ETSI TS 102 285 V1.1.1 (2003-11)

Technical Specification

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); TIPHON/UMTS Harmonization: General aspects

Reference

DTS/TIPHON-00003

Keywords

3GPP, IP, telephony, UMTS, VoIP

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.org

Copyright Notification

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 Technical Specification (TS) has been produced by ETSI Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).

Introduction

EP TIPHON has taken an initiative to harmonize with the 3GPP UMTS system, and the IP Multimedia Subsystem (IMS) in particular. This task involves identifying the differences between the two systems, with a view to identifying how to harmonize the approaches.

The results of a gap analysis between TIPHON Release 3 and 3GPP UMTS Release 6 are described in the present document. This analysis is then used as an input to other documents forming part of the harmonization framework. These documents are identified as follows:

- TS 102 283 [16] introduces new service capabilities required, which are missing in TIPHON Releases 3 and 4, to achieve harmonization with 3GPP.
- TS 101 315 [3] contains proposals derived from studies into interworking and harmonization between TIPHON and 3GPP service architectures to identify the extensions and additions to the TIPHON Release 3 and future Release 4 Deliverable on the Application of TIPHON Functional Architecture to inter-domain services.
- TS 101 314 [1] contains proposals for extensions and additions to the TIPHON Release 3 and future Release 4 Deliverable on Network Architecture and Reference Points. The extensions are based on the studies from 00003.
- TS 101 882 [17] contains proposals for extensions and additions to the TIPHON Release 3 and future Release 4 Deliverable on the Protocol Framework Definition.

1 Scope

The present document provides a comparison between TIPHON Releases 3 and 4 and 3GPP UMTS Release 5 system specifications (concentrating on IMS) with a view to harmonize the two. It provides a gap analysis between the two systems, and identifies actions to be taken to resolve any gaps, and achieve harmonization between the two approaches.

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.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ETSI TS 101 314: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Abstract Architecture and Reference Points Definition; Network Architecture and Reference Points".

[2] ETSI TS 123 228: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS); Stage 2 (3GPP TS 23.228)".

[3] ETSI TS 101 315: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Information Flow and Reference Point Definitions; Implementation of Service Capabilities".

[4] ETSI ES 201 915 (all parts): "Open Service Access (OSA); Application Programming Interface (API)".

[5] IETF RFC 3261: "SIP: Session Initiation Protocol".

[6] ITU-T Recommendation H.323: "Packet-based multimedia communications systems".

[7] ETSI TS 101 878: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Service Capability Definition; Service Capabilities for TIPHON Release 4".

[8] ETSI TS 123 221: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Architectural requirements (3GPP TS 23.221)".

[9] IETF RFC 2916: "E.164 number and DNS".

[10] ETSI TS 101 329-2: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; End-to-end Quality of Service in TIPHON systems; Part 2: Definition of speech Quality of Service (QoS) classes".

[11] ETSI TS 123 107: "Universal Mobile Telecommunications System (UMTS); Quality of Service (QoS) concept and architecture (3GPP TS 23.107)".

[12] ETSI TS 101 885: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Interface Protocol Requirements Definition; Implementation of TIPHON using H.248/MEGACO".

[13] ETSI TS 101 331: "Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[14] ETSI ETR 336: "Telecommunications Management Network (TMN); Introduction to standardizing security for TMN".

[15] ETSI TS 102 165-2 :"Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 2: Counter Measures".

[16] ETSI TS 102 283: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); TIPHON/UMTS harmonization; Service capabilities for harmonization between TIPHON and 3G UMTS".

[17] ETSI TS 101 882 (all parts): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition".

[18] ETSI TS 122 105: "Universal Mobile Telecommunications System (UMTS); Services & service capabilities (3GPP TS 22.105)".

[19] ETSI TR 122 121: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Service aspects; The Virtual Home Environment; Stage 1 (3GPP TR 22.121)".

[20] ETSI TS 101 884 (V1.1.1): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Technology Mapping; Implementation of TIPHON architecture using SIP".

3 Abbreviations

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

3GPP	3rd Generation Partnership Project
AES	Advanced Encryption Standard
AoC	Advice of Charge
API	Application Programming Interface
AS	Application Server
BC	Bearer Control
BG	Border Gateway
BGCF	Border Gateway Control Function
BS	Bearer Service
CAI	Charge Advice Information
CB	Call Barring
CBS	Cell Broadcast Service
CC	Call Control
CCBS	Completion of Calls to Busy Subscriber
CD	Call Deflection
CDR	Call Detail Record
CF	Call Forwarding
CN	Core Network
CS	Circuit Switched
CSCF	Call Service Control Function
CUG	Closed User Group
CW	Call Waiting
DHCP	Dynamic Host Control Protocol
DNS	Domain Name Server
DTMF	Dual Tone Multi Frequency
E2E	End-to-End
ECT	Explicit Call Transfer
eMLPP	enhanced Multi-Level Precedence and Pre-emption service
GGSN	Gateway GPRS Serving Node
GPRS	General Packet Radio System
GUP	Generic User Profile
HE-VASP	Home Environment - Value Added Service Provider

HOLD	call HOLD
HSS	Home Subscriber Server
ICF	InterConnect Function
I-CSCF	Interrogating - Call Service Control Function
ID	IDentity
IM	IP Multimedia
IMS	IP Multimedia Subsystem
IM-SSF	IP Multimedia Service Switching Function
ISC	IMS Service Control
LCS	LoCation Services
MAP	Mobile Application Part
MC	Media Control
MGCF	Media Gateway Control Function
MGW	Media GateWay
MNP	Mobile Number Portability
MPTY	MultiParTY
MRFC	Media Resource Function Control
MRFP	Media Resource Function Protocol
MS	Mobile Station
MSP	Multiple Subscriber Profile
MTU	Message Transfer Unit
NITZ	Network Identity and Time Zone
NS	Not Supported
ODB	Operator Determined Barring
OSA	Open Services Architecture
OSP	Open Settlement Protocol
P-CSCF	Proxy - Call Service Control Function
PDF	Policy Decision Function
PDN	Public Data Networks
PDP	Packet Data Protocol
PEF	Policy Enforcement Function
PLMN	Public Land Mobile Network
PS	Packet Switched
PSTN	Public Switched Telephony Network
QoS	Quality of Service
RAN	Radio Access Network
RpoA	Registration point of Attachment
S	Supported
SC	Service Capabilities
SC	Service Control
SCS	Signalling Capability Set
S-CSCF	Service - Call Session Control Function
SDP	Session Description Protocol
SGSN	Serving GPRS Serving Node
SIP	Session Initiation Protocol
SLF	Service Location Function
SOR	Support Optimal Routeing
SpoA	Service point of Attachment
SS	Supplementary Services
TDM	Time Division Multiplex
TpoA	Transport point of Attachment
TTP	Trusted Third Party
TUP	TIPHON User Profile
UE	User Equipment
UMTS	Universal Mobile Telephony System
URI	Uniform Resource Identifier
URL	Universal Resource Locator
UUS	User-to-User Signalling
VBS	Voice Broadcast Service
VHE	Virtual Home Environment

4 Introduction

The present document provides a study of TIPHON and 3GPP IMS subsystem with a view to harmonize the two standardization efforts. The objective of harmonization is to develop a network system that can serve in both the fixed and mobile environments with minimum adaptation, irrespective of the access and transport technologies. This includes interworking between the two systems. The target harmonization will lead to true convergence between traditional Circuit Switched, Packet Switched and Mobile technologies such as UMTS IMS.

The harmonization objectives can further be explained in the context of the following scenarios.

- Completion of Calls originating in the TIPHON domain and terminating in the 3GPP domain.
- Completion of Calls originating in the 3GPP IMS domain and terminating in TIPHON domain.
- Completion of Calls originating in a 3GPP IMS domain, transiting through a TIPHON domain, and terminating in another 3GPP domain.
- TIPHON users roaming in the 3GPP IMS domain to gain access to the serving domain's services, as well as the services from the Home (TIPHON) domain. 3GPP IMS users roaming to a TIPHON domain to receive services from the serving domain, as well as the HOME (3GPP) domain.
- 3GPP IMS users in the Home domain accessing the services provided in a TIPHON domain
- TIPHON users in Home domain accessing services executed/provided in a 3GPP IMS domain.

The objectives described above can be achieved by closely aligning the concepts, functions, capabilities and behaviour of 3GPP IMS and TIPHON systems. It is understood that a complete alignment will not be achieved due to certain fundamental differences in some of the services provided by both the fixed (TIPHON) and mobile (3GPP IMS) systems. Nevertheless, the two systems should be aligned closely enough so that the resulting TIPHON system can be adapted to serve both the fixed and mobile markets, with minimum additions and changes.

5 Architecture

TIPHON and 3GPP IMS have developed architectures that identify concepts addressing the requirements related to their respective systems. These architectures consist of functions and capabilities that fulfil their requirements. In order to harmonize the two systems, TIPHON and IMS, it is important to compare the concepts, functions, capabilities, protocols and behaviour of these two systems. This comparison will be used to identify any gaps and differences between the two systems, and recommend changes to prospective system to achieve harmonization.

The TIPHON architecture is a generic architecture that specifies functions and capabilities required to support a set of services using application and transport planes. 3GPP has developed an implementation specific architecture specified for an access network based on the air interface and a core network that provides access to services, such as telephony and messaging. Note that TIPHON assumes that the access to transport resources is available, and provides a framework to develop and provide services. Detailed descriptions of the architectures are available in TS 101 314 [1] and TS 123 228 [2]. The 3GPP architecture is split into the circuit and packet switched domains. The circuit switched domain provides the traditional telephony services including supplementary services, whereas, the packet switched domain provides access to data networks to enable the provision of new value added services including data and voice communications. 3GPP has now taken the approach to develop service capabilities instead of standardizing services. These service capabilities can be used to develop differentiating services. The latter approach is also adopted by TIPHON. The 3GPP service capabilities can be used to develop services for both the circuit and packet switched domains, as is the case in TIPHON.

The comparison of 3GPP IMS and TIPHON architectures in the present document is limited to the concepts, functions, behaviour and protocols supported by both the systems.

5.1 Concepts

TIPHON and 3GPP IMS have developed their architectures on the following concepts, to serve their respective requirements. These concepts will be used as a basis for the comparison between TIPHON and 3GPP IMS.

- Mobility.
- Session control.
- Signalling.
- Security.
- Quality of Service (QoS).
- Services and Service Capabilities.
- Virtual Home Environment (service provisioning from home and visited domain and OSA APIs).

These concepts are used to develop functions and capabilities, which are described in the rest of the present document.

5.2 TIPHON and IMS Functional architectures

Both the TIPHON and 3GPP IMS architectures are shown in the figures 1 and 2 respectively. The TIPHON architecture TS 101 314 [1] is a generic architecture that can be used on any underlying technology be it circuit or packet switching. It can be vertically decomposed into several application and transport layers, as well as horizontal decomposed into serving, intermediate and home domains.

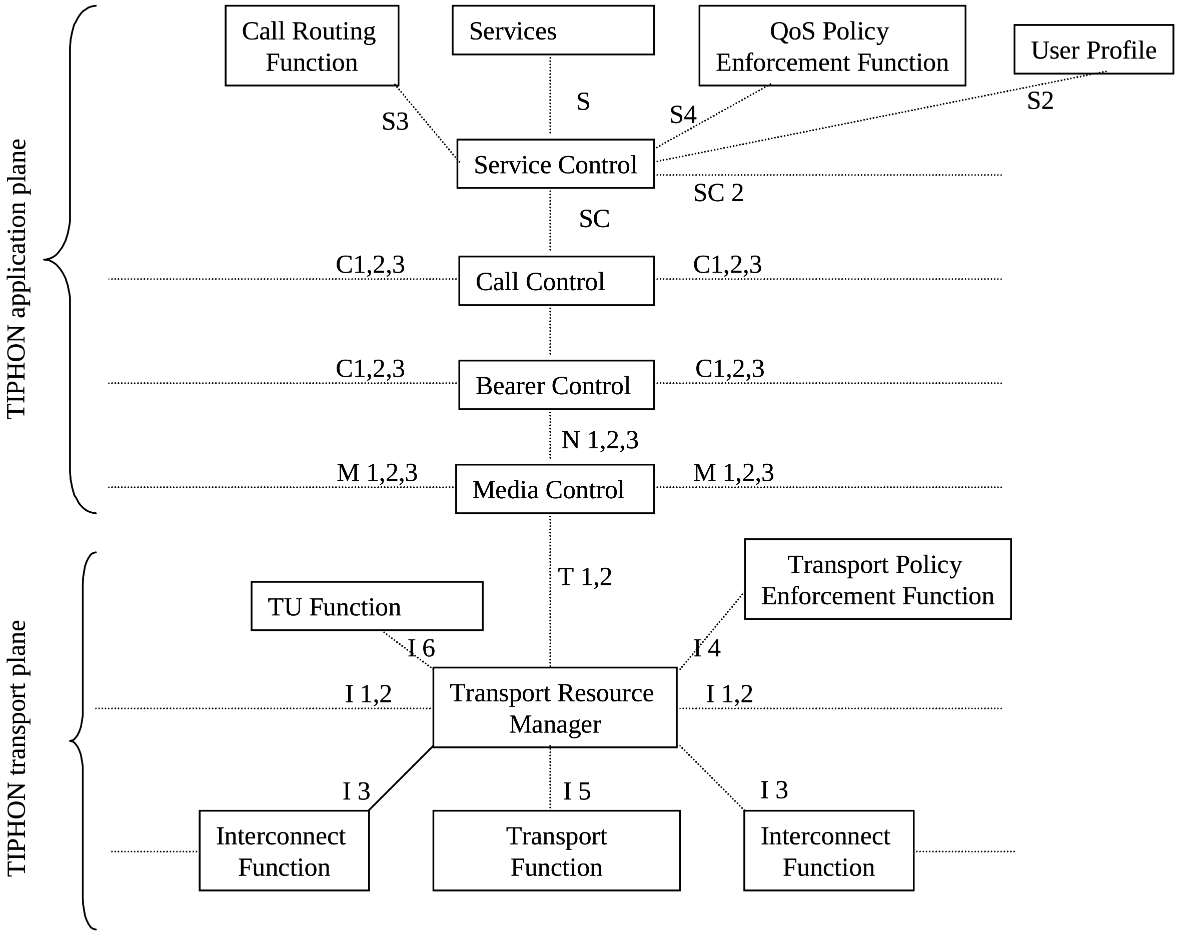

Figure 1: TIPHON functional architecture

The IMS architecture illustrated in figure 2 shows the configuration of IMS functional entities.

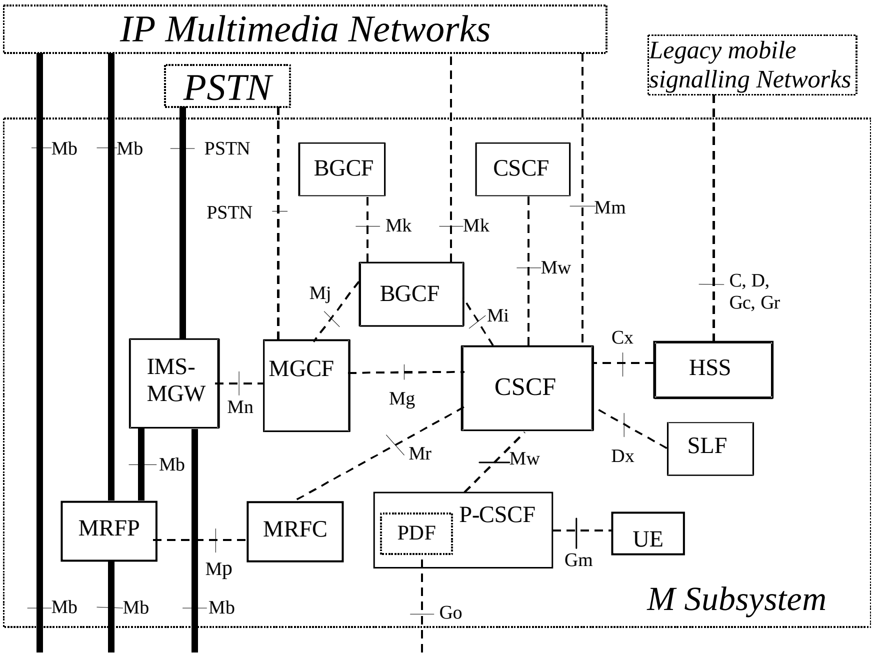

Figure 2: IMS systems configuration

The TIPHON architecture for Release 4 is focussed mainly for the support of telephony applications, whereas, IMS is focussed on multimedia services. However, it is believed that the TIPHON architecture can support the multimedia services with minimum changes.

5.3 Functions

This clause provides the comparison of functions supported by both the TIPHON and IMS. The TIPHON functions are standalone functions that provide services of the same kind. For example, the Call Control (CC) function provides services related to call management. One or more of these functions can be deployed to form another function. For example, CC, Bearer Control (BC) and SC can be combined to develop a CSCF function. TIPHON and IMS have developed the functions identified in table 1 to support the concepts identified in clause 5.1. Table 1 shows that for each IMS function, a set of equivalent functions is available in TIPHON.

Table 1: Comparison between TIPHON and IMS functions

3GPP IMS functions	TIPHON Functions	Comments
HSS	Service function: User profile	TIPHON user profile performs most of the functions as HSS
SGSN	Interconnect Function, ICF Transport Function, TF	
GGSN	Interconnect Function, ICF Transport Function, TF Transport Resource Manager, TRM	
BG	Interconnect Function, ICF	
MS	Terminal Functional Group	
P/I/S-CSCF	Call Control (CC) and Bearer Control (BC) and Service Control (SC) functions	CC functions of type: S- Serving (home and visited domain), I-Intermediate.
MGCF	Call Control (CC) and Bearer Control (BC) functions	
IMS-MGW	Media Control (MC) function	
MRFC	A specialized CC	
MRFP		
SLF	RpoA	
BGCF	Call Routing (CR) function, CC	
Signalling GW	Call Control (CC) and Bearer Control (BC) function	CC supporting C2 and C3 reference points
Application Server	Application Server	"S" reference point. Detailed behaviour not specified

It can be seen from table 1 that all of the 3GPP IMS functions and concepts described in TS 123 228 [2] are supported by TIPHON. Note that there may be differences in the behaviour of these functions in TIPHON and IMS. