: Hooks for the multi-language services, export control info, qualification for filtering, intellectual rights and protection. Ready for technology transfer. Ready for MHEG. Capable of Universal Service (when apply). Ready for encapsulation to allow the proxies and similar. Ready for powerful Conditional Access systems based on one or two smart cards. See also all the roles in the reference mode at the Chapter 3.



8. QUESTIONNAIRE Explanation

In order to know the current level of Compatibility and Interoperability of all the **APPLICATIONS** intended or already in use in the InfoCities project, the WP2 recommend that the InfoCities project management WP1 and the Advisory board WP10 would ask to all contractors to fill-in the questionnaire:

On the following pages the Questionnaire is given including explanation on how to fill it in. To actually fill in yours, please use the Questionnaire template from the separate questionnaire document.

- One page per Contractor
- One page for the Basic mode (if available for that contractor), listing all the Applications offered in that basic mode. If Ancillary Facilitators are available in "basic mode", mention it!
- One page per each of the Enhance Service modes (if any for that contractor), listing for each all the Applications offered in this particular Enhanced Service mode.
- One page describing each Application and the list of the available Service Modes by which the Application is reachable (Offered in Basic mode, Enhanced mode with Ancillary Basic mode and possibly Ancillary Facilitators.

Because in version 6 of the reference model the item of “how shall I represent the content and the service technologies for a given service?” was added, the questionnaire is also changed. The questionnaire that has been send to the partners is therefor slightly different.

The next time

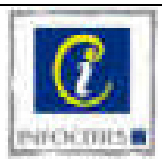
Our advices for any of the readers who will do a similar research in the future.
We have noticed it is not easy to keep the attention of all participants to the work we have done. Presentation should therefor be well accessible and easy to overview. this web-based-report attepts to do so.

Getting feedback

Doing a questionnaire is most definitely easier to do with a web form than using a document. Here are the advantages and disadvantages:
document advantage: 1) It is more flexible for the user. sections can be delete if not applicable and multiplied if more is needed. 2) Information can be fed back by any means (fax, e-mail, etc.).
Document disadvantage: 1) File size. 2) Text editor version problems. 3) Different styles of using a word editor. 4) No immediate overview.
Web form advantage: 1) Feedback is led immediately into database. 2) Uniform format.
Web form disadvantage: 1) less flexible. (comment fields should always be added.)
On http://magica.dma.be/infocities/index.htm you can see a web based questionnaire, on-line with help pages.

- getting information and results across.

Person to person meetings are best to keep the attention. We therefor intend to organise a Technical Workshop during the INFOCITIES seminar in Den Haag in March 1999.



Date of filling: *<YYYY-MM-DD>*

1. Contractor QUESTIONNAIRE

please use the Questionnaire template from the separate questionnaire document.

1.1- CONTRACTOR

< Insert here the name of the Contractor >

1.2- CONTACT to the CONTRACTOR

- WEB site address: URL: http://www. *<name>.<domain>*
- WEB master: *<name> @ <domain>*
- Local project leader: *<name> @ <domain>*

<Full address of the Contractor & Contact: Name, Mail address, Tel., Fax., etc >

If not available: *< Explain why not>*

1.3-Service modes on OFFER (or planned to be on OFFER)

- Basic Service mode: *<yes or no>*

- Enhanced Service mode ES 1: *<give a name to the Enhanced Service ES 1, if any >*
- Enhanced Service mode ES 2: *<give a name to the Enhanced Service ES 2, if any >*
- Enhanced Service mode ES 3: *<give a name to the Enhanced Service ES 3, if any >*
- Enhanced Service mode ES 4: *<give a name to the Enhanced Service ES 4, if any >*

……

1.4-Intranet

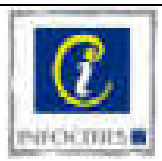
- If the contractor has organised (or plan to organise) a boundary to the access space:
  <explain and give the technical characteristics>

1.5-Licensing policy

- If the contractor has organised (or plan to organise) a boundary to the access space:
  <explain the licensing policy to the tools and the intellectual rights>

- If the contractor has (or plan to have) specific general licensing rules for the applications:

  <explain and give the characteristics>



Date of filling: *<YYYY-MM-DD>*

2. BASIC MODE QUESTIONNAIRE

please use the Questionnaire template from the separate questionnaire document.

2.1- CONTRACTOR

< Insert here the name of the Contractor >

2.2- SHORT DESCRIPTION OF THE ACCESS NETWORKS AVAILABLE OR PLANNED

< PSTN / ISDN and other characteristics >
< Give explanations if ancillary facilities have been organised: like mirroring, cache, proxy or squid redirectors>

2.3- LIST OF APPLICATIONS OFFERED (or planned to be offered) IN BASIC MODE

<for each application give the name of the Application, and the applicable situation: at paragraph 5.3 (cases A to H and option P to T); at paragraph 5.4 (cases V to U)>

- Application A 1: *<give a name to the Application A 1, if any > <give stage>*
- Application A 2: *<give a name to the Application A 2, if any > <give stage>*
- Application A 3: *<give a name to the Application A 3, if any > <give stage>*
- Application A 4: *<give a name to the Application A 4, if any > <give stage>*

……

3 ENHANCED SERVICE QUESTIONNAIRE

please use the Questionnaire template from the separate questionnaire document.
<Fill one page per Enhanced Service mode applicable for the contractor>

