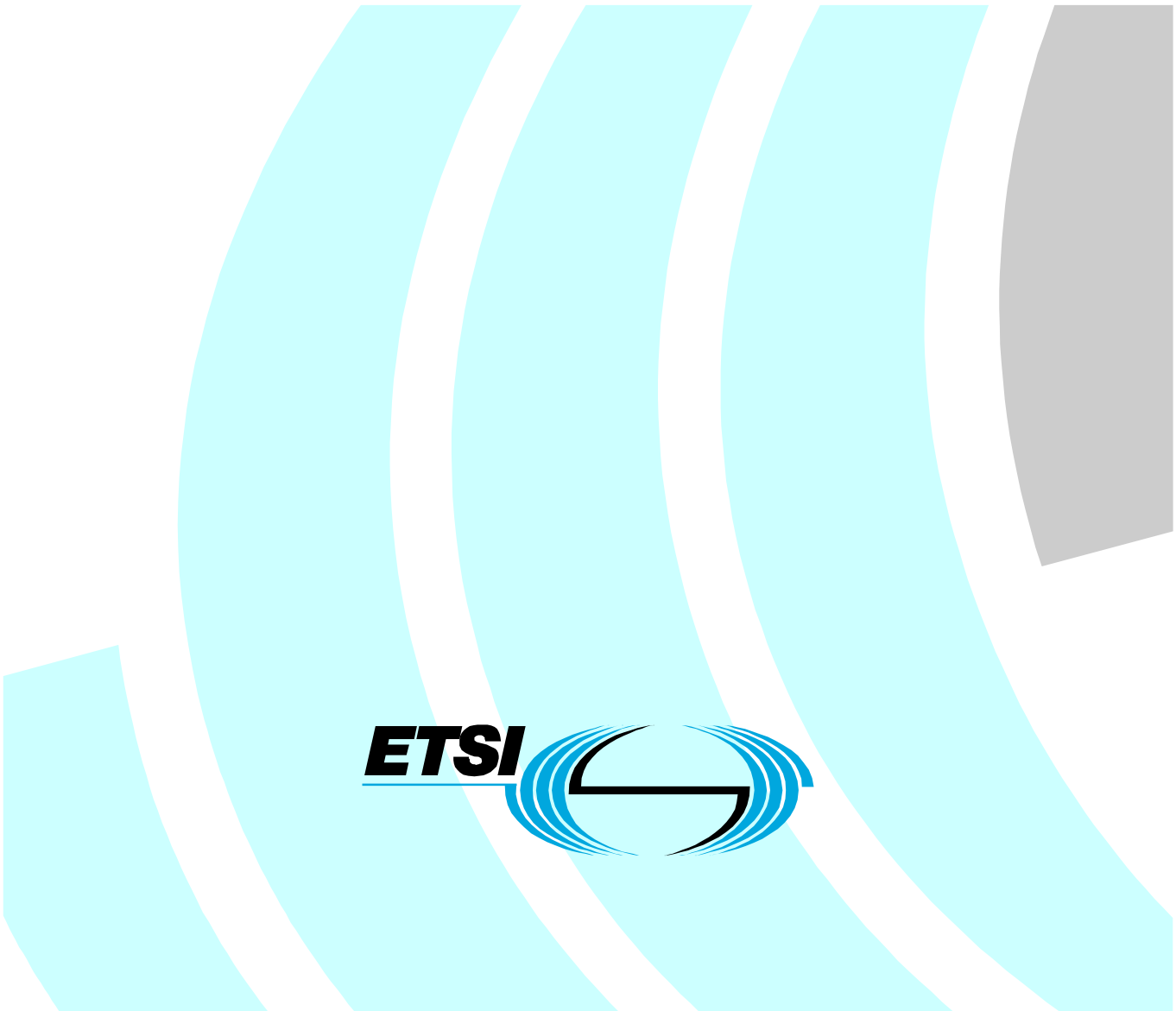
Final draft ETSI EG 201 936 V1.1.1 (2002-01)

ETSI Guide

Services and Protocols for Advanced Networks (SPAN); Interworking; IP Federating Network (IPFN) architecture



Reference
DEG/SPAN-140104

Keywords
interworking, IP, gateway, service

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Guide (EG) has been produced by ETSI Technical Committee Services and Protocols for Advanced Networks (SPAN), and is now submitted for the ETSI standards Membership Approval Procedure.

Introduction

The present document deals with the IP Federating Network (IPFN), an intelligent open interworking platform utilizing IP technology, allowing interconnection of existing and future networks. The networks interconnected may be fixed or mobile, 2G or 3G, IP or non-IP, public or private. The IPFN is composed of a set of functional subsystems, enabling users and applications of these networks to interoperate in fixed and mobile environments, and allowing for provision of value added services. From the users requirements and scenarios, a functional model is established, an architecture is defined based on the harmonization and evolution of existing architectures, reference points are identified, so as to list the existing protocols, identify the need for any protocol extensions and interworking specifications.

Levels of internetworking are defined depending of the Services offered like Security, Quality of Service, Supplementary Services and Data facilities.

Data may be exchanged, collected or shared between users.

New Services like global addressing, internetwork broadcast, multileg communications, etc, which are not yet available on the actual network to which the user is connected, may be offered.

Security will be an intrinsic capability of the architecture.

From this a set of recommendations is made in annex B, in order to help identifying the work in the different areas.

1 Scope

The present document identifies the services requirements from the users perspective. It then defines the functions necessary for interoperability required to establish an "IP Federating Network (IPFN)". It identifies the architecture and the reference points that are sufficient to meet the user's requirements in order to:

- allow Voice, Video and Data or combination of this (Multimedia) interworking between users on heterogeneous interconnected Networks;
- allow users to roam between networks, i.e. to allow the users to change network point of attachment;
- ensure secured communication when required by the users;
- maintain all or some Services (Supplementary Services, Data facilities, etc.) to the users;
- offer new Services like global name/addressing, internetwork broadcast, multileg communications, etc. which are not yet available on the actual network to which the user is connected;
- ensure lossless Data exchange between users of different Networks and between Databases, if required;
- provide extended addressing and naming capabilities;
- allow desirable feature interaction between applications that interwork across different networks;
- offer scalability of network interconnection;
- ensure some corresponding levels of Priority, Quality of Service;
- provide necessary network and service management capabilities for all of the above.

The present document aims to provide an analysis of the status of the subject, make recommendations for future work.

The objective is not to redefine existing standards when they can be reused (see note), but in a global analysis to review standards applicable, their limitations and the rules for implementing interoperability. For example a list of candidate protocols are SIP for interworking between gateways, Mobile IP, LDAP, IPSec, HTTP, XML.

NOTE: The standards referred to here are developed by ETSI, WWRF, IETF, IPv6 Forum and W3C, details of which are available in the Bibliography (annex C).

Levels of interworking will be investigated when appropriate in the context of the IPFN.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] IST 2000-28345 EGERIS: "European Generic Emergency Response Information System".

[2] ETSI TS 101 314: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Network architecture and reference configurations; TIPHON Release 2".

[3] ITU-T Recommendation F.16: "Global virtual network service".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

IP Federating Network: intelligent, open interworking platform utilizing IP technology, allowing interconnection of any kind of existing and future networks

user: any entity that actually uses a service. Examples of users in the context of the present document are as follows:

public users;

regulators;

services providers;

emergency authorities;

corporate users;

utilities;

agents/applications.

interworking: ability of equipments to communicate together from different systems and with similar services

interoperability: ability of equipments from different manufacturers (or different systems) to communicate together on the same infrastructure (same system), or on another while roaming

location based services: specific services offered depending of the user geographical location like mapping services, points of interest, routing services

portability: ability of an entity or element to be used in different systems or environments

roaming: process of changing the network access point from one location area network or domain to another within one system or between different systems

agent: application program that performs management operations in response to received management messages or that sends notifications

client: application program that sends request

gateway: interface, between two (or more) systems that have similar functions but dissimilar implementations, enabling users on one network to communicate with users on the other

proxy, proxy server: intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients

redirect server: server that accepts requests, maps the address into zero or more new addresses and returns the requests with the new addresses to the client

server: application program that accepts requests in order to service those requests and send back responses to those requests

user agent client: client application that initiates requests on behalf of a user

user agent server: server application that contacts the user when a request is received

user agent: application that contains both a user agent client and user agent server

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAA	Authentication, Authorisation and Accounting
API	Application Programming Interface
BICC	Bearer Independent Call Control
CLIP	Calling Line Identification Presentation (supplementary service)
DNS	Domain Name Server
EP	ETSI Project
GERAN	GSM EDGE Radio Access Network
GIS	Geographical Information System
GSM	Global System for Mobile communications
GVNS	Global Virtual Network Service
GW	GateWay
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
IIP	Intelligent Interworking Plane
IP	Internet Protocol
IPFN	IP Federating Network
IPSec	IP Security
ISP	Internet Service Provider
ISSI	Inter Sub System Interface
IST	Information Society Technologies
ISTAG	IST programme Advisory Group
ISUP	ISDN User Part
IT	Information Technology
ITEA	Information Technology for European Advancement
LAN	Local Area Network
LDAP	Light Directory Application Protocol
MCU	Media Conferencing Unit
MESA	Public Safety Partnership Project (Project MESA)
MG	Media Gateway
MGC	Media Gateway Controller
NAT	Network Address Translation
NSB	Network Service Broker
OSI	Open System Interconnection
PDA	Personal Digital Assistant
PIM	Presence and Immediate Messaging
PKI	Public Key Infrastructure
PMR	Private Mobile Radio
PSTN	Public Switched Telephone Network
PTN	Private Telecommunications Network
QoS	Quality of Service
RFC	Request For Comment
ROBO	Remote Office Branch Office
SG	Signalling Gateway
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMS	Short Message Service
SOHO	Small Office Home Office
UMTS	Universal Mobile Telecommunications System
URL	User Requirements Language
UTRAN	UMTS Terrestrial Radio Access Network
V+D	Voice plus Data
VHE	Virtual Home Environment
VoIP	Voice over IP
VPN	Virtual Private Network
WAP	Wide Area Paging
WLAN	wireless local area network
XML	X Modelling Language

4 Background information

It is a fact that wireless and wireline technologies are diverse with their specific adaptations to different markets. There is an increasing need to interconnect these public and private networks to provide Multimedia, not only a discrete Voice, Video and Data interworking, but also including global Name/addressing, Mobility, Value Added Services, Security.

IP based networks, by connecting functional subsystems, can federate those different wireless and wireline technologies for the users and for applications enabling implementations of new cross technology services and new business models between networks. These IP Core networks can use a common IP transport network for wireless and wireline subscribers and are independent from the access networks. Multiple access technologies should include: UTRAN, GERAN, Hiperlan2, etc. This will include wireline access in addition to the existing radio accesses, i.e. MESA.

Also, this convergence between wireline and wireless technologies should be seen as a key area of alignment, both at the network and service layers. It is important to derive common mobility requirements that could be adopted for wireless and fixed IP technologies, based on the study and review of mobility solutions of already evolving mobile networks (i.e. the R4 release and beyond) and fixed networks (e.g. WLAN networks).

This is actually needed to identify: mobility, security, multimedia call control and service control requirements before progressing the work on harmonized networks solutions for IPFN. It is also needed to ensure true seamless roaming and efficiency between wireless and fixed technologies. This includes the concept of VHE that has been developed in different fora.

The overall objective of the IPFN is to provide an interworking architecture (with harmonized facilities) for the support of Voice, Video, Data and any combination resulting applications (i.e. Multimedia). However, it is important to note here, that interworking with many different types of legacy networks and access systems is very complex. Therefore, interworking schemes shall be harmonized to as great extent as possible, and where possible avoided.

No assumptions about the physical architecture of the connected networks will be made during the study. Nevertheless, allocation of resources and functionalities may be required as is feasible in the connected network.

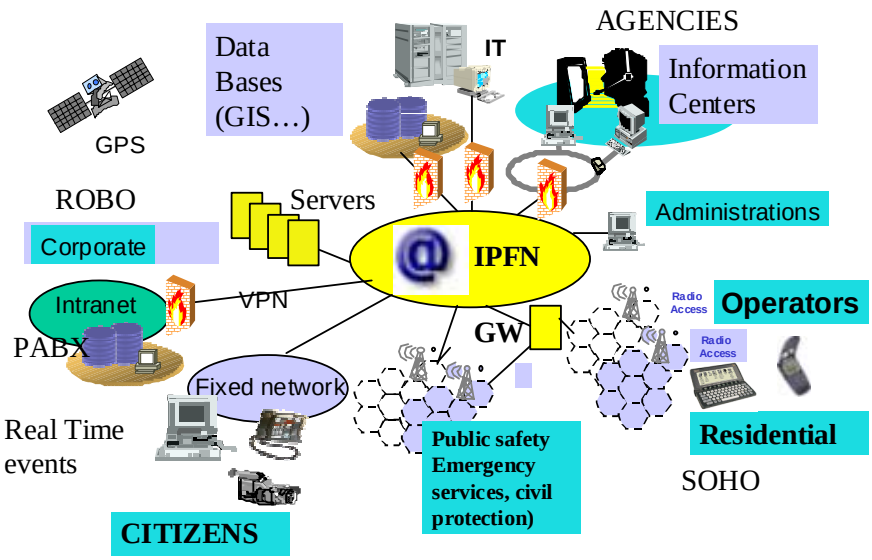


Figure 1: Global configuration

5 Users requirements

5.1 Market requirements

The market requirements taken here are those given by the EC from their global analysis and ongoing projects with industrials and users in the **Information Society Technologies programme** (IST), **Ten Telecom** business program and

Information Technology for European Advancement (ITEA) programme. Some extracts of such reports are listed below:

IST new organizations and markets (EC Directorate- General):

> "Smart organization is knowledge driven, adaptable and **internetworked**"…"IST enables public agencies to make the delivery of public services more citizen centric"…

Referring to the IST Information Society Technologies programme (2000 workprogram-/2000/350):

> "the emphasis is on citizen-centred approach with significant support for standardization, **interoperability** and market stimulation"…"disseminate information"…"users will be able to access data with **ubiquity**"… (Intelligent environment management).
>
> "Effective collaboration requires standardization, concerning how the data is collected and stored, and **interoperability** in the solutions applied". (Health services).

Draft synopsis of 2001 program ISTAG key enabling technologies:

> "To develop middleware, distributed systems, multi-layered architectures and agent based systems to enable **interoperability, interworking**, openness and integration of applications and services across platforms"…"To emphasize trust and **security** "…

Trans European Telecommunications Networks (2000/C299) in its business plans and market validations quotes the need to "help improving the overall accessibility to the Services and to ensure that customers of equivalent services from different providers can communicate and **work together** transparently"…

Information Technology for European Advancement technology roadmap on Software Intensive Systems (Ref 29 9 2000) reports "we are confronted with a conglomerate of networks which, from the perspective of users, should work seamlessly together"…And in 2001 IST work program "develop middleware, distributed systems, multi-layered architectures and agent based systems to enable interoperability, **interworking**, openness and integration of applications and services across platforms"…

The EC has also issued a draft mandate on a standard interface between PTN operators and emergency services support centre for the automatic localization of the distressed caller.

Several European projects are launched with new projects like EGERIS [1] involving the IPFN, VESPER, WINEGLASS, and LOCUS, etc.

Going further (DG INFO/E4) one can consider an **Open Interworking Platform** which is an independent middleware for a wide range of terminals and applications, enabling services, user to user, independently of the underlying network.

Such an ultimate architecture can lead to new business models with 'Network Service Brokers' (NSB) ensuring a unified security platform, control mechanisms, location mechanisms, etc.

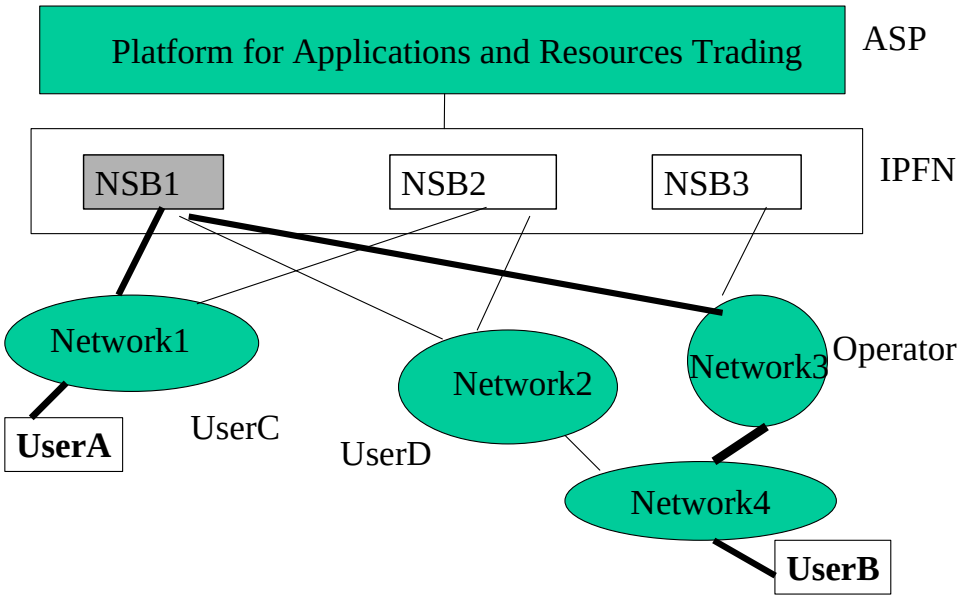


Figure 2: Possible future business model

5.2 Users requirements

Due to the multiple types of networks and protocols available today, there is a need to allow Voice and Data interworking between users, applications on different networks public and private, fixed and mobile. Roaming may also be possible in case of same standard based networks, multimode and multi-frequency terminals, etc.

Interworking requires being able to eventually control the information exchanged, its access according to different policies and procedures, to be able to collect it from different data bases on different networks, to be able to handle different formats.

Interworking requires offering the user same/subset/similar Services including Priority, Security, at least the user shall be aware of it, in case the services are downgraded.

Users requirements are being set up in the EGERIS project [1].

6 Operational scenarios

The scenarios chosen shall reflect user cases of interworking, including a mix of different types like public and private, public and corporate users.

6.1 Scenario 1 - Environmental crisis situation

In this scenario a major environment crisis is detected on an industrial site, citizens have to be warned locally, emergency services have to intervene on site, coordination is ensured by the local regional administration, environmental agencies provide information, etc.

The scenario corresponds to the interworking of different types of Users for Voice and Data Information, as represented on figure 3 in a scenario:

- citizens using public networks, fixed or mobile like PSTN, GSM, UMTS;
- operators and ISPs of the fixed or mobile public or/and private networks;
- emergency Services, civil protection using fixed and mobile networks and their Information Centres;
- administrations taking decisions in crisis situations from the available Information;
- policy makers defining policies;
- IT Agencies (Like Environment, etc.) using different communications means and Information Centres (IT users);
- corporate users;
- tiers for example for certificates in secured communications.

These users exchange Voice and Data (forms, images, video, etc.) information between themselves, according to different policies, formats, languages, etc, and according to different Procedures related to the location, region, country.

