



High Level Strategy Group
for ICT Standards

HLSG REPORT No. 1

**Barriers to Broadband Information
Networking**

Edition 1.0 - Sept. 1996

Author: T Rowbotham
Director, Technology
BT Laboratories
Martlesham Heath
Ipswich
IP5 7RE
UK

CONTENTS

1. INTRODUCTION.....	4
2. SCOPE OF THE PROJECT.....	4
3. GAPS IN STANDARDS, LEGISLATION AND POLICY WHICH IMPEDE THE DEPLOYMENT AND USE OF EUROPEAN BROADBAND NETWORKS	5
3.1 Architectural Issues.....	5
3.2 Security	6
3.3 The Terminal.....	6
3.4 Terminal to Value Added Service Provider (VASP) or Basic Telecommunications Provider	6
3.5 Content Provider	7
3.6 Terminal to Information Service Provider, Terminal to VASP/PNO, Information Service Provider/VASP/PNO to Content Provider.....	7
3.7 Terminal to VASP, VASP to PNO	8
3.8 Terminal to Information Service Provider, Information Service Provider to Content Provider	8
3.9 Interworking and Interoperability	8
4. NON-TECHNICAL BARRIERS TO A BROADBAND INFORMATION INFRASTRUCTURE.....	9
4.1 Minimal Regulation	9
4.2 Legal Framework	9
4.3 Global Issues	9
4.4 Third Party Trust Services	9
4.5 Government use of Information Networks	10
4.6 Public Broadband Access	10
4.7 Naming, Numbering and Addressing.....	10
5. RECOMMENDATIONS	11
6. NOTE TO ANNEX A	12
7. ABBREVIATIONS	12
8. REFERENCES.....	13
9. HISTORY	13
ANNEX A INFRASTRUCTURE STANDARDS REQUIRED FOR AN APPLICATION TO RUN ON A BROADBAND NETWORK.....	14
ANNEX B DEFINITIONS.....	19

1. Introduction

At the 2nd meeting of the High Level Strategy Group (HLSG) on ICT Standards [1], three projects were set up:

- Broadband Infrastructure Interoperability
- Barriers to Electronic Commerce in support of SMEs
- City Information Services

This report summarises the findings of the team set up to carry out the first project on Broadband Infrastructure Interoperability.

The recommendations are addressed primarily to the ICT Standards Board (ICT-SB), the European Commission (EC) and to national governments.

2. Scope of the Project

The scope of this project was taken to be the identification, in strategy terms, of what must be done to achieve a pan-European Broadband Information Infrastructure. This is a wider question than simply considering interoperability between broadband telecommunications networks, and the title of the report has been chosen to reflect this.

The method used was to answer the question:

“What barriers would prevent the operator of an application of the broadband information infrastructure from delivering it to customers across Europe?”

The effect of starting, in this way, with the user of the EII (European Information Infrastructure) is inevitably to broaden the scope of the task from that of a narrow consideration of technical barriers to the roll-out of a broadband network. However, there seems little point in identifying or solving technical and standards problems that are delaying the realisation of broadband in Europe, if commercial, market or legal problems mean that broadband still does not happen and broadband terminals do not become available.

Just as important, if the technical and standards problems relating to broadband telecommunications are not solved in a way which is right for the commercial, regulatory and broader legal environment, then broadband applications will not emerge and broadband roll-out will be stunted. The lessons of the past suggest that only by solving technical and standards problems which respond to a requirement in the marketplace, can we expect to speed successful installation and take-up of broadband infrastructure.

Therefore, by identifying the non-technical as well as the technical barriers, we are, in effect, suggesting the kind of commercial environment in which broadband will be used, and without which the work on technical barriers may well prove a waste of effort.

3. Gaps in Standards, Legislation and Policy which impede the deployment and use of European Broadband Networks

This section lists the key issues to be addressed by standards bodies, legislators and regulators to enable a broadband information infrastructure to come about. It is not exhaustive but focuses on gaps in standards, legislation and government policy which could seriously impede the spread of broadband applications in Europe. The interfaces referred to are shown in Figure 1, together with 'stop signs' indicating barriers discussed in the following sections. Recommendation numbers from Section 5 are shown inside the stop sign. Red stop signs have resulted in high priority recommendations. Barriers considered lower priority are shown in orange. Barriers that are discussed but have not resulted in recommendations are shown in grey.