3.1- CONTRACTOR

< Insert here the name and co-ordinates of the Contractor >

3.2- IDENTIFIER OF THE ENHANCED SERVICE

<identifier as mentioned at the point 2.3 of your Contractor questionnaire >

3.3- SHORT DESCRIPTION OF YOUR ENHANCED SERVICE MODE

< A 100 word description>

3.4- KEY WORDS

< The applicable key words >

3.5- Enhanced service characteristics

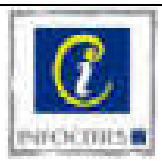
- Stage: *<give stage>*
- WEB site address: URL: *<if any>:* http://www. *<name>.<domain>*
- WEB master: *<if the Enhanced Service has one>: <name> @ <domain>*
- Which access mode? *< 5.1- § 1 or 5.1-§ 3 or 5.1-§ 2.3 to §2.5 or 5.1-§ 3 to §5? >*
- Which Access space boundary? *< 5.2- § or 5.2- §§ ? > <add boundary description>*
- Access criteria for the local domain? *< If 5.2- §§, criteria for affiliation & control (password)?>*
- Which return mode? *< 5.3- § A to 5.3- § G ? and option P to T >*
- Which mode of organisation of the service? *< 5.4- § W to 5.4- § U ? >*
- Which compatibility? *< Fill all cases applicable 6- § 1 to § 3 ? >*
- Which interoperability *< Explain your possibilities in relation to 7 >*
- Ready to licence, sell, …? *< Explain your policy for migration of your service type >*
- Which representation Technique *< Explain how the content of your service is represented >*
- Others *< Explain your policy>*

If not available: *< Explain why not and fill the point 8.5 >*

3.6- LIST OF APPLICATIONS OFFERED IN ENHANCED MODE

- Application AE 1: *<give a name to the Application AE 1, if any > <give stage>*
- Application AE 2: *<give a name to the Application AE 2, if any > <give stage>*
- Application AE 3: *<give a name to the Application AE 3, if any > <give stage>*
- Application AE 4: *<give a name to the Application AE 4, if any > <give stage>*

……



Date of filling: *<YYYY-MM-DD>*

4 APPLICATION QUESTIONNAIRE

please use the Questionnaire template from the separate questionnaire document.
<Fill one page per Application applicable for the contractor>
Please also refer to the questionnaire on Intelligent Agents of Mark Bergers. (see chapter 5, 6b)

4.1- CONTRACTOR

< Insert here the name and co-ordinates of the Contractor >

4.2- SHORT DESCRIPTION OF YOUR APPLICATION

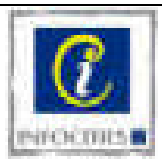
< preferably according to the simplified taxonomy (point C. of the Chapter 5) without filling the last point (the technical one) of the template >

4.3- KEY WORDS

< The applicable key words >

4.4- BASIC MODE Access *< See § 7.2 ; if you have it, give the listed info; if not explain >*

- Stage: *<give stage>*
- WEB site address: URL: http://www. *<name>.<domain>*
- WEB master: *<name> @ <domain>*
- Service leader: *<name> @ <domain>*
- Is it a degraded service of the application?
  <If yes, then fill the point 4.5 & following and explain there what remains >
- Which access mode? *< 5.1- § 2.1 or 5.1- § 2.2 ? >*
- Which access space boundary? *< 5.2- § or 5.2- §§ ? > <add boundary description>*
- Access criteria (for the local domain)? *< If 5.2- §§, criteria for affiliation & control (password)?>*
- Which return mode? *< 5.3- § A to 5.3- § G ? and option P to T >*
- Which mode of organisation of the service? *< 5.4- § W to 5.4- § U ? >*
- Which compatibility? *< Fill all cases applicable 6- § 1 to § 3 ? >*
- Ready to licence, sell, …? *< Explain your policy for migration of your service type >*
- Which representation Technique *< Explain how the content of your service is represented >*
- Others



4.5-ENHANCED MODE Access (AE 1)

- Stage: *<give stage>*
- WEB site address: URL: http://www. *<address>*
- WEB master: *<name> @ <domain>*
- Service leader: *<name> @ <domain>*
- Which access mode? *< 5.1- § 1 to § 4.2 ? >*
- Which access space boundary? *< 5.2- § or 5.2- §§ ? > <add boundary description>*
- Access criteria(for the local domain)? *< If 5.2- §§, criteria for affiliation & control (password)?>*
- Which return mode? *< 5.3- § A to 5.3- § G ? and option P to T >*
- Which mode of organisation of the service? *< 5.4- § W to 5.4- § U ? >*
- Which compatibility? *< Fill all cases applicable 6-§ 1 to § 3 ? >*
- Ready to licence, sell, …? *< Explain your policy for migration of your service type>*
- Which representation Technique *< Explain how the content of your service is represented >*
- Others: *< Explain! For example, why is the service not Internet based? >*

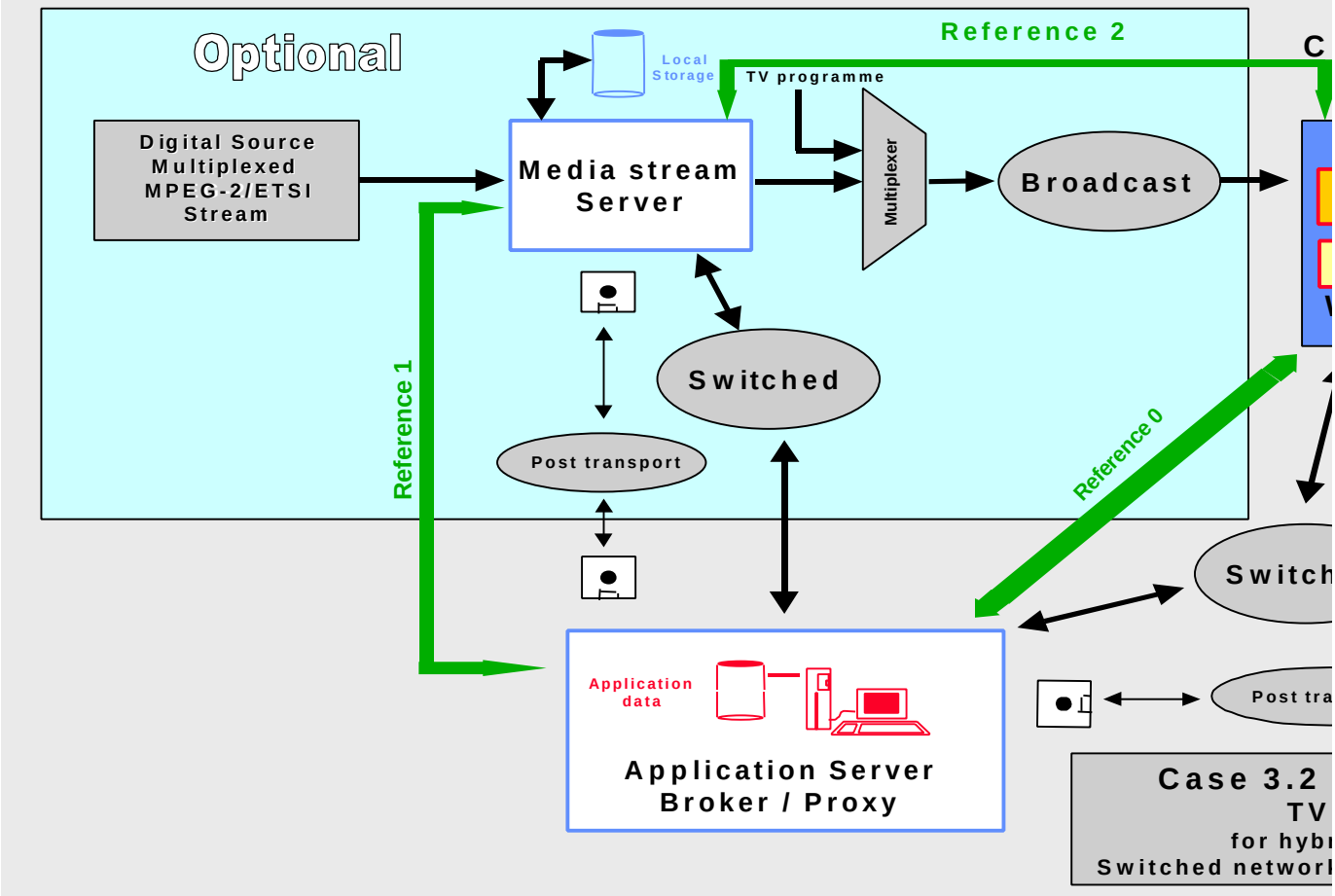
4.6-ENHANCED MODE Access (AE 2)

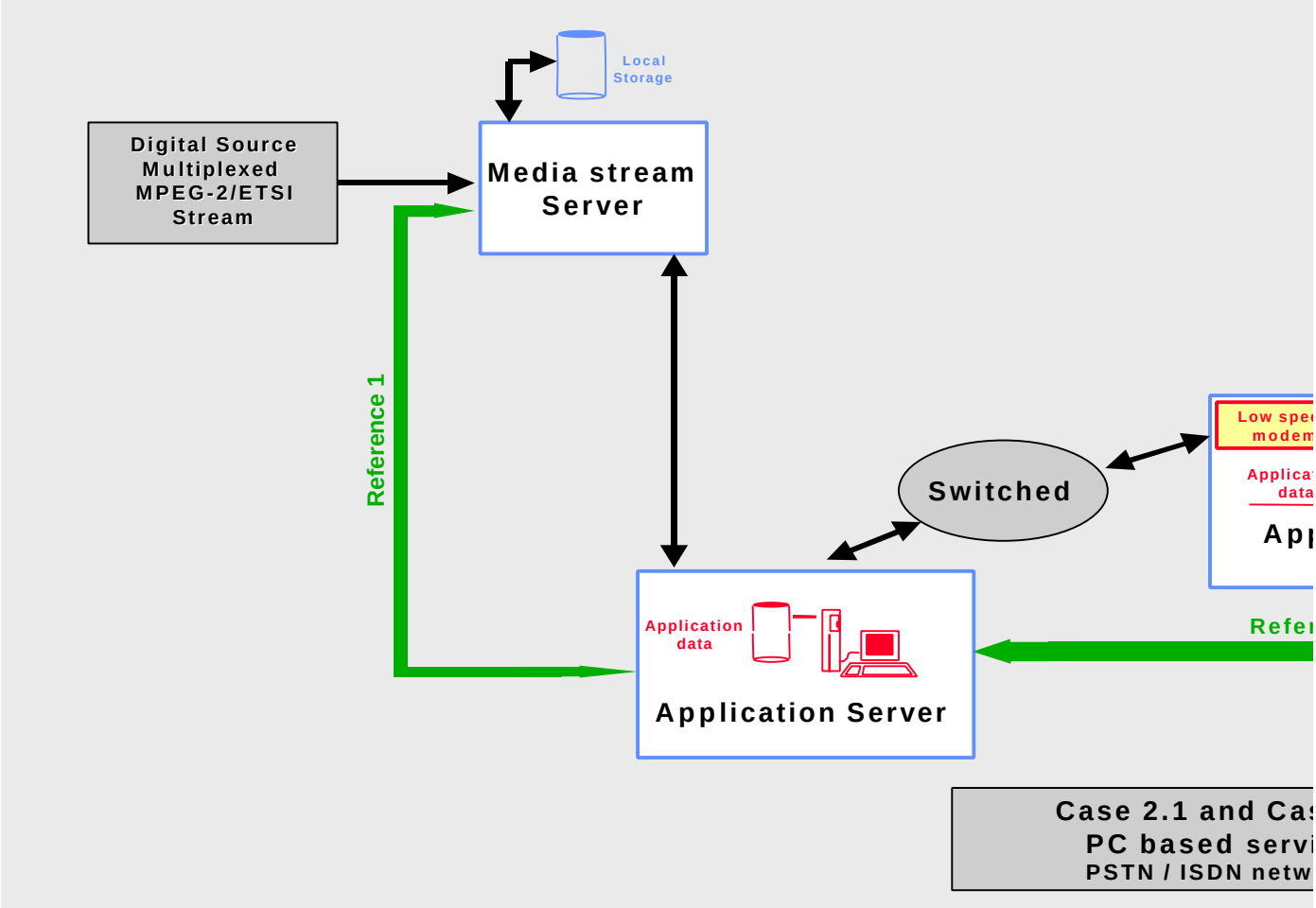
- Stage: *<give stage>*
- WEB site address: URL: http://www. *<address>*
- WEB master: *<name> @ <domain>*
- Service leader: *<name> @ <domain>*
- Which access mode? *< 5.1- § 1 to § 4.2 ? >*
- Which access space boundary? *< 5.2- § or 5.2- §§ ? > <add boundary description>*
- Access criteria(for the local domain)? *< If 5.2- §§, criteria for affiliation & control (password)?>*
- Which return mode? *< 5.3- § A to 5.3- § G ? and option P to T >*
- Which mode of organisation of the service? *< 5.4- § W to 5.4- § U ? >*
- Which compatibility? *< Fill all cases applicable 6-§ 1 to § 3 ? >*
- Ready to licence, sell, …? *< Explain your policy for migration of your service type>*
- Which representation Technique *< Explain how the content of your service is represented >*
- Others: *< Explain! For example, why is the service not Internet based? >*

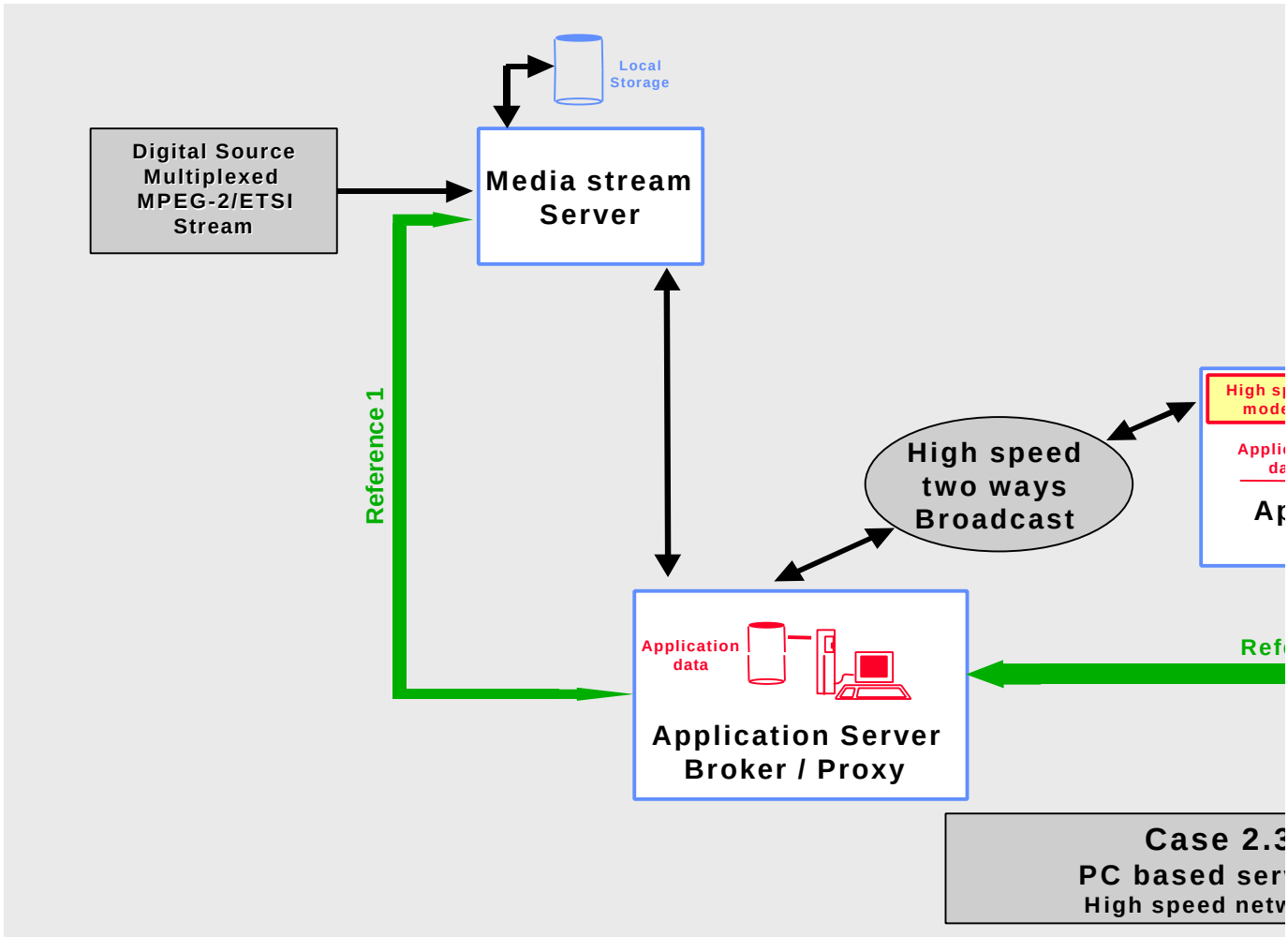
4.7-ENHANCED MODE Access (AE 3)