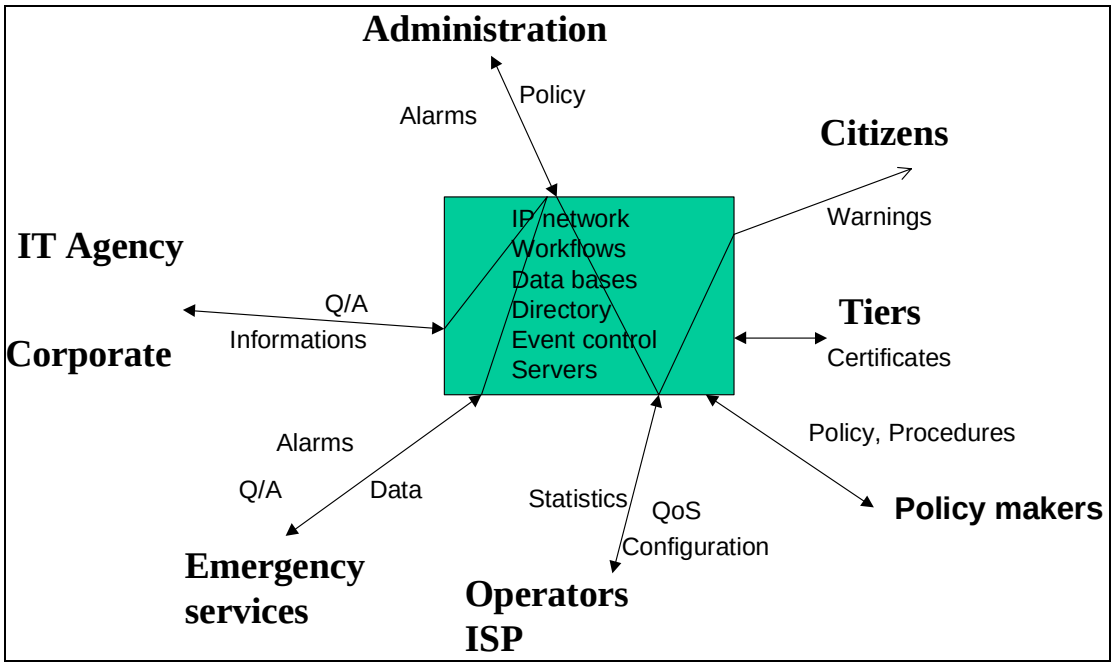


Figure 3: Users involved in scenario 1

Figure 4 represents the different functional sub-systems involved for such interworking, which can be optional and which can be split in different planes:

- heterogeneous terminals plane with the users and applications;
- heterogeneous access and core networks plane;
- Intelligent Interworking Plane (IIP) with, for example, the following functions:
  - call control function for GW s interworking;
  - multi legs set-up functions;
  - security functions;
  - directory functions;
  - DNS functions;
  - location functions;
  - translation/transformation/intermediation functions;
  - value added services like broadcast.
- IP backbone with a 'bit pipe' transport and routing main functions, public or private;
- application servers plane with Web servers, GIS, etc.

The IPFN is the Interworking plane corresponding to an **Open Interworking Platform**. The IPFN is composed of an IP core network with its Inter Sub System Interface (ISSI) to the Intelligent Interworking Plane (IIP).

Some of these functional sub-systems are optional, they can also be merged between themselves, they have been split here only for the purpose of the scenario.

Heterogeneity of information format, type, etc. of the associated policies and procedures, of the data rates, priorities, of the types of Terminals, of the Services offered, etc. is dealt partially or totally by the interworking 'middleware'.

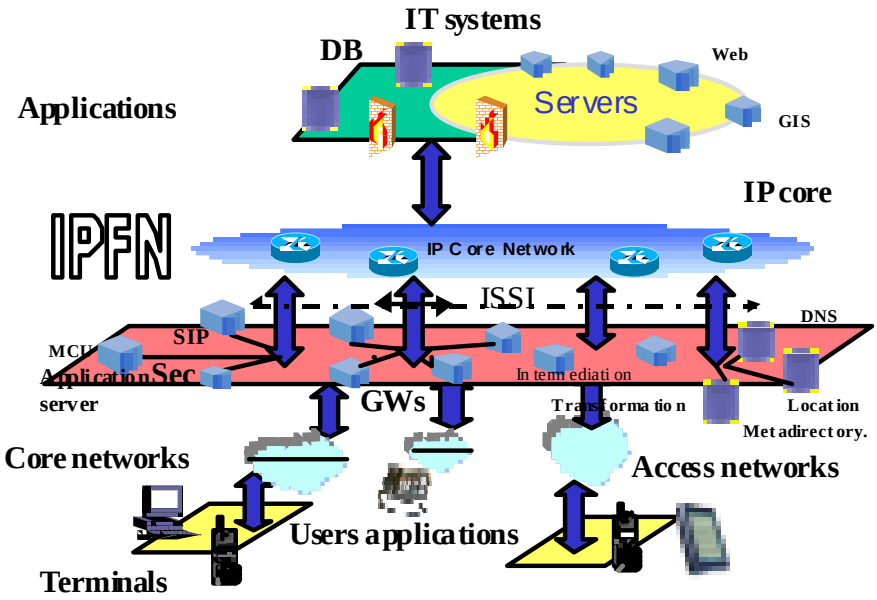


Figure 4: IPFN plane

6.2 Scenario 2 - Multileg call

This scenario presents a possible example of multileg call application involving voice communication, catalogue consultation, and secured payment. In this scenario a user wants to purchase an airline ticket in a foreign country, being away from his home network, this may involve different operations like:

- consultation, remotely via his mobile of his corporate agenda;
- consultation via his mobile of the airline timetable;
- simultaneous contact with vendor to get information while checking timetable;
- purchase of ticket with secured payment;
- update agenda;
- call home.

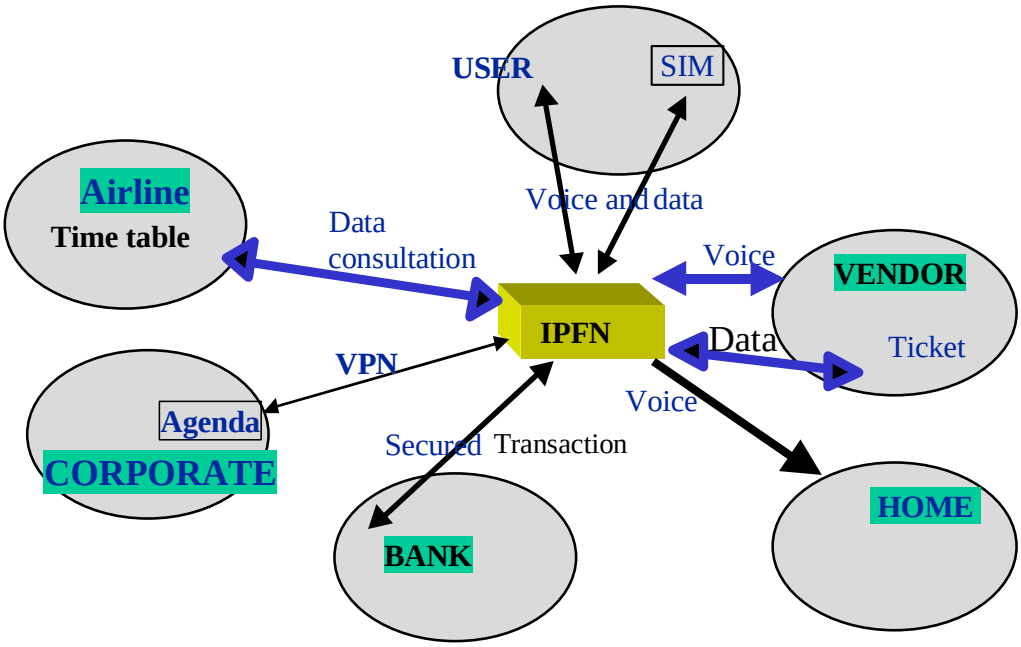


Figure 5: Multileg call scenario

6.3 Scenario 3 - Corporate application

This scenario is a possible example of a corporate application.

This is the case of a Corporate extending its offices with a new site, following a merger. Each site has its own wireless and fixed communications systems and addressing. To avoid major changes in the extensions of the corporate site, the IPFN may interconnect the networks to provide the functions in order to allow communication between sites. The same applies to a ROBO connected or added.

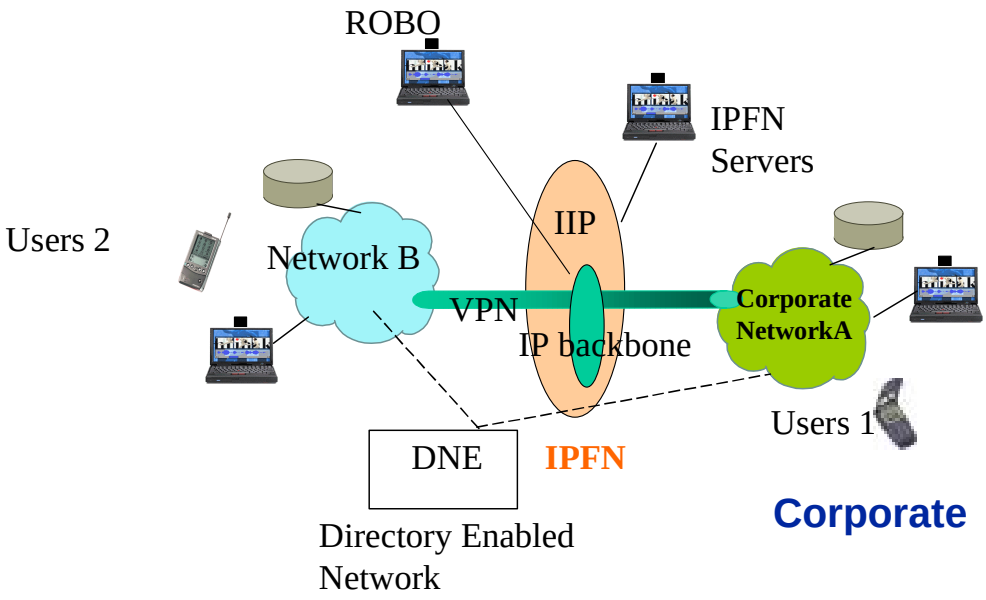


Figure 6: Corporate scenario

Employees on site B are connected now through the IP backbone/IIP to corporate network A. Interworking is setup between sites.