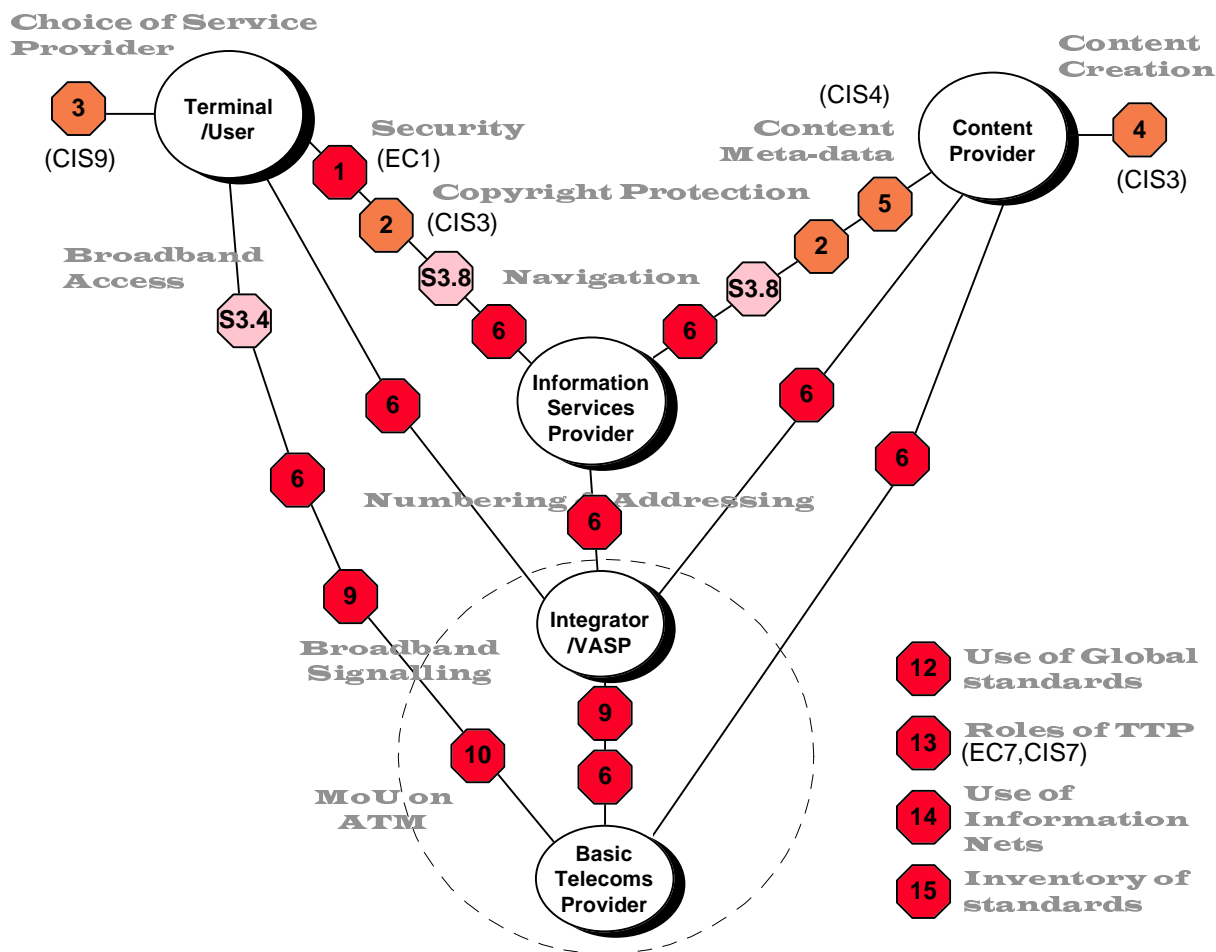


Figure 1: Location of Technical Barriers.

Section 4 makes further recommendations on some of the non-technical barriers to a broadband information infrastructure. These are also shown in Figure 1 although they are harder to allocate. Recommendations corresponding to those included in the other HLSG project reports "Electronic Commerce in support of SMEs" (ECn) and "City Information Services" (CISn) are also shown.

3.1 Architectural Issues

These are issues affecting the entire infrastructure.

REUSABILITY OF BUILDING BLOCKS. The costs of implementing one-off solutions for Information Networking applications is inhibiting the growth of information services and networks as a whole. A way must be found of re-using building blocks at a level higher than simply re-use of software code.




3.2 Security

Security encompasses a wide range of issues, including encryption, authentication, access control and authorisation, as defined in Annex B. This is a difficult area requiring collaboration by a variety of types of organisation (technical developers, standards writers, legislators and government planners). There are urgent issues that would impede an applications operator from deploying a commercial service using a broadband network. For example, agreement is needed on an encryption policy which meets government requirements for the control of crime and terrorism, whilst safeguarding commercial transactions. Many international initiatives are in progress that impinge upon this. It is not that we need one policy, but we need a set of stable policies that do not impede business use of, for example, electronic commerce.

Safe encryption algorithms are currently classed as munitions of war by most governments, and their export is restricted. Following the end of COCOM, a new framework, the Wassenaar agreement, is being established to harmonise controls. Legislation in many countries is currently being changed to reflect the needs of secure exchange of information.


An option for managing the use of encryption which has received wide-spread support is the development of Trust Services. Whilst there is a European policy on this at present the national frameworks to support this are not yet in place. This is a legislative and a standards problem.

In the longer term, a security architecture is required and work should be put in hand to create and agree such an architecture. In the meantime, the following are high priority and require the use of strong encryption. For this reason we recommend that these items are studied first:

- a) **INTRANET SECURITY.** This provides a protected environment for closed user groups, and includes the introduction of firewalls between domains to prevent unauthorised access to information. This service is typically provided to large multinationals by network providers. 
- b) **SECURE PAYMENT.** This would allow secure payment for goods and services to be made electronically. A trusted third party is required to guarantee the transaction as well as providing keys for encryption. This service is typically provided today by banks to customers. 
(EC1)
The issue of secure payment has been considered by the HLSG project "Barriers to Electronic Commerce in support of SMEs" [2] and is not considered further here.
- c) **CONTENT PROTECTION.** Systems are needed which allow control of distribution of films etc. so that owners are paid. These would rely on technologies such as electronic watermarking, so that content and parts of content can be identified. However, these need: 
(CIS6)
 - (i) standards
 - (ii) regulation to ensure terminal equipment, including software, complies with the standards.

This issue is also being looked at by the HLSG project "City Information Services" [3].

3.3 The Terminal

- a) **USER CHOICE OF SERVICE PROVIDER.** Standards exist for Broadband Terminals (Set Top Boxes) which allow users to choose between service providers, but these are not being implemented in Europe. 
(CIS9)

This issue is also being looked at by the HLSG project "City Information Services" [3].

ICT-SB should ensure that there is only one consistent set of standards for broadband terminals. These should allow for the economic creation of broadband terminals commensurate with the range of services they offer.

3.4 Terminal to Value Added Service Provider (VASP) or Basic Telecommunications Provider

There is no true **INTERACTIVE BROADBAND ACCESS** to the home. This is largely an economic problem, which requires that conditions be made right - i.e. adequate incentive be provided to basic telecommunications providers. The DAVIC solution is too expensive for small operators. The options for overcoming this barrier include the use of cable modems on existing cable networks, as well as the deployment of broadband access by PNOs.

3.5 Content Provider

- a) **CONTENT CREATION and CONTENT ENCODING.** There are currently no standards for interfaces within the content provider domain. Whilst this is not a problem for large, experienced content providers such as traditional movie-makers and TV broadcasters, it impedes information service providers who wish to assist many small content providers to join their networks.

4
(CIS3)

This is a standards problem. ICT-SB should ensure that standards are developed for content creation and content encoding that are applicable within the content provider domain. This issue is also being looked at by the HLSG project "City Information Services" [3].

- b) **CONTENT PROVIDER to INFORMATION SERVICE PROVIDER CONTROL DATA.** The standards agreed by DAVIC for the meta-data¹ which flows between the Content Provider's infrastructure and the VoD Server may not prove adequate for applications where there is a large number of 'short' files (e.g. for teleshopping which contains many short image files). A robust standard capable of supporting all applications is vital. At present, the link between Content Provider and VoD Server is generally achieved by means of a messenger on a motorcycle, and this is limiting the growth of interactive TV.

5
(CIS4)

This is a standards problem. ICT-SB should agree standards for content meta-data that are also usable for applications involving a large number of short files. This issue is also being looked at by the HLSG project "City Information Services" [3].

Additionally, the need has been identified for an Application Control Interface between the Content Provider and the Information Service Provider. This would enable the transfer of metadata relating to the Content Provider's application, such as the type of service via which it may be offered or the way in which it is presented, rather than to the content itself.

3.6 Terminal to Information Service Provider, Terminal to VASP/PNO, Information Service Provider/VASP/PNO to Content Provider

There are several **NAMING, NUMBERING AND ADDRESSING** issues to be addressed. At the Terminal/Information Service Provider/Content Provider level, the use of names and the naming conventions defined by the IETF (Internet Engineering Task Force) are well established. The increasing use of names that require translation to addresses generates an increasing burden on the systems that undertake this function. The current system where such servers are provided as part of the requirements placed on a name registration authority may need reviewing. This is a policy problem.

6

The roll-out of large ATM public networks will be delayed unless the issue of numbering and addressing for multiple domains, and multiple providers within domains, is solved. Within the scope of the requirement for a minimum pan-European service, there should remain a degree of flexibility for the numbering and addressing formats to be offered. The international standards recognise both E.164 and OSI NSAP (Network Service Access Point) formats for use with ATM networks. ICT-SB should ensure that both E.164 and Internet addressing is supportable by a broadband information network.

For the VASP, the main contender is IP addressing, with OSI NSAP addressing being considered as an option for ATM services. Internet standards which are established in the marketplace should be taken into account by ICT-SB and its members.

7

In the information era it is not inevitable that E.164 will remain the major way of identifying the user of services. Even in today's narrowband information services, the name of a service provider or user is far more important to the user than the arbitrary numbers that are used for addressing within the network. This different role for names and addresses is not reflected in the regulations, and it will not be possible to build large networks that can support the complex routing decisions that are required. ICT-SB should encourage the development of standards that are based on the importance of naming to the user, and

8

¹ Information about, for example, a film for indexing purposes. This might include the writer's name, the director, the censorship category, etc.

provide a framework for the registration of names.

3.7 Terminal to VASP, VASP to PNO

BROADBAND SIGNALLING is still not ready for implementation and is in danger of being over-specified. Agreed interfaces between VASPs (Value-Added Service Providers) and PNOs (Public Network Operators) are required (i.e. agreement about access to IN, and control of switched network).



This is a regulatory and a standards problem. It is desirable that services can be provided seamlessly over networks using different technologies and in public and private domains as noted in Section 3.9. ICT-SB should ensure that a consistent and not too complex set of signalling standards is available to enable seamless interoperability of networks, (value-added) services and applications, both in the public and private domain.

3.8 Terminal to Information Service Provider, Information Service Provider to Content Provider

Advanced **NAVIGATION** techniques, such as the use of natural language processing and agent technology to look for products, services and information, will require standards in due course. However, European standardisation work on these still emerging technologies would be premature and stifle innovation at present.

3.9 Interworking and Interoperability

Interworking and interoperability are defined in Annex B. They are important issues that could delay the uptake of services on a broadband information network. Issues seen as most important include:

- Interworking between services in a network independent fashion.
Similar services offered on different networks (e.g. ISDN, B-ISDN, PSTN and Cable) should be interoperable.
- Interworking between terminals on different networks.
It is important that existing terminals should be able to interwork with new network services and that new terminals can interwork with existing services (e.g. between G3 and G4 facsimile terminals).

ICT-SB should investigate the standards that are needed to achieve interworking and interoperability and commission the required technical standards from the appropriate standards bodies.

ETNO should investigate the establishment of an MoU to enable interoperable European ATM services by an agreed date. The technical standards need to address the Broadband Inter-Carrier Interface (B-ICI), the Network Node Interface (NNI), the User-Network Interface (UNI), and the management interfaces (M5) that are necessary to ensure interoperability of management services. To be effective, the scope should not be widened to include interworking with existing networks, although this is also considered important. An MoU should be established in time for the World-Wide G7 conference on standardisation issues related to interconnectivity of networks and interoperability of applications [4], or by February 1997 at the latest.



4. Non-Technical Barriers to a Broadband Information Infrastructure

As well as challenges which are amenable to technical development or standardisation, the effective spread of a European broadband information infrastructure poses many non-technical problems which government must address if it is to be achieved. These span economic, legal, regulation and financial spheres, and also include process problems requiring government action. Some of these barriers were touched on in Section 3 and are developed further here.

The main messages from the HLSG to the European Commission (EC) and to national governments in Europe should include:

4.1 Minimal Regulation

Regulation should be frequently reviewed to ensure that it is at the minimum level consistent with meeting the objectives of industry openness and competition, to foster user choice and keen pricing.

Care should be taken to ensure that regulation does not overly constrain the commercial environment, inhibiting natural change. This would cause the EC to be less competitive than other environments.

4.2 Legal Framework

The EC is responsible for ensuring that there is a legal framework which encourages the spread of information services, with the following characteristics:

- Copyright will be protected by arrangements which support and endorse the use of technologies such as watermarking and other relevant techniques.
- In order to enable Trust Services and to allow authentication of transaction messages generally (see below), digital signature will be defined and recognised and the techniques supporting it will be endorsed. To be effective this requires the use of encryption.
- Defamation and obscenity over information networks will be clearly and consistently defined and subject to law that makes sense. Implementation will depend on the medium.
- Legal barriers to the use of information networks, such as insistence on the use of paper for certain documents, should be carefully considered, and, wherever possible, removed, and criteria for what constitutes a “legal” document will have been updated and clarified.



(EC09)

The application of the laws of one country to or via service providers operating infrastructure in a different country (presumably under that country's laws) must be clarified. Apart from being undemocratic, this leads to ambiguity, and it is almost impossible to ensure that no breach takes place. Government should resolve this problem, by treaty if necessary.

4.3 Global Issues

Most services should be capable of being offered globally. Unless legal frameworks around the world are harmonised, the spread of information services will be seriously impeded.

Standards should also be applicable globally where possible. Standards should be chosen from the most appropriate place and the emphasis should not be on promoting European standards exclusively. EU initiatives in this field should take full account of leading global activities, in particular the more market-oriented fora such as DAVIC, OMG, IETF, W3C and ATM Forum.



4.4 Third Party Trust Services

There is a wide measure of agreement that Third Party Trust Services offer a way to resolve the conflict between:

- a) the need to provide secure (i.e. encrypted authorisation and non-repudiation) access to information and evidence of transactions,

- b) the requirement to protect society from crime and terrorism, planned and/or executed via information networks.

The EC should provide a legal and procedural framework for Trust Services, by setting the rules, licensing Trust Services providers, etc.



This issue is also being looked at by the HLSG projects “Electronic Commerce in support of SMEs” [2] and “City Information Services” [3].

(EC07)
(CIS7)

4.5 Government use of Information Networks

Government typically spends about one third of GDP each year. The opportunities for encouraging the spread of information services as substitutes for more traditional methods and systems is enormous. Government should be the most extensive and enthusiastic participant in the Information Society.

Government should also encourage the development of secure information systems allowing the transfer of cash, including across national borders, in order to improve conditions for trade between countries.



4.6 Public Broadband Access

Many services are either impossible or unattractive without true, interactive broadband access. However, providing it represents an enormous up-front investment cost for network providers. This is an economic problem which was identified in Section 3. Government should carefully consider how to create an environment in which such investment is commercially attractive.

Care must be taken not to set universal standards for user access at such a level that they:

- a) cannot be rolled out for technical reasons,
- b) are too expensive to provide.

A long period of transition may be needed to ensure that universal access to Information Services is possible. Ideally, Information Services should be provided in a network independent fashion, so that the same service can be provided over PSTN, Cable, ISDN, mobile or Internet.

4.7 Naming, Numbering and Addressing

The absence of an agreed technical approach to naming, numbering and addressing was identified in Section 3. Although these are technical issues, the administration of names and numbers can be used to either enhance competition or restrict it, and so there are commercial implications. Naming, numbering and addressing is therefore the subject of regulatory interest.

This subject becomes ever more complex as convergence proceeds, and a model of the Information Industry, flexible enough to cope with developments over time, is needed by both Government and Industry itself. In considering action with regard to naming and numbering, EC and national governments should, using such a model as a guide, favour schemes which lend themselves to delegated administration in a highly pluralist (i.e. competitive at all levels) environment. These schemes should be apposite to the concerns of the Information Age where, for example, geography becomes ever less important, access by the user to services from multiple points and for multiple purposes ever more important, and the name becomes the pre-eminent identifier of a user or service rather than the address.

The commercial and economic disadvantages to all players, including end users, of changes to the naming scheme should also be considered (the E.164 number is becoming equivalent to a name).

5. Recommendations

#	to	priority	requirement	section
1	ETNO	1	To encourage the EC to ensure harmonised laws and regulations which allow network operators to provide multinational companies, for example, with secure information networks.	3.2
2	HLSG	2	To devote resources to the study of information content protection.	3.2
3	ICT-SB	2	To ensure that there is only one consistent set of standards for broadband terminals. These should allow for the economic creation of broadband terminals commensurate with the range of services they offer.	3.3
4	ICT-SB	2	To ensure that standards are developed for content creation and content encoding that are applicable within the content provider domain.	3.5
5	ICT-SB	2	To agree standards for content meta-data that are usable for applications involving a large number of short files.	3.5
6	ICT-SB	1	To ensure that E.164, Internet and OSI NSAP addressing are supportable by future broadband information networks.	3.6
7	ICT-SB	1	Internet standards which are established in the marketplace should be taken into account by ICT-SB and its members.	3.6
8	ICT-SB	1	To encourage the development of standards that are based on the importance of naming to the user, and provide a framework for the registration of names.	3.6
9	ICT-SB	1	To ensure that a consistent and not too complex set of signalling standards is available to enable seamless interoperability of networks, (value-added) services and applications, both in the public and private domain.	3.7
10	ETNO	1	To investigate the establishment of an MoU to enable interoperable European ATM services by the dates given in Section 3.9, and to commission the required technical standards from the appropriate standards bodies.	3.9
11	EC/national governments	1	To ensure that the consistent legal framework described in Section 4.2 is established as soon as possible. Otherwise the development of a European Information Infrastructure able to support, for example Electronic Commerce and Information Services, will be severely retarded.	4.2
12	ICT-SB	1	Standards should be applicable globally where possible. Standards should be chosen from the most appropriate place and the emphasis should not be on promoting European standards exclusively.	4.3
13	EC/national governments	1	To clarify rapidly the roles and activity domains of secure trusted third parties (TTP) in the field of secure information networks.	4.4
14	EC	1	To use and encourage the development and use of information networks as substitutes for more traditional methods of exchanging cash and information where appropriate.	4.5
15	ICT-SB	1	To set up and maintain an inventory of standards required for an application to run over a broadband network that could perform a similar function to the table in Annex A. This would be a useful reference to identify gaps in existing technical standards.	6

6. Note to Annex A

Annex A lists the functions required for an application to run over a broadband network and the standards that are either available or where work is in progress to meet the requirements of these functions. Annex A is for information only. It provides a snapshot of the situation as at April 1996 and may not be complete. It does not indicate the adequacy or otherwise of the standards available, or the progress of work not yet complete.

The most important part of Annex A, as far as the HLSG is concerned, is the list of functions required for an application to run over a broadband network. These functions are listed down the left hand side of the table and provide the requirements for standards. The Information Infrastructure Standards Panel (IISP) provides a similar function to the HLSG in the US, and for this reason the correspondence with the IISP 'needs' is also given in the table.

The 3rd column of Annex A lists the European Project on the Information Infrastructure (EPII) projects that are carrying out work of relevance to these functions [5].

It is considered useful for ICT-SB to set up and maintain such an inventory of standards so that they can readily identify gaps in existing technical standards.



7. Abbreviations

B-ICI	Broadband Inter-Carrier Interface
DAVIC	Digital Audio-Visual Council
EC	Commission of the European Union
EII	European Information Infrastructure
EPII	European Project on the Information Infrastructure
ETNO	European Public Telecommunications Network Operators' Association
ETSI	European Telecommunications Standards Institute
GDP	Gross Domestic Product
GII	Global Information Infrastructure
HLSG	High Level Strategy Group for ICT Standards
ICT-SB	ICT Standards Board
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IISP	ANSI Information Infrastructure Standards Panel (US)
ISO	International Organisation for Standardisation
ITU	International Telecommunication Union
ITU-T	ITU - Telecommunication standardisation sector
MoU	Memorandum of Understanding
NNI	Network-Node Interface
NSAP	Network Service Access Point
OMG	Object Management Group
PNO	Public Network Operator
SME	Small or Medium sized Enterprise
STAG	Security Techniques Advisory Group (ETSI)
STB	Set Top Box
TTP	Trusted Third Party
UNI	User-Network Interface
URL	Universal Resource Locator (WWW)
VASP	Value-Added Service Provider
W3C	World-Wide Web Consortium

8. References

- [1] Report of 2nd Meeting of the High Level Strategy Group (HLSG) on ICT Standards, London, 30 October 1995.
- [2] HLSG Project “Barriers to Electronic Commerce in support of SMEs”, Draft V1, C Boulle, 12 July 1996.
- [3] HLSG Project “City Information Services”, Draft 1, G Lütteke, 23 August 1996.
- [4] EC/DGXIII, “Europe’s Way to the Information Society - Update of the Action Plan”, 1 April 1996, available from <http://www.ispo.cec.be/infosoc/legreg/actionla.html>.
- [5] ETSI/EPIISG(96)4 rev 1, “Final report of the European Project on the Information Infrastructure Starter Group (EPIISG)”, 15/3/96.
- [6] ETSI SRC6, “Report of the Sixth Strategic Review Committee on European Information Infrastructure”, June 1995.

9. History

Status	Author	Date	Comments
Drafts A-D	K Dickerson/ B Ralph	26/4/96	Drafts for discussion within BT prior to issuing to ETNO WG on Standards Strategy.
Draft E	K Dickerson	1/5/96	Changes made to Section 3 and Recommendations following discussion and endorsement by ETNO WG on ICT Standards Strategy on 29 April.
Draft F	K Dickerson	20/5/96	Updated following meeting between T Rowbotham (ETNO), K Linden (ECTEL), W Koch (EUROBIT) and G Wahlberg (EACEM) at Heathrow Airport on 17 May 1996.
Draft G	K Dickerson	30/5/96	Updated at meeting with C Boulle in London, 28 May, prior to presentation to ICT-SB, 11 June. Comments from W Koch also included. Recommendations re-ordered according to the sections in the document.
Draft H (Final)	K Dickerson	12/6/96	Correction to Recommendation 6, inclusion of Recommendation 9 on broadband signalling drafted by ETNO WG on ICT Standards Strategy on 10 June.
Issue 1	K Dickerson	22/7/96	Updated and issued following presentation to 6th HLSG, Milan.
Issue 1A	K Dickerson	20/9/96	Figure 1 modified to include recommendation numbers from all 3 HLSG projects.

File Reference: G:\hlsG\bbinf.doc

Annex A Infrastructure Standards required for an Application to run on a Broadband Network

<u>Function</u>	<u>IISP Need</u>	<u>EPII Project</u>	<u>ETSI</u>	<u>ITU</u>	<u>ISO/IEC</u>	<u>IETF</u>	<u>Other</u>
<u>All networks of all types</u>							
Naming	#29, #26	1.5, 2.10				RFC 1101, 1630, 1735 (NARP), 1808 (URL), DNS, CIDR RFC 1517-1519, IPng RFC 826, 903 (ARP, RARP)	ANSA, OMG CORBA services: naming
Numbering/addressing	#17	1.5		E.164, X.121	8348	RFC 791, 1550, RFC 1630 (URLs), RFC 1884	BS 7306 (NSAP addressing)
Security	#9, #21	2.5	ETR 232, ETR 233, TCRTR 042, DTR/NA-002304-5, DTR/NA- 002801	Q29/11	7498-2	RFC 1507-1510, aft, cat, otp, IPSEC wgs	ECMA TR46, TR138
Trust Services Authentication	#32	2.1, 2.5 2.5		X.509		tnfs wg RFC 1826, 1828, 1334	PGP DAVIC 1.1, ECMA TR219
Confidentiality	#31		TCRTR 030, ETR 235			RFC 1827, 1810 (MD5), MOSS	IEEE P1363, PGP, DVB Common Scrambling Mechanism
Integrity Access Control	#39	1.6	DE/NA-002308				DVB Common Scrambling Mechanism
Key Management						PKI wg	IEEE P1363, ECMA TR219, DES Public Key Algorithm
Non-repudiation Security Evaluation Security Management			TCRTR 049, DTR/NA-002701 DTR/NA-002602			MOSS, receipt wg	DAVIC 1.1 ECMA TR205 ECMA TR206, DES Public Key Algorithm
Audit Trail	#35						
Performance							
Speed of delivery	#10					intserv wg	
Responsiveness	#10	1.6				best effort, Intserv wgs	
Resilience	#1, #11	1.6					TINA Fault Management Architecture
Control							
Configuration)		1.6				RFC 1533 (DHCP), 1157 (SNMPv1), 1441-1452 (v2)	TINA Resource Management

<u>Function</u>	<u>IISP Need</u>	<u>EPII Project</u>	<u>ETSI</u>	<u>ITU</u>	<u>ISO/IEC</u>	<u>IETF</u>	<u>Other</u>
Provision) Cessation) Diagnostics) Usage measurement	#34, #35	1.6				SNMP SNMP SNMP, RFC 1333 SNMP	Architecture TINA Connection Management Architecture
Reservation/prioritisation of capacity			DTR/NA-053001			RSVP wg, ST2+, sd	
Directory	#18	1.6		X.500		ids wg, RFC 1836-1838, 1801- 1804, 1684	TINA Resource Management Architecture
Inventory Interworking						SNMP	
Network Interworking		1.3, 1.4	ETS 300 345, ETR 172 DTR/IMCC-00001, DTR/NA- 052102, IN/UMTS Framework DTR/NA-052110, DTR/SMG- 050101, DTR/SMG-051201				DAVIC 1.0
Management Interworking	#34	1.4	IN/UMTS Framework		ISO Internet Management Coexistence (IMCC)		
Service Interoperability	#16	2.7	ETS 300 387, ETR 197, DTR/NA- 060603, DTR/NA-060109, DTR/NA- 061101 NA1 Guidelines	I.130, I.140, I.210			
Application Interoperability 3rd Party Service Provision	#5, #41	2.1, 2.7		T.411-418 (ODA)			OMG CORBA IDL / CORBA 2.0 TINA Service Architecture
Management Network Management	#19	1.6	ETR 062 (TMN/IN), DTR/NA-60801, DTR/SMG-50501	M.3010, M.3020, M.3200, X.710, X.711, X.cnma	9595 (CMISE), 9596-1 (CMIP)	RFC 1157, 1418	TINA Management Architecture, NMF IIMC, OMNIPPOINT
Service Management	#34	1.6, 2.5					NMF Service Management Strategy, SPIRIT, OMNIPPOINT 2 X/Open
Computing Systems (DPE) Management		2.5		X.700 series		7498-4	
Application Management Information Management	#40	3.3					

<u>Function</u>	<u>IISP Need</u>	<u>EPII Project</u>	<u>ETSI</u>	<u>ITU</u>	<u>ISO/IEC</u>	<u>IETF</u>	<u>Other</u>
<u>Telecommunications Networks</u>							
Transport and Control				X.200 (OSI), X.214 (Transport Service)	7498-1 8072	ipng, st2+ wgs	TINA Connection Management Architecture
Bearer control			ETS 300 389, DTR/NA-052112, DTR/NA-052625			RFC 1577 (IP, ARP over ATM), RFC 1390 (IP, ARP over FDDI), RFC 793, intserv wg	
Basic call control			ETS 300 143-144 (N-ISDN) ETS 300 436, 438 (B-ISDN layer 2)	Q.700-704 (SS7), Q.711-714, Q.730, Q.741, Q.761-764, Q.767 (ISDN), Q.771- 775, Q.931, Q.2110, Q.2140, Q.2610, Q.2650 (DSS2-B- ISUP), Q.2660 (N- ISUP-B-ISUP), Q.2761-4 (B-ISUP)		RFC 1112, 1122, IRC, CCCP, sd	IMTC (+PCGW)
Access		1.1, 1.2	ETS 300 436-437 (layer 2) ETS 300 443 (layer 3)	Q.2110, Q.2130 (layer 2), Q.2931 (layer 3), Q.295x (sup serv), V.24, X.21, I.420		PPP, RFC 1055 (SLIP), IGMP	IEEE 802.14, ATMF RBB DAVIC 1.0 Part 8
Terminal Mobility			IN/UMTS Framework ETS 300 303, DTR/NA-052110, DTR/SMG-050101, DTR/SMG- 051201, DTR/SMG-051202	ITU-R Rec. 687 (FPLMTS)		mobile ip wg	
Multicast Routing Enhanced Service Provisioning						RFC 1112, 1584 RFC 1680	TINA Service Architecture
Service creation) Complex call control)			DTR/NA-060603, DTR/NA-060109, DTR/NA-061101 ETS 300 303, ETS 300 374 DE/SPS-01023, DE/SPS-02004, DE/SPS-03038 (INAP for CS2)	Q.2931		RSVP, intserv wgs	IMTC
Address management) Messaging				X.400		addrconf, ipng wgs RFC 821 (SMTP), RFC 1521-2 (MIME), RFC 1421-4 (privacy enhanced mail), mixer, mimesgml, mailext, receipt wgs RFC 959 (FTP)	
File Transfer		2.7	ETS 300 383 (EUROFILE) ETS 300 388 (FTAM), prETS 300				

<u>Function</u>	<u>IISP Need</u>	<u>EPII Project</u>	<u>ETSI</u>	<u>ITU</u>	<u>ISO/IEC</u>	<u>IETF</u>	<u>Other</u>
Document Transfer	#24, #25, #28		409				
Personal Mobility	#3, #23		UPT application protocol			ipng	TINA Service Architecture
<u>Utilisation</u>							
Video coding			ETS 300 174, ETS 300 294	H.261	11172-1/2/3 (MPEG-1) 13818-1/2/3 (MPEG-2)	AVT wg, RTP	ATMF AMS wg, IMTC
Speech coding			ETS 300 163 (NICAM)	G.711, G.722, G.728		AVT wg, RTP	ATMF AMS wg, IMTC
Text coding		3.10, 4.3	ETS 300 382 (Videotex)			AVT wg, RTP	ATMF AMS wg, IMTC
Image coding		2.2		T.81	10918-1 (JPEG)	AVT wg, RTP	ATMF AMS wg, IMTC
Graphics coding		2.2				AVT wg, RTP	ATMF AMS wg. IMTC
VR coding							
<u>Integration of functions</u>							
Voice on information nets						mmusic, avt wgs	TINA Service Architecture ATMF Voice over ATM
Videoconferencing on information nets						mmusic, avt wgs	
Multimedia Mail		2.2		X.400		RFC 1521-2 (MIME)	
<u>Information Networks</u>							
Information capture)	#12, #26, #27, #15	2.2, 2.9					
Information loading)							
Information storage							
Information retrieval		3.2					
Information compression		3.2	DE/TE-01046	T.81, T.171	10918-1 (JPEG) 13522-1 (MHEG)		
Information merging	#38	3.2					
Information recording		3.2					
User interface		2.9, 3.9	ETS 300 382 (VEMMI) ETR 160				
Application creation	#7	2.8, 4.8					

<u>Function</u>	<u>IISP Need</u>	<u>EPII Project</u>	<u>ETSI</u>	<u>ITU</u>	<u>ISO/IEC</u>	<u>IETF</u>	<u>Other</u>
Application protocols	#41	2.7				RFC 959 (FTP), 1157 (SNMP), Telnet, Newsgroups, IRC	OMG IDL
Hypertext			ETR 160			HTML, HTTP wgs	W3C
Hypermedia including VR		2.2				VRML	W3C
Navigation		2.4	ETS 300 382 (videotex)			HTTP wg	TINA Service Architecture
CD-ROM control							DSM-CC (DAVIC)
Trading		4.1					DPE functions (CORBA+)OMG Trading RFP, CommerceNet
User profile	#22, #23	2.9					TINA Service Architecture
Distributed Processing Environment (expandability)	#38	2.7, 2.11	MI/TE-06041 (X.500)	X.500 X.901-904 (ODP)		RFC 1101 (DNS)	OSF DCE, RPC, OMG CORBA 2.0, CORBA services
Personal Intelligent Agent		2.7					TINA Service Architecture
Network Agents (representative of resources)	#37	2.7					TINA Service Architecture
Gateway Provider							TINA Service Architecture
<u>Terminals</u>							
NNI	#2, #3, #4, #6	1.4		G.703-4, G.707-9		Routing protocols (many), RFC 1812 (IPv4 routers)	TINA Connection Management Architecture
API	#8	1.7, 2.8	ETS 300 325 (PCI for ISDN) DE/TE-01043 (file transfer) DE/TE-01045 DE/TE-02025 (PCI) DTR/TE-01063 (MHEG)	SCAI			ECMA 217-218 (CSTA), NMF SPIRIT, X/OPEN XTI (+XAPI)
Set-top box	#14	4.2					IMTC, Winsock-2 DAVIC 1.0, DVB, ATMF AMS, RBB wgs

Annex B Definitions

Agent: As telecommunications, computing, education and entertainment collide to forge the so called information superhighway new opportunities and challenges will arise. One class of solution to help meet these challenges is software agent technology. This branch of systems engineering offers the promise of software being able to act in intelligent manner on the behalf of its human clients. Although there are many definitions of what constitutes a software agent, two main types of agent can be defined:

- (i) Personal Digital Assistants (PDAs): Interface agents act as personal assistants that may perform such tasks as prioritise, filter and organise incoming information, and learn personal preferences. Other personal agents or proxies may be active in searching for information on your behalf or developing contacts with other useful agents or individuals.
- (ii) Co-operating Agents: Complex control and management tasks are also the domain for intelligent agents, but these tend to be of a different class of agents whose modelling power and ability to cooperate and negotiate with other agents is a major factor. These agents are therefore being used for applications such as complex distributed management tasks as would be seen in network and service management and business process control.

API: There are three generic types of interface that are essential to the EII, namely telecommunications interfaces (i.e. UNIs and NNIs), applications protocols (APs), and applications programming interfaces (APIs).

APIs are vital to the development of general processing and storage platforms which can support a wide variety of applications. The API effectively gives independence between the applications above the API and the computing hardware and telecommunications networks which are below the API. While there are emerging standards for APIs, there are currently several de facto standards which must be considered including Microsoft Windows. We anticipate the need for a variety of APIs however, the number should be restricted to a useful set. In addition, standardisation work should recognise that historical standards in this area have been dominated by standards forming processes which do not involve consensus forming including commercial force majeure (e.g. Windows 95) and “free” distribution followed by de facto usage (e.g. UNIX and TCP/IP).

Application Creation Environment: The market environment is leading to increases in product complexity, compressed product life cycles, and the need to get closer to customers and offer solutions rather than products. To meet these challenges the distinction between Information Service Provider and Information Infrastructure Provider is emerging, with the Information Infrastructure provider viewing the infrastructure as a platform that offers well defined capability to internal or third-party service providers.

Within this market structure the Application Creation Environment is a facility where an Information Service Provider, its customers and its partners can collaboratively develop applications for rapid delivery on one or more Information Infrastructures. This is enabled through the ready access to correctly skilled commercial and technical people, application creation tools, reference platforms and reference networks.

Broadband: Networks offering services at bit rates of 2 Mbit/s and above (not just ATM-based networks).

Content Capture/Loading: The content capture/loading is the process which enables a Service Provider to obtain material or content from a Content Provider, and to load it into the Service Provider domain (usual onto a server, or set of servers) and so enable the material to be access by the relevant targeted end customers/users.

Distributed Processing Environment: A distributed processing environment (DPE) is a collection of autonomous computers interconnected through a communication network. These computers do not share common memory. Information exchange between them is achieved using messages over the network. Middleware facilitates this messaging.

Interworking and Interoperability (SRC6):

Interoperability is required whenever the basic standards used on one side of an interface are different to those used on the other side. This will occur for many reasons and cannot be directly controlled by any practical means including standardisation, commercial pressure, or even regulatory pressure. Indeed, these pressures are more likely to result in a limited set of standards which support any one function which reflect technological development, competitive differentiation, and different interpretation and implementation of standards by organisations. In

addition, interoperability is not simply a technical problem, as it often involves issues related to the way different players provide service, purchase equipment, and even the way they are regulated. All of these factors come to bear as extra issues complicating the different types of technical interoperable interfaces.

Interworking across an interface allows the interface to be fully transparent on each side of the interface. This means that the user on one side of the interface believes that the user on the other side of the interface is part of his own network and vice versa. Interworking is fully transparent, fully symmetric peer-to-peer interoperability. For example, there is full interworking of voice telephony between PSTN and ISDN networks.

Naming, Numbering and Addressing:

A network *number* is a unique identification of an endpoint of a public telecommunications network which is used by the transport and control platform for routing across the network.

A network *address* is a unique identification of an endpoint of a communications network. Such an address may consist of a number and additional sub-addressing information to determine the destination from the set of destinations that are reachable beyond the public network.

A *name* is a user friendly means of identifying a user or resource within a system that is involved in communications. Examples of names include Universal Resource Locators (URLs) on the World Wide Web.

Navigation and Indexing:

Navigation refers to the processes and services associated with resource discovery (looking for products, services, information etc.).

Indexing refers to the processes and services associated with creating a database of references to the resources.

Security (ETSI STAG)

Authentication may be for the communication parties and/or the source of data. Accordingly, two different authentication features can be distinguished:

- peer entity authentication: the corroboration that a peer entity in an association is the one claimed;
- data origin authentication: the corroboration that the source of data received is as claimed.

Data *Confidentiality* provides that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data *Integrity* provides for the property that data has not been altered or destroyed in an unauthorised manner.

Access Control provides for the prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner.

Key Management provides for the generation, storage, distribution, deletion, archiving and application of keys in accordance with security policy.

Non-Repudiation provides for a proof of the sending or delivery of data by communicating IT assemblies which prevents subsequent false denials by a recipient.

Security Management is the subject of a dedicated ETSI work item leading to a TCR-TR: DTR/NA-002602.

Trust Services provide the essential means to secure message transactions in an open and non-discriminatory way between co-operating parties who do not otherwise have a trusted relationship. This includes private individuals as well as business, commerce and national administration.

A *Trusted Third Party (TTP)* is security authority or its agent trusted by other entities with respect to security related activities. In particular, a trusted third party is trusted by a claimant and/or a verifier for the purposes of authentication.

Trading: The trading service (the service provided by one or more traders) supports the flexible configuration of distributed applications through the late binding of the application components. The trading service enables client components to identify server components dynamically by referring to the type of service required rather than by some pre-defined (i.e. programmed) name. A distributed application must be flexible enough to configure and reconfigure itself in order to minimise the effects of partial network and system failures, and to support administration functions such as load-balancing. Dynamic configuration is a fundamental premise in the design of distributed applications and hence the trading service is seen as a fundamental service in distributed processing environments.