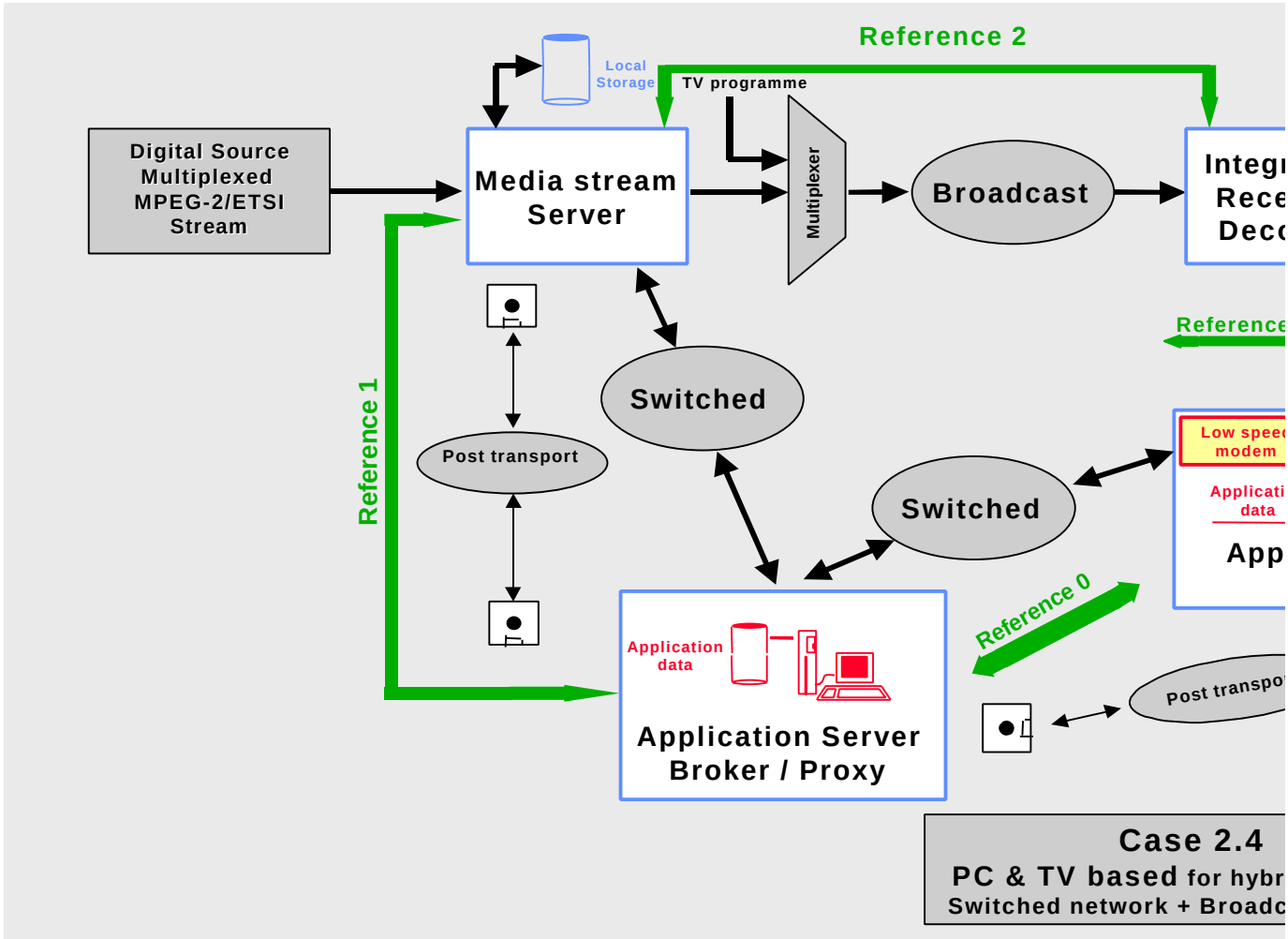
- Stage: *<give stage>*
- WEB site address: URL: http://www. *<address>*
- WEB master: *<name> @ <domain>*
- Service leader: *<name> @ <domain>*
- Which access mode? *< 5.1- § 1 to § 4.2 ? >*
- Which access space boundary? *< 5.2- § or 5.2- §§ ? > <add boundary description>*
- Access criteria(for the local domain)? *< If 5.2- §§, criteria for affiliation & control (password)?>*
- Which return mode? *< 5.3- § A to 5.3- § G ? and option P to T >*
- Which mode of organisation of the service? *< 5.4- § W to 5.4- § U ? >*
- Which compatibility? *< Fill all cases applicable 6-§ 1 to § 3 ? >*
- Ready to licence, sell, …? *< Explain your policy for migration of your service type>*
- Which representation Technique *< Explain how the content of your service is represented >*
- Others: *< Explain! For example, why is the service not Internet based? >*

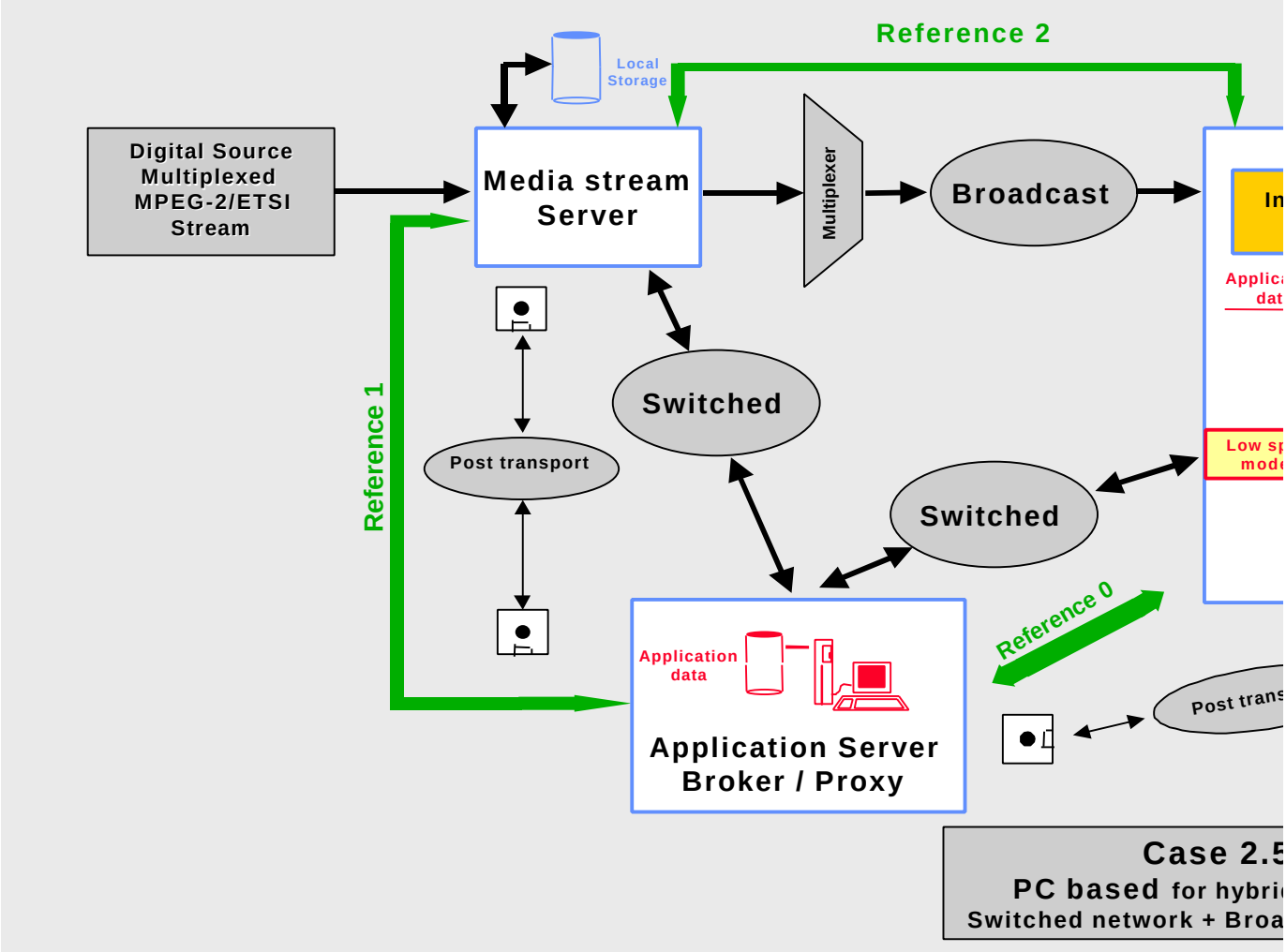
9. APPENDIX A: Seven illustrations of typical cases

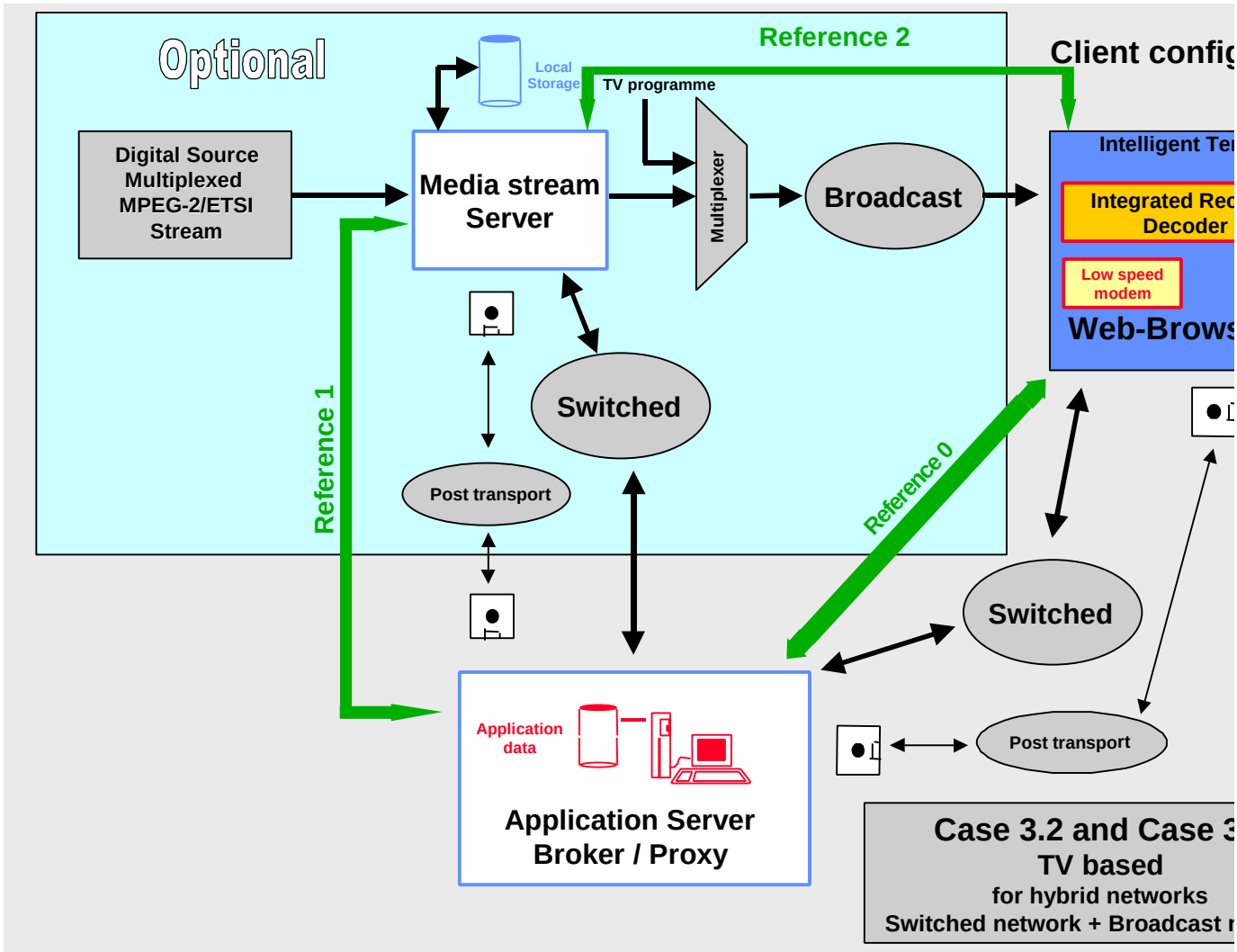


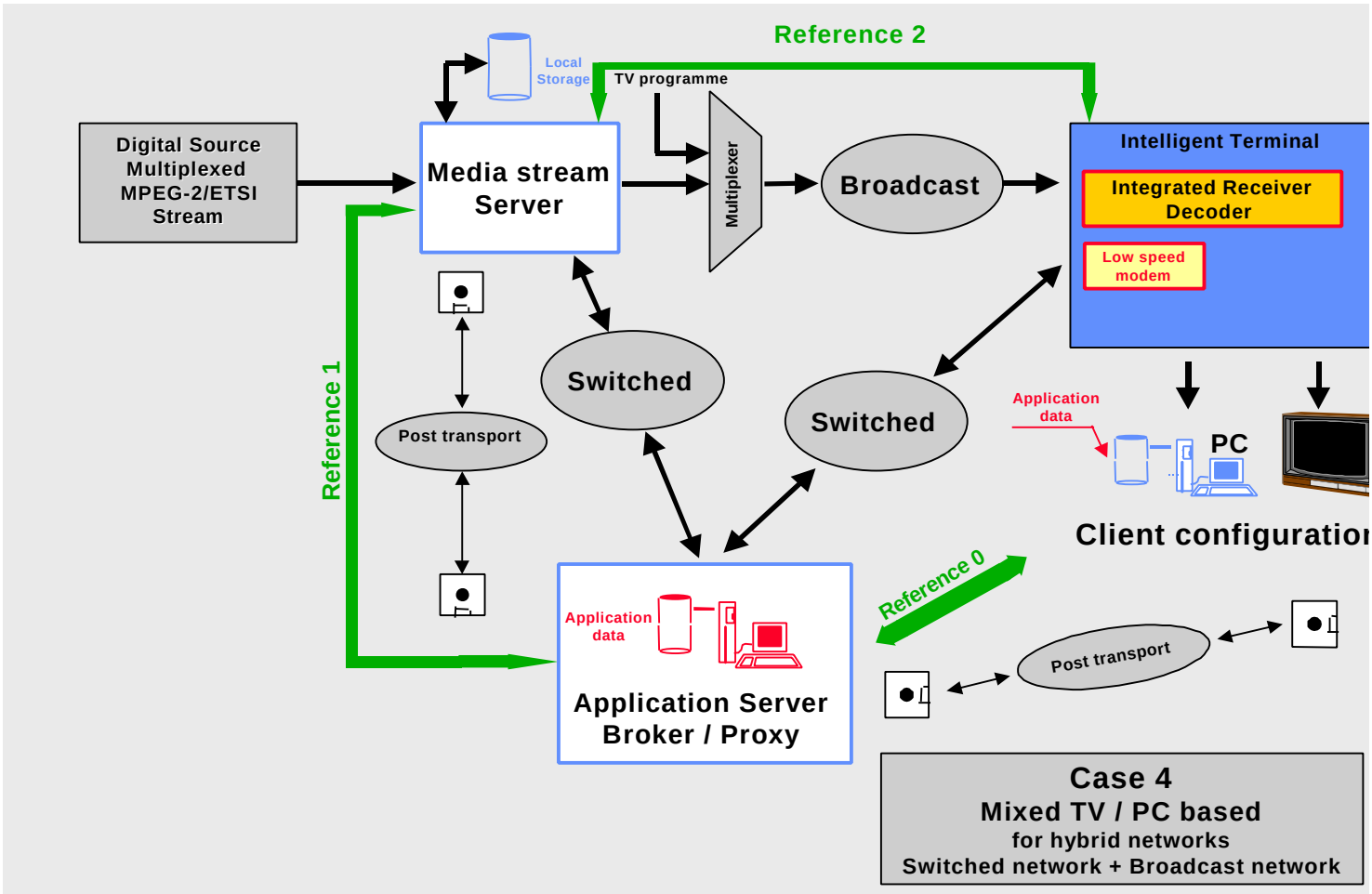


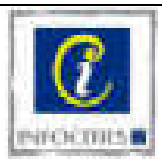












10. APPENDIX B: Glossary

A comprehensive, structured, commented, glossary is available at:

URL: http://www.titan.be

The following glossary refers to the most important entries needed to be understood in order to fill the questionnaires in.

The chapter 5, 6 and 7 include also self explaining definitions and structuring.

- The word "**application**" covers the type of service with its content of information.

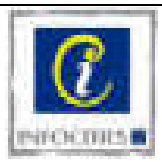
- The word "**cache**" corresponds to the cases where data are duplicated on the bases of the last requested parts, simply limited by the cache size, extracted in the original server. The purpose is to speed up the access to the data for the local users. The cache server works on behalf of the local server in a full automatic and transparent way. It means that the searches, queries, modifications, … could be done with use of the original data when the size of the cache is not large enough for avoiding that too often the requested data have been overwritten by more recent requests.
  See also "proxy", "mirroring" and "cache" which could be used combined through "squid redirector". For more information find a very understandable document written by John Heaton john@manchester.ac.uk available on http://www.mcc.ac.uk/John.

  You can also ask the proceedings of the WWW caching work-shop at http://wwwcache.ja.net

- The word "**duplicated data**" covers the cases when services of a specific common type are supplied at several places but that the data are supplied from several sources. The approach is a particular case of mirror services.

- The word "**encapsulation**" covers the transfer of a set of data from one place to another where the server uses one protocol to ensure the transfer, addressing and other controls to the client, while the client open the "capsule" to recover the data for further processing according to a structuration and representation according to another protocol. The most current encapsulations cover the transfer of data coded with the Internet Protocol (IP) on broadcast networks according to the DVB-ETSI broadcast standard format and protocol.

- The word "**interaction**" covers the fact that the service is given in a way that the "client" has the feeling that he can receive responses or reactions depending of his choices. This can be obtained in several ways:
  - a real time link exist between the "server" and the "client". It is called "full interaction". It means that the service is given from end to end in **real time**;
  - a real time link exist between a local "server" and the "client". It is called "interaction in **proxy/cache/mirror** mode". It means that the service is possibly given from end to end in real time through the use of ancillary servers;



- a **carousel** of information is permanently sent to the client(s). The client tool selects what the client has requested from the carrousel when the requested information passes.
- A **download** of data occurs in the client tool. The client operates in stand alone, as long as the local data suffice.

Note: several of those modes can be combined for performing one service! A typical example is the Internet browsing in full interaction with downloads of Java applets from the Server to the PC of the Client.

- The word "**ISDN**" covers the "Integrated Services Digital Network", the well known universal interactive network which, for the capillary part could used the PSTN two wires infrastructure with its addressing scheme. For the professional use and for the interconnection between exchanges, fibre optics is the most common solution.

- The word "**formats**" cover all ways in which "sense" can be expressed: i.e. the semiotic, syntactical and semantic elements of documents or messages, as well as the interaction types between people through such documents or messages possibly exchanged via telecommunication. In particular, the format means:
  - In which natural language the document is expressed (French, English, Spanish, …)
  - In which way it is represented (Microsoft® Word, WordPerfect, …)
  - In which way it is coded (ASCII, ISO G2, …)

  In particular, the encoding and representation techniques used within a specific format cover the interface protocols for the various layers of the tri-axes analysis model proposed below.
  In particular, the analysis of the content of a message and legal monitoring could be based on these formats.

- The word "**hybrid**" covers the cases when a service is given using more than one network: for instance the PSTN for interaction in the requests and the Satellite for the broadcast of huge set of data.

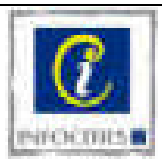
- The word "**media home platform**" (**MHP)** covers the way in which hybrid and mixed services could be obtained at home, in particular in liaison with cable networks. The MHP is planned to be release by the DVB in mid 1998.

- The word "**mirror**" corresponds to the cases where data are duplicated with their structure and content. The purpose is to speed up the access to the data for the local users. It means that the searches, queries, modifications, … could be done without using necessarily the original data. In simple mirroring, the update is made on the initiative of the master server. So there is a risk that the local data will not be at the last revision.
  See also "proxy", "mirroring" and "cache" which could be used combined through "squid redirector". For more information find a very understandable document written by John Heaton john@manchester.ac.uk available on http://www.mcc.ac.uk/John.

- The word "**mixed**" covers the type of service which is given through one type of equipment for several types of services. For example, the access to the TV broadcast and the Internet Web service through an IRD connected to the cable network.

- The word "**piping**" covers the transfer of a set of data from one place to another where the client is listening and the server sends them when it want to.

- The word "**proxy**" corresponds to the cases where data are duplicated with their structure and content with



reference to the original. The purpose is to speed up the access to the data for the local users. The proxy server works on behalf of the master server. It means that the searches, queries, modifications, … could be done with limited use of the original data (simply checking that the local data are up-to-date and, if not download of the updating).

See also "proxy", "mirroring" and "cache" which could be used combined through "squid redirector". For more information find a very understandable document written by John Heaton john@manchester.ac.uk available on http://www.mcc.ac.uk/John.

- The word "**PSTN**" covers the "Public Switched Telephone Network", the well known two wires infrastructure with its addressing scheme.

- The word "**rooming**" covers the fact that a telecom service provider supply a service of world type (like GSM or Digital TV) by him self for his own subscribers and supplies it also to the customers/subscribers of colleagues when, casually, they enter in his sphere of action.

- The word "**service**" covers all types of multimedia services and programmes, whatever medium they use: CD-ROM, etc. (in non-real time), Satellite, Cable, Fibre Optic, terrestrial radio, etc. (in real-time); whatever the mode: broadcast, addressed, with interaction, client-server, client-server-client, etc.

- The word "**stage**" covers the main phases of a project:
  - **M stage:** Management "go" given on the bases of a "strategy" document;
  - **F stage:** Functional definition ready;
  - **P stage:** Product ready and validated;
  - **T stage:** Trial for evaluation before launch at large scale;
  - **O stage:** Running operations and maintenance;
  - **E stage:** End of life; date for end of service decided

- The word "**squid redirector**" corresponds to the cases where the techniques of "proxy", of "cache" and/or "mirror" are combined to make profit of the advantages of all those facilities. The purpose is to speed up the access to the data for the local users and to optimize the use of the resources. The squid redirector works on behalf of the local server on contract with the master servers boosted by the redirector.

  See also "mirror", "proxy" and "cache". For more information find a very understandable document written by John Heaton john@manchester.ac.uk available on http://www.mcc.ac.uk/John.

- The word "**streaming**" covers the transfer of data from one place to another where the client is listening the stream as it comes. The stream can include data intended to be sent for different clients (including broadcast to all listeners); the stream can include several consistent set of data called "programs".