The IIP functions of the IPFN provide services to the corporate network VPN service under a Service Level Agreement (SLA) with the VPN providers. These services may include Security negotiation, the application of an encryption mechanism, transcoding between schemes used, performance management, QoS negotiation, name/address translation, user registration and collecting information for charging purposes. These services may be distributed or centralized, for example the functionalities of the IPFN may be owned by a variety of organizations and maintained in dispersed discrete locations.

6.4 Scenario 4 – Secured transactions

This scenario involves an heterogeneity of terminals with mobility on a mix of networks and operators. The users involved in the scenario involve public customers, retailers, banks, tiers, trusted parties, etc. Different currencies, public keys handling, policies, certificates mechanisms, etc. make this scenario complex as shown on the figure.

The IPFN allows to keep heterogeneity while, by adding new functions (IIP) to the core IP network, it allows mobility and security.

One example is certificate handling where different protocols are available, a server on the IPFN can make the protocol conversion at the edge of the core backbone. Other examples concern currencies conversion, format handling, etc.

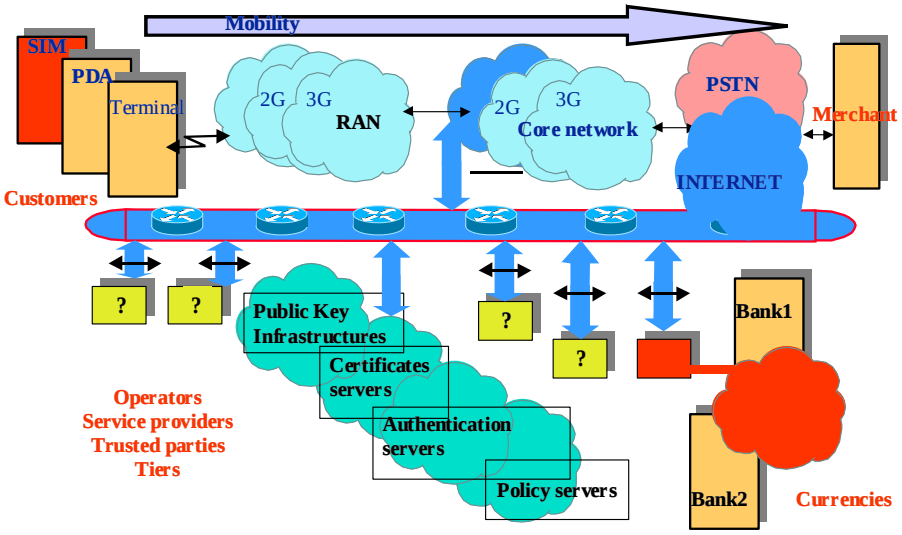


Figure 7: Secured transactions

According to events secured transactions are setup, the workflow is federated as well as the data exchange. Policy, authentication, certificates servers may be one or several servers connected to different types of networks as well as PKI.

7 Services offered

Interworking does not necessarily mean to offer all application and network services to the user as the ones he had on his home network. Some similar or equivalent services may be offered as a subset, in some cases new services can be added. Different levels of services can be defined such as for example:

Level 1: this includes the minimum mandatory interworking functions needed for Voice and Data communications; for example point to point voice communications, fax, SMS.

Level 2: a chosen limited set of Teleservices like multiparty voice and multimedia calls, a chosen set of Supplementary Services and Data facilities would be available on both ends.

Level 3: new services are offered to the user by the introduction of the IPFN. The value-added features can be for example: security, multi-leg, access control, mobility, and multicast.

Another point is the security level to the user in his home network that may have to be guaranteed for interworking.

7.1 Voice services

Voice services can be split into classical voice services and interactive multimedia voice services:

teleservices:

- individual call;
- multi leg calls;

supplementary services (e.g. call forwarding, etc.).

7.2 Data services

Data services and facilities shall be classified and the dimensioning of the information checked for data rate, priority, QoS and response time:

Classification can be done as:

- time dependant bi-directional services: Video conferencing, VoIP;
- real time short data services: Location services, Telemetry, Biodynamic;
- database access: online forms, data base access to video, image and multimedia;
- image transfer: image, video, video streaming, graphics, maps, webcast, video broadcast;
- office application: emails with attachments, web browsing, mobile computing;
- file transfer: file, content push.

7.3 Mobility services

The mobility services are set up in order to know on which access network the user is located and in order to track his mobility from one network to another they comprise:

- user registration;
- user location;
- user profile management;
- user policy management (service subscription);
- policy negotiation and the reservation of capabilities offered by the access network;
- user Authentication, Authorization and Accounting (AAA).

There may also be the possibility to control the interoperability and services offered.

7.4 Priority services

Different levels of priority may be defined according to the priority level users need to have. These priority levels may be assigned in the user profile in their home network.

This includes the automatic allocation of a priority level for emergency services, and the provision of essential data for the automatic location of the distressed caller. This feature is supported by the allocation of a priority indication to session control signalling.

7.5 Data management

Some data may need to be stored on the IPFN as for example:

- network location information of a user roaming;
- user information of a user roaming, etc. (Naming/addressing, Security, Priority, QoS policy, etc.);
- main characteristics of a connected network (Network Virtual image) like:

  maximum data rate, types of coding, types of compression, services offered, etc.

Some of this information may be obtained by interrogating the interconnected network databases.

7.6 Security features

Security services should have different levels corresponding to different services offered as:

- authentication;
- confidentiality (end to end);
- integrity and authenticity;
- availability and non repudiation;
- digital signature and certificates;
- key management, secret and public.

NAT, firewalls traversal, VPNs, IPSec and lawful interception are to be considered.

7.7 Application server services

These services allow from a request of a user/application on one network to collect and assemble the information on the different network databases, e.g. using LDAP services.

7.8 Translation service

Data may be translated/reformatted before being sent to the user. It is a data interoperability function in order to have the possibility to have XML internal standard format. This could include voice services translation.

7.9 Administration

Administration of the IPFN covers network management.

7.10 Presence services

Presence based multimodal communications should be considered by the IPFN.

7.11 Messaging services

(Instant) messaging should be considered by the IPFN.

7.12 Location based services

The IPFN should consider access to location information by emergency services and services offered to the user depending of his geographical location.

7.13 Directory services

The IPFN should support various addressing plans related to unit, multileg, networks configurations.

7.14 Compression features

The IPFN should support compression of IP datagram headers, signalling messages and payload data, as appropriate.

7.15 Value added services

These services include optional services that are offered to the user to handle: the invocation of a service according to an event, the management of information according to events or procedures.

7.16 Interworking features and capabilities

These capabilities include optional features that are offered to the user to handle: the heterogeneity of terminals, the heterogeneity of data formats, etc. The user may not be aware of these capabilities.

8 Functional model

The functional model can be split into mandatory and optional functions. Some of these functions can then be classified into intelligent functions in the IIP.

Figure 8 represents an example of such decomposition with the core IP backbone (and eventually VPN) with a function of (secured) 'bit pipe', in a multidomain environment, with mandatory and optional edge functions, and the optional Intelligent IP functions. SIP is assumed for interworking between users A, B, C.

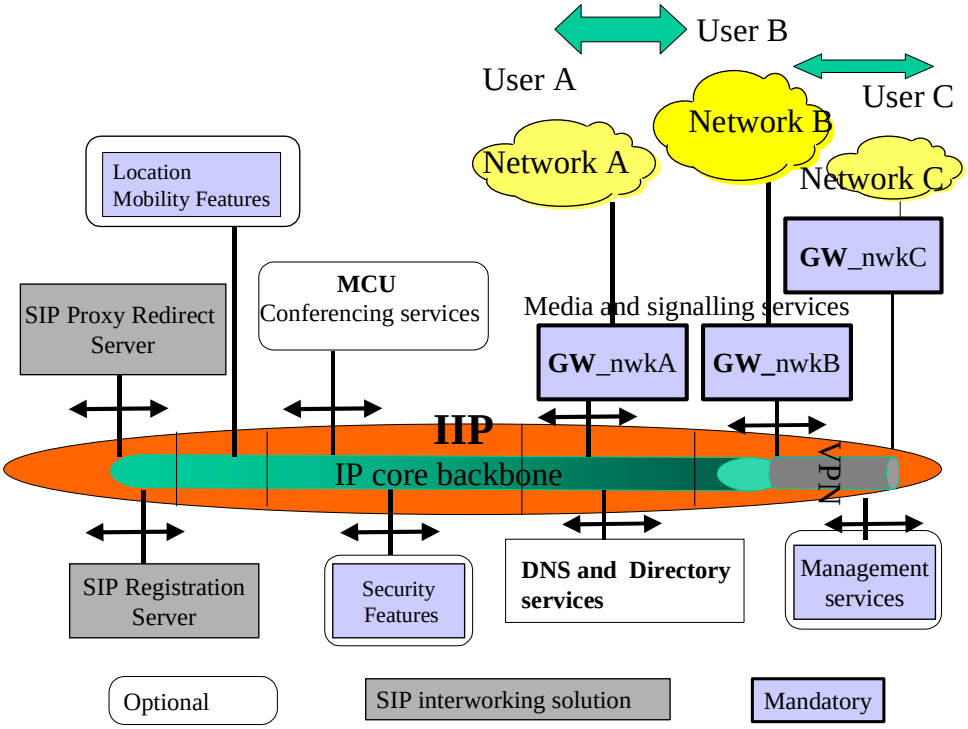


Figure 8: IPFN functional architecture example

8.1 Mandatory functions

The following functions are mandatory:

- GateWay (GW) functions with media and call control VoIP interworking functions. The Signalling and Call Control Gateways may include candidate protocols for interworking, such as: SIP (The Proxy Redirect server, Registration server functions are assumed SIP (Session Initiation Protocol) based sub-systems), SIP-T (Tunnelling ISUP), BICC, H.225.0, Q.931. The Meta protocol developed in project TIPHON can be used, it avoids making any assumption on the protocol used and may then be mapped to the real protocol in use between gateways. In case of H.248 (IETF Megaco) a Media Gateway Control (MGC) function is needed that controls Media Gateways (MG). This MGC can be common to various Media Gateways.
- Location register function offering mobility management capabilities;
- security function offering security capabilities for example the security function is required for the support of Reliable Identification, non-repudiation, etc;
- management function: minimal support;
- naming/addressing function offering DNS and directory services.

8.2 Optional functions

The following functions are optional:

- security function offering security features for example the security function may be required for the support of a Global VPN service (GVNS [3]);
- Media Conferencing Unit (MCU) function offering multi-leg services;
- management function: e.g. QoS, end to end services;
- intelligent IP functions.

8.3 The Intelligent Interworking Plane (IIP) functions

The Intelligent Interworking functions (IIP) include the optional functions described as follows:

The mediation function: is an intelligent layer which manages the heterogeneity of terminals with mobile terminals, fixed PCs, PDAs, low capability terminals (e.g. Set Top Box/TV), LAN or remote access to network based terminal profiles. This does not define the location of the user/terminal profile. This function is expected to be mandatory.

The converter function is an Intelligent layer which manages the different formats of data representation, typically it can be the (V) XML model with its related standards for transforming the data formats, and language transformations, used in the respective systems. It may support a unique internal language. This function is expected to be mandatory.

The triggering function is an intelligent layer that allows invocation a service according to an event.

The service transformation function: is an intelligent layer which supports the transformation of a service into a value added service, according to specific rules agreed in the Service Level Agreement (SLA). For example the transformation of the CLIP service into a Calling Name Address Presentation service (CNAP).

The service builder function is an intelligent layer that allows building of a service from services capabilities. This may include services capabilities as defined in EP TIPHON (see bibliography).

The event and procedure function: is an intelligent layer that allows the management of information according to defined events and e-procedures. This involves federating data from different databases to be pushed, as defined in "Push" services. As an example, the e-procedure can be location dependent.

From this a functional model is derived as represented in figure 10, these functions may be physically located at the edge the Intelligent IP, in Servers.

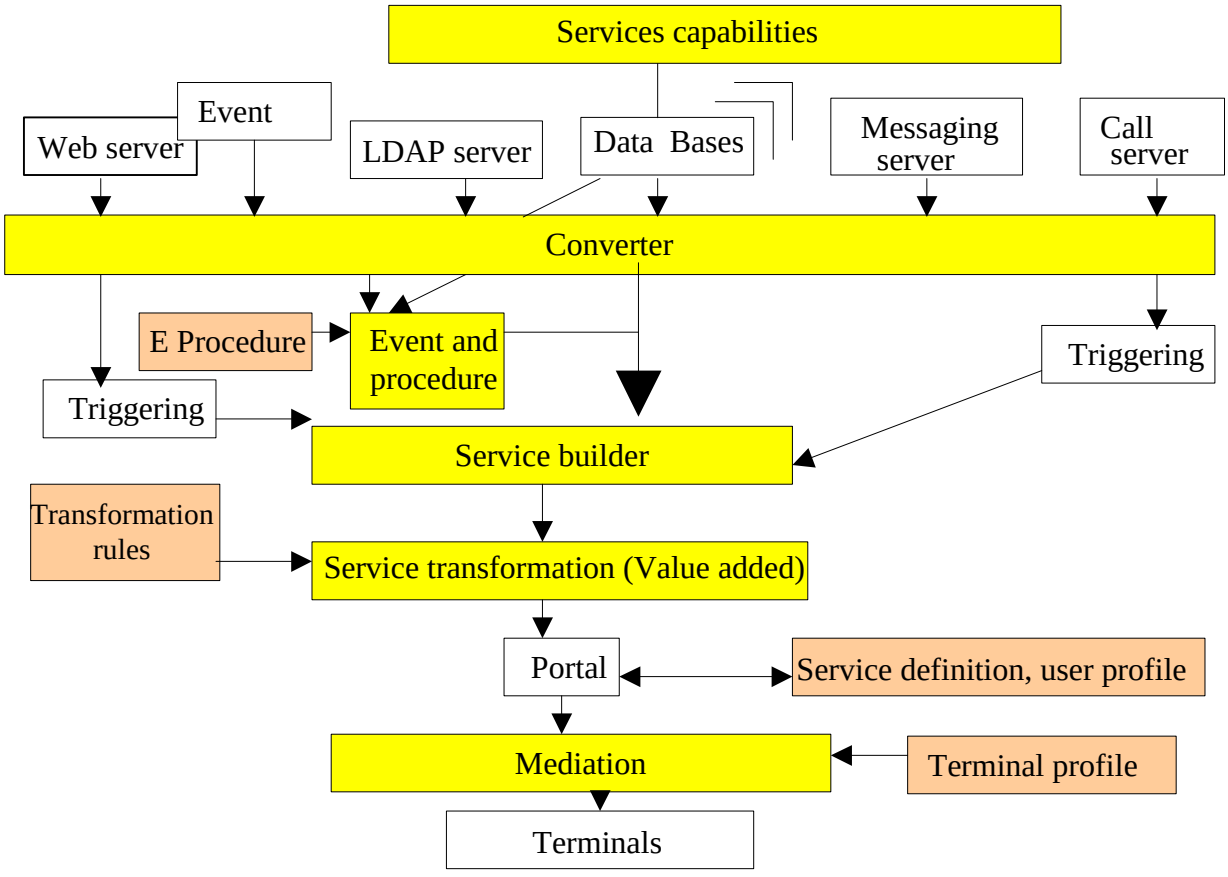


Figure 9: Intelligent IP functional layer

8.4 Recommendations

The following recommendations are made:

Recommendation 8.1: Interworking is provided with the candidate protocols within the IPFN.

Recommendation 8.2: The interfaces between IP to the different functional subsystems shall be open and standardized and reuse of existing IP based standard suites.

Recommendation 8.3: Scalability, though potentially being better addressed by a decentralized architecture, should be a primary concern.

Recommendation 8.4: The IPFN shall support the location Registration and Mobility Features Services.

Recommendation 8.5: The IPFN shall support Emergency and other Essential Services, including the required priority capabilities and the secure transfer of required user data.

Recommendation 8.65: The IPFN shall support optional Security features.

Recommendation 8.76: The IPFN shall support optional QoS features including priority.

9 Levels of interworking

9.1 Levels

In order to offer interworking it is not possible to offer all possible functions to interwork, except eventually in case of multimode, multiband or same standards systems. Levels of interworking are proposed to be defined which may be set up dynamically, negotiated or static.

Level 1 of interworking would include a Media Gateway, a Signalling Gateway and a DNS subsystems for point to point voice communication plus SMS and Fax:

Gateways include Media interworking functions and Signalling interworking functions. For instance, Media Gateways (MGs) will convert media formats from the radio/cordless access part to the IP network and vice-versa. In a similar manner, MGs are needed between the IPFN and external networks. At the same tine, Signalling Gateways (SG) will be providing the signalling interworking from/to wired/wireless access to/from MGC and for the interconnection towards external networks.

The Directory function will support legacy X.500 directory systems and new LDAP directory systems, it may also contain information on new services offered, to the interconnected Networks. The architecture concept is similar to DNS (Domain Name Server) with a hierarchy, which provides for federation with billing, services information. Naming and naming/addressing rules have to be set up and agreed. It shall include also information to handle mobility for internetwork roaming. It may contain information on the services of the roaming users for mapping purpose, obtained by request to the network databases. The Gateways and the Management sub system can access it. Global @dressing is offered through IP global @dressing v4 or v6.

Level 2 would require adding a limited set of teleservices like multiparty voice and multimedia calls, a chosen set of Supplementary services and Data services, the MCU, Directory access and Management functions:

The Media Conferencing Unit (MCU) function will allow, for example, interconnection of several call legs to different endpoints to make multi party voice, data or multimedia communications.

The Management function may control the management of the subsystems of the IPFN for example to ensure end to end QoS is the same or similar to the QoS of the user including priority, security. Charging functions as well as transfer of charging information has to be addressed.

The Policy Enforcement function may include:

1) selecting a network according to the quality asked by the user/application;

2) selecting a network according to the level of priority requested;

3) selecting a network according to the level of security requested;

4) getting or checking the QoS of a network connected.

It may require/check information on the services, QoS offered by the interconnected networks.

Level 3 would require adding the Security and Mobility management functions as value added services such as multicast, broadcast, etc.

The Security function allows handling of security features (e.g. Certificates, Security algorithms, etc.). Security may be offered through the use of standards like L2TP (layer 2 tunnelling protocol), IPSec (IP security). X.509 (OSI directory authentication framework) is to be considered.

The mobility management function is to:

- be split between the access network (micro mobility handling – mobility towards the air interface management without any control from the core network, i.e. soft handover) and the core network(macro mobility management – macro mobility triggers procedures in the core network to govern the movement of wireless terminals in the radio access part, i.e. hard handover). In any case each interconnected network (access and/or core) handles the mobility of its terminals/users. The IPFN is concerned about Network mobility in order to know in which network the terminal/user is;

- be supported by a location register function and enhanced MGC function in the core network;

- may take into account wireless terminal states (connected, idle or detached) and using of the paging mechanism;

- may provide seamless accesses to subscribers databases using protocol such as LDAP from the various entities in the IPFN (SIP servers, MGCs, etc.).

The following table gives a possible configuration of levels.

Table 1: Configuration levels

Interworking Service	Level 1	Level 2	Level 3
Point to point voice call	X	X	X
SMS	X	X	X
Directory function	X	X	X
Multileg call		X	X
Priority call		X	X
Broadcast			X

NOTE: Does this put requirements on the connected networks? For example does a connected network need to be able to push some information to the IPFN or to allow some data access?

9.2 Recommendations

The following recommendations are made:

Recommendation 9.1: Define interworking levels.

Recommendation 9.2: Introduce mechanisms to negotiate the interworking services or have equivalent tables.

Recommendation 9.3: Introduce mechanisms to route according to service, like QoS request, policy negotiation, and availability.

Recommendation 9.4: Introduce mechanisms to warn users of degradation or upgrade of service.

10 User profile structure and modelling for IPFN

This clause is focused on the architecture of the IPFN profile servers needed to store user data for mobility in fixed and mobile networks. The proposed approach extends the current IPFN concept with the use of a common profile server (from a logical point of view) to federate all the involved networks and provide a seamless roaming between different type of accesses (e.g. fixed & mobile). The provisioning of the core profile server is done by database management techniques.

The following functional database architecture can be proposed for the Core profile server of IPFN.

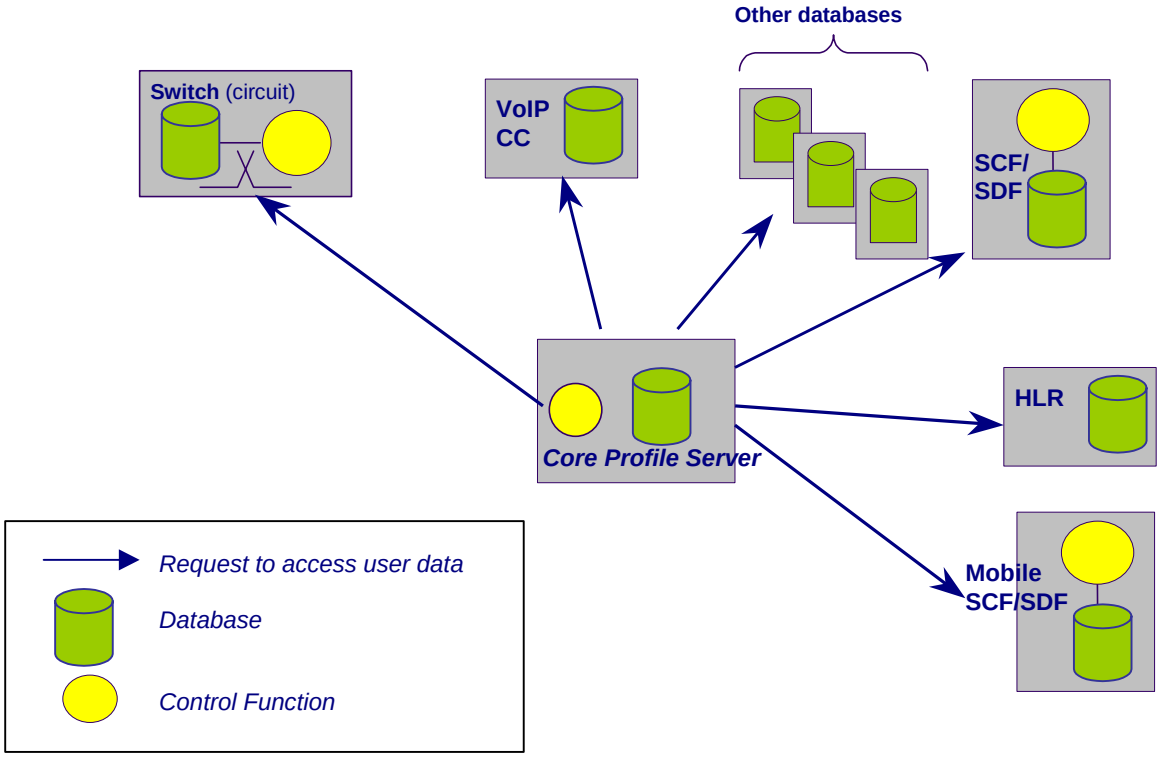


Figure 10: Proposed functional architecture of the core profile server

This core profile server can be accessed by client entities in fixed and mobile systems as indicated in figure 11.

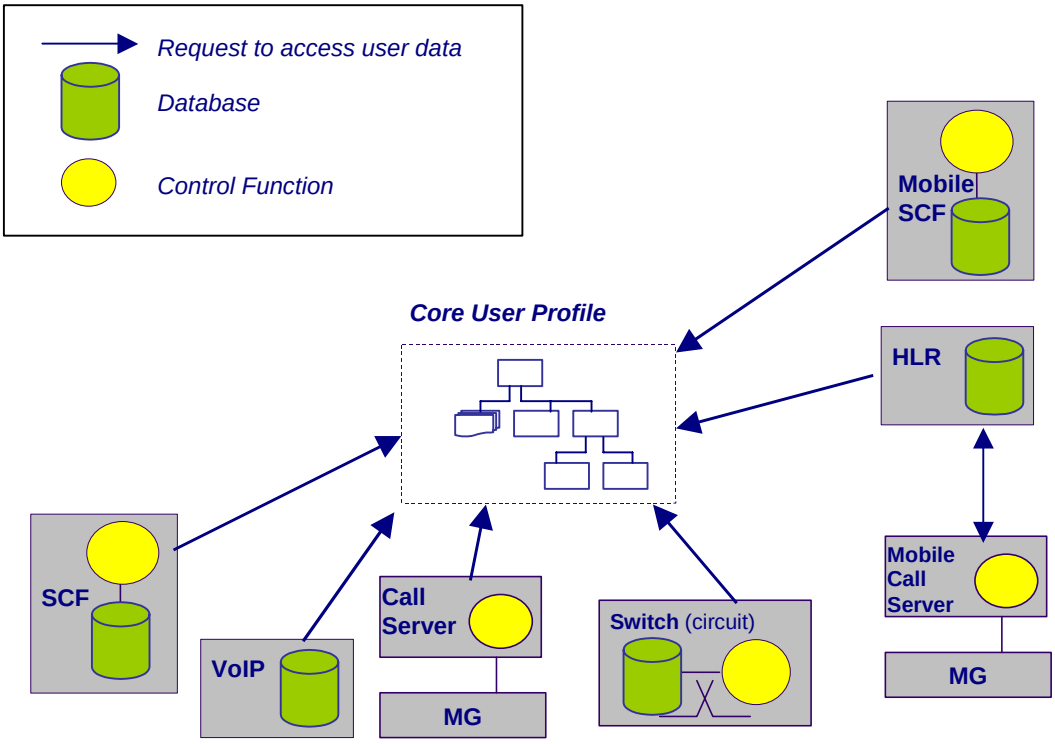


Figure 11: Accessing the core user profile

The core profile server includes the common needed user data, i.e. a first list would be:

- user identity, e.g. URL;
- other user identities for the user and their services (e.g. E.164 for circuits switched services, e-mail addresses, etc.), mapping the specific User Identity to a database as the Entity Address;
- authentication data (e.g. method, authentication centre identity) related to a service request and user identity;
- routeing addresses (e.g. E.164 for circuit based services, IP address(es), etc.);
- identity of local register for user profile copy in visited environment;
- service related data when these services can be delivered on various access technologies (e.g. call forwarding and voice mail, etc.).

Service related data may be only accessed by various clients network elements, and as they are implemented in various service platforms, we consider that user service data can be stored on a wide range of equipment. Therefore a limited set of user service data is to be made easily accessible: this may be limited to a pointer in the common core profile pointing to the whole set of user service data, stored in a service specific equipment.

Modelling of the role, content and behaviour of the Core Profile Server, address translation or rely point, requires further study.

In summary:

- the proposed database architecture provides a single logical user profile for mobility in and across fixed and mobile networks;
- this core user profile modelling encapsulates the specific data structures of each service profile (and its potential evolution) by providing a single database access point to client network entities;
- this architecture enables the easy introduction of new network entities, either as client or a user service profile server, without any impact on existing infrastructure. In a similar manner the evolution of one network entity has no impact on other equipment except the profile server.

11 Reference model

The basic reference point can be based on the TIPHON meta protocol model [2] mapped to the different protocols (SIP, etc.). Then new reference points have to be defined mainly at the service and service control level of the model. The following figures give one TIPHON reference model applicable, to be expanded to include the IPFN functions.

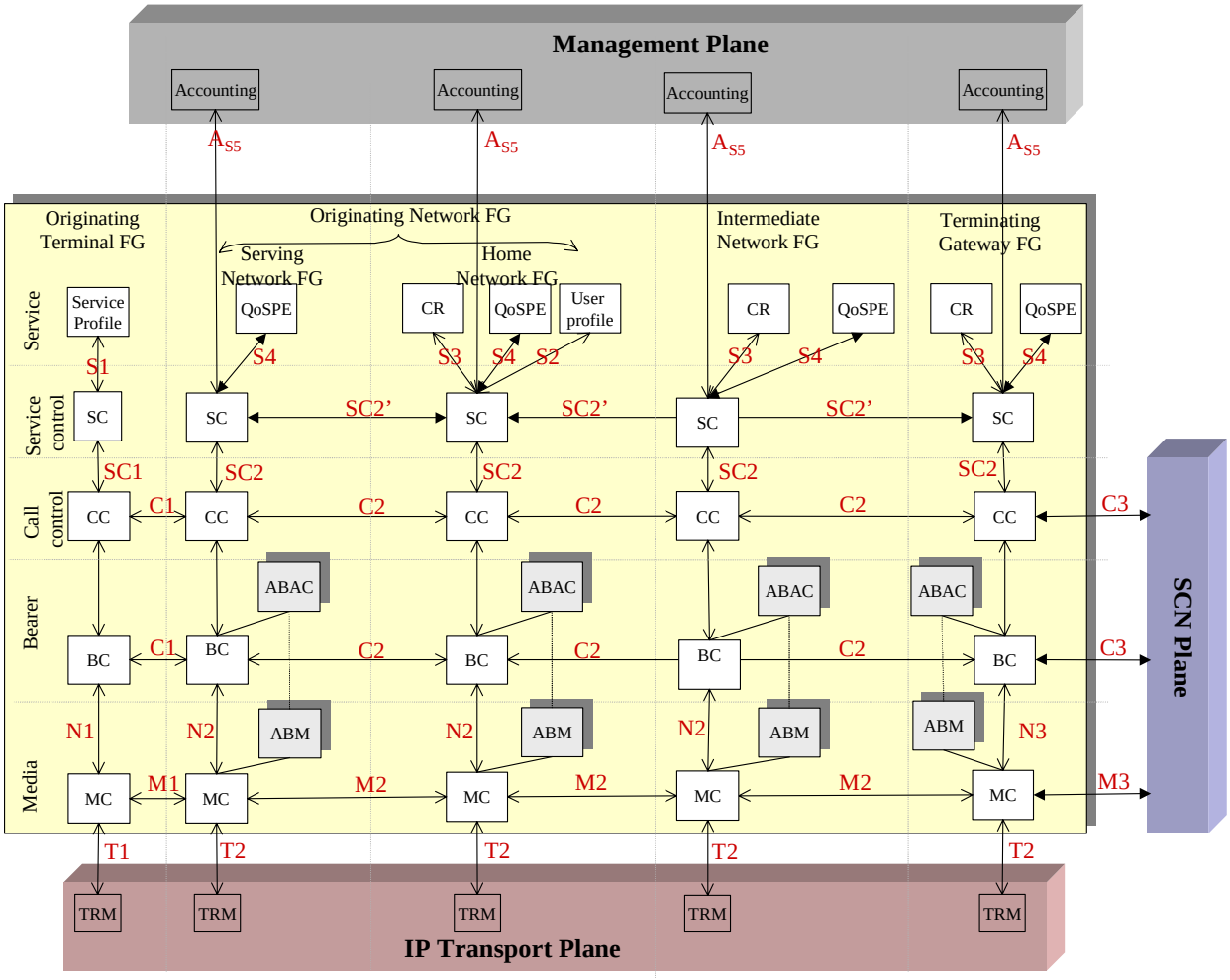


Figure 12: Basis of reference model

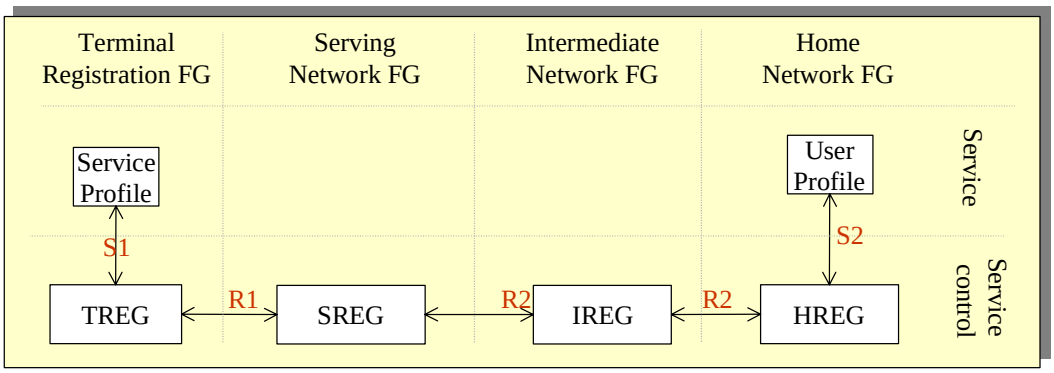


Figure 13: Reference model for registration

Both lists, quoted below, compare as follows:

Table 2: Mapping of ISSI reference points to TIPHON reference Points (Release 3)

ISSI functional domains	Observed TIPHON phase 3 reference points for IP network to IP network interworking	Open issues requiring extension to TIPHON phase3 reference points for IP network to IP network interworking proposed for TIPHON release 4
Call control Data services Directory services Mobility services Security features and capabilities Terminal management	C2 (call control) M2 (Media control) SC2' (user information) R2 (registration) T2 (transport network control)	C2, M2, T2 R2 Is this an extension of SC2', or embedded over the C1 reference point, within a session? Is this an extension of R2 outside of a session?

This mapping shows some areas are covered as defined and other areas that need to be covered in discussion.

Recommendation 11.1:

The convergence between TIPHON and the IPFN should rely on mapping the ISSI of the IPFN on to the TIPHON IP network to IP network reference points, defined in [2] (namely: M2, C2, T2, R2, SC2' reference points).

Recommendation 11.2:

Phase 4 of TIPHON includes numerous new features in its scope. In the scope of the IPFN, the following features are important in order to support corporate voice and data networks:

- Support of mobility from one network to the other:

  In case homogeneous networks are connected through the IPFN, roaming should be possible.

- Support of encryption across networks:

  Maintaining end-to-end encryption possibilities between networks connected through the IPFN requires specific exchange of information across ISSI this should be taken into account.

- Support of multi-leg communications with fast set-up times:

  Multi-leg communications may include telephony like conference calls, where participants join with a dial up operation, but also calls without dial up from participants, for example broadcast call from information centre to multiple predefined participants.

- Support of emergency services:

  Handling of emergency services includes the setting up calls with highest priority, and may include the sending out of call related information with the same priority (for example sending emergency advice to several information centres). User and location information shall also be included in this priority call set-up to the authorized emergency service centre.

- Integrated voice and data services:

  Support shall be provided not only for call-oriented services, but also for user to user data services (e.g. SMS, WAP and Fax.) and server to user data services, including mobility problems.

12 Data flows

The data flow is composed of:

- signalling information;
- user and application information.

Figure 14 shows a possible information flow between a real time application on a terminal, the information centres and the public networks.

Following a real time event an application on a terminal sets up a multi legs connection to different subsystems according to localization based procedures. Data is collected from a metadirectory application server and pushed to private information centres and public operators in order to warn the concerned citizens in a certain area.

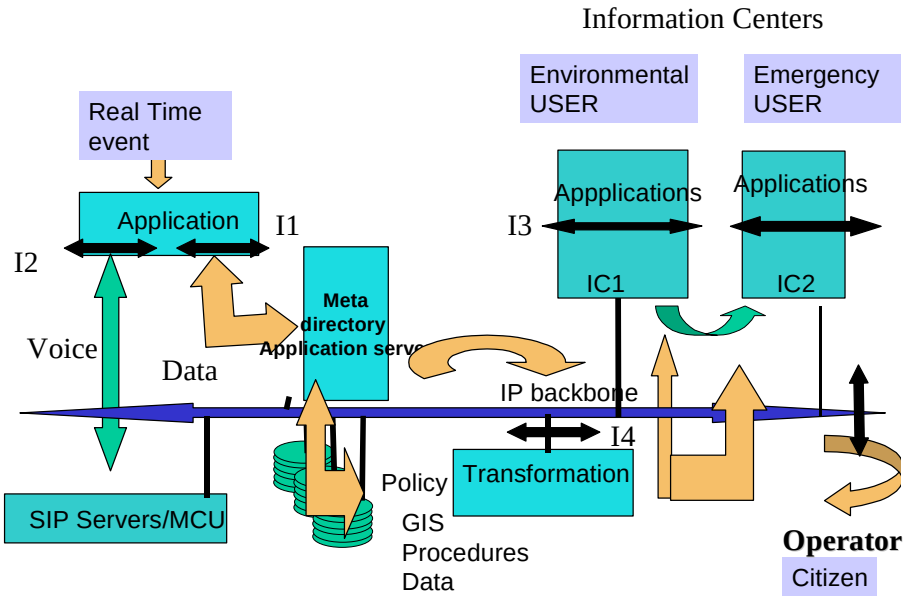


Figure 14: Data flow and interfaces

13 Existing protocols

This clause lists the protocols applicable and standard bodies/forum concerned.

The status of these protocols and their development is categorized as 'Status 1' as contributed material (Internet-drafts) or informational documentation (informational RFCs), 'Status 2' as Standardization in Progress or 'Status 3' as agreed material in approval or published standard. Most protocols belong to IETF unless specified.

Table 3: List of protocols

Function	Comment	Protocol	Status
Multicast	IETF: Group membership protocol	IGMP: Internet Group Management Protocol	Status 3
	IETF: Routing protocol	DVMRP: Distance Vector Multicast Routing Protocol	Status 2
		MOSPF: Multicast OSPF	Status 3
		PIM: Protocol Independent Multicast	Status 3
		DNS: Domain Name System	Status 3
Directory service	IETF: Database access	LDAP: Lightweight Directory Access Protocol	Status 3
Registration	IETF	SIP MIP	Status 2 & 3
Dynamic host configuration	IETF	DHCP: Dynamic host configuration protocol	Status 3
QoS	IETF: Transport Quality of service	DIFFSERV: Differentiated Services	Status 3
Transport protocol	IETF	ICMP: Internet Control Message Protocol IPV4 and V6	Status 2 & 3
Location	IETF	SLP: Service Location Protocol	Status 3
Management	IETF	SNMP: Simple Network Management Protocol	Status 3
Transfer	IETF	HTTP: Hypertext Transfer Protocol	Status 3
Languages	W3C	HTML: Hypertext Markup Language	Status 3
	W3C	WSDL: Web Service Description Language	Status 2
	IETF	DHTML: Dynamic HTML	Status 2
	W3C	XML: eXtensible Markup Language	Status 3
	VXML forum	VXML: Voice XML WXML: Wireless WML XMI: XML Metadata Interchange	Status 2
Session advertisement, invitation, description	IETF	SIP: Session Initiation Protocol	Status 2 & 3
	IETF	SDP: Session Description Protocol	Status 2 & 3
Media flows/real time protocols	IETF	RTP/RTCP: Real Time (Control) Protocol	Status 3
	IETF	RTSP: Real Time Streaming Protocol	Status 3
Security	IETF: Encryption, etc.	IPSec	Status 3
	IETF	IPv6	Status 2
	IETF	SSL Secure Socket Layer	Status 3
	IETF	TLS Transport Layer Security	Status 3
	IETF: Authentication	Radius, Diameter	Status 2 & 3
Signalling	IETF	SIP	Status 3
Interoperability	IETF	MGCP: Media Gateway Control Protocol Megaco/H.248 SIGTRAN	Status 1 Status 3 Status 3
Tunnelling		L2TP, GRE, IP in IP encapsulation	Status 3
Mobility management	IETF	MIP and/other protocol	Status 2 & 3
Billing/charging	IETF	AAA, Radius, Diameter	Status 2 & 3
Data Access	W3C	SOAP	Status 2
Messaging	IETF	SMTP: Simple Mail Transfer Protocol POP3: Post Office Protocol 3	Status 3 Status 3
Video		MPEG	Status 3
Transmission	IETF	TCP: Transmission Control	Status 3

Function	Comment	Protocol	Status
		Protocol	
	IETF	UDP: User Datagram Protocol	Status 3
Header compression	IETF/ROCH	ROCCO	Status 2
Middleware	OMG	CORBA	Status 3
	3GPP	OSA	Status 3
	TINA-C	TINA	Status 3
		Parlay	Status 2 & 3
		JAIN	Status 2
Presence and Instant Messaging		IMPP SIMPLE	Status 2
VHE	3GPP	USAT: USIM Application Toolkit	Status 3
	3GPP	MExE: Mobile Execution Environment	Status 3
Addressing		URL URI/NAI ENUM	Status 3 Status 3 Status 2

14 Protocol extensions

The ETSI and IETF protocols in a first approach cover most of the required functions, a certain number of extensions are identified also listed in the recommendation in annex B.

Recommendation 14.1: the identified extensions are:

- core profile server and its interfaces to the networks;
- e-procedures defining for an event the local procedures to apply;
- service APIs related to event and procedures functions, triggering functions;
- priority indication carried in signalling; for the signalling itself and for the communication sessions;
- transport of User and Location data securely carried with the signalling for priority services to be used by authorized Emergency or Essential Service Centres, etc.

15 Dimensioning

For a SIP based IPFN, performance results are needed in order to ensure the user a good service. The identified related work as recommended on a SIP based protocol, also listed in the recommendations in annex B.

Recommendation 15.1: SIP based scenario needs to include multileg calls.

Recommendation 15.2: SIP Call set up time shall be determinable, and limited within a configurable range of values.

Recommendation 15.3: SIP based network transit time needs to be modelled, to determine message compression requirements.

Recommendation 15.4: Configuration of proxies and firewalls, border gateways, network address translation points (NATs) and firewall traversal needs to be modelled and their impact determined.

16 Naming conventions

This clause intends to give interworking users a global naming/IP addressing to allow to access them:

- external addressing plan;
- IPFN addressing plan;
- individual addressing plan;
- multilegs addressing plan;
- organization addressing plan.

Recommendation 16.1: Specify an IPFN addressing plan and its relation to existing or developing numbering plans (E.164, ENUM, etc.).

Annex A (informative): Cross user interworking examples

An X means that interworking between the corresponding users is possible. In some cases X is replaced by an example of reason of interworking.

In some cases interworking can be more than a one to one relationship, several users can be concerned.

Table A.1: Cross user interworking examples

	Residential	**Operator/ISP**	**Corporate**	**Private/PMR**	**IT Agencies**	**Administration**	**ROBO**	**SOHO**	**Tiers**	**NSB**
Residential	V+D	Internet	eCommerce	Emergency				echo	X	
Operator/ISP	X	Roaming	X	X	X	X	X	X	X	QoS
Corporate	X	X	B to B	Security			X	X	X	
Private/PMR	X	X	X	Crisis	X	X			X	
IT Agencies		Warning			X	X				
Administration		X		Coordination	X	X				
ROBO		X	VPN				X		X	
SOHO	X	X	X					X		
Tiers	X	Certificates	X	X			X			
NSB		QoS								X

Annex B(normative): Recommendations

Recommendations are listed with a numbering associated to the clause to which they refer:

Recommendation 8.1: Interworking is provided with the candidate protocols within the IPFN.

Recommendation 8.2: The interfaces between IP to the different functional subsystems shall be open and standardized and reuse of existing IP based standard suites.

Recommendation 8.3: Scalability, though potentially being better addressed by a decentralized architecture, should be a primary concern.

Recommendation 8.4: The IPFN shall support the location Registration and Mobility Features.

Recommendation 8.5: The IPFN shall support Emergency and other Essential Services, including the required priority capabilities and the secure transfer of required user data.

Recommendation 8.6: The IPFN shall support optional Security features.

Recommendation 8.7: The IPFN shall support optional QoS features including priority.

Recommendation 9.1: Define interworking levels.

Recommendation 9.2: Introduce mechanisms to negotiate the interworking services or have equivalent tables.

Recommendation 9.3: Introduce mechanisms to route according to service, like QoS request, policy negotiation and availability.

Recommendation 9.4: Introduce mechanisms to warn users of degradation or upgrade of service.

Recommendation 11.1: The convergence between TIPHON and the IPFN should rely on mapping the ISSI of the IPFN on to the TIPHON IP network to IP network reference points, defined in [2] (namely: M2, C2, T2, R2, SC2' reference points).

Recommendation 11.2: Phase 4 of TIPHON includes numerous new features in its scope. In the scope of the IPFN, the following features are important in order to support Corporate Voice + Data networks:

- Support of mobility from one network to the other:

  in case homogeneous networks are connected through the IPFN, roaming should be possible.

- Support of encryption across networks:

  maintaining end-to-end encryption possibilities between networks connected through the IPFN requires specific exchange of information across ISSI, this should be taken into account.

- Support of multi-leg communications with fast set-up times:

  multi-leg communications may include telephony like conference calls, where participants join with a dial up operation, but also calls without dial up from participants, for example broadcast call from information centre to multiple predefined participants.

- Support of emergency services:

  handling of emergency services includes the setting up calls with highest priority, and may include the sending out of call related information with the same priority (for example sending emergency advice to several information centres). User and Location information shall also be included in this priority call set-up to the authorized Emergency Service Centre.

- Integrated Voice and Data services:

  support shall be provided not only for call-oriented services, but also for user to user data services (e.g. SMS, WAP and Fax.) and server to user data services, including mobility problems.

Recommendation 14.1: the identified extensions are:

- core profile server and its interfaces to the networks;
- e-procedures defining for an event the local procedures to apply;
- service APIs related to event and procedures functions, triggering functions;
- priority indication carried in signalling; for the signalling itself and for the communication sessions;
- transport of user and location data securely carried with the signalling for priority services to be used by authorized emergency or essential service centres , etc.

Recommendation 15.1: SIP based scenario needs to include multileg calls.

Recommendation 15.2: SIP Call set up time shall be determinable, and limited within a configurable range of values.

Recommendation 15.3: SIP based network transit time needs to be modelled, to determine message compression requirements.

Recommendation 15.4: Configuration of proxies and firewalls, border gateways, network address translation points (NATs) and firewall traversal needs to be modelled and their impact determined.

Recommendation 16.1: Specify an IPFN addressing plan and its relation to existing or developing numbering plans (E.164, ENUM, etc.).

Annex C (informative): Bibliography

EURESCOM Project P909-GI: "Enabling Technologies for IN Evolution and IN-Internet Integration; Deliverable 1; What an IN System Should Be". (http://www.eurescom.de/public/projects/P900-series/P909/default.asp)

ITU-T Recommendation Y.140 (2000): "Global Information Infrastructure (GII): Reference points for interconnection framework".

ETSI TR 101 287 (V1.2.1): "Services and Protocols for Advanced Networks (SPAN); Terms and Definitions".

ETSI TS 101 884: "Telecommunications and Internet protocol Harmonization Over Networks (TIPHON) Release 3; Technology Mapping; Implementation of TIPHON architecture using SIP".

ETSI TR 101 308: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Requirements Definition Study; SIP and H.323 Interworking".

ETSI TS 101 878: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service Capability Definition; Service Capabilities for a simple call".

ETSI TS 101 315: "Telecommunications and Internet protocol Harmonization Over Networks (TIPHON) Release 3; Functional Entities, Information Flow and Reference Point Definitions; For application of TIPHON functional architecture to inter-domain services".

ETSI TS 101 882: "Telecommunications and Internet protocol Harmonization Over Networks (TIPHON) Release 3; Protocol Framework Definition and Interface Requirement Definition; General".

A range of standards related to the present document are available from the following locations:

- ETSI: http://www.etsi.org
- WWRF (Wireless World Research Forum): http://www.wireless-world-research.org/
- WSI (Wireless Strategic Initiative): http://www.ist-wsi.org
- IETF (Internet Engineering Task Force): http://www.ietf.org
- IPV6 (Internet Protocol Version 6): http://www.ipv6.org
- W3C (World Wide Web Consortium): http://www.w3.org/
- SOAP (Simple Object Access Protocol): http://www.w3.org/TR/SOAP
- XML (Extensible Markup Language): http://www.w3.org/XML/

History

Document history		
V1.1.1	January 2002	Membership Approval Procedure MV 20020329: 2002-01-29 to 2002-03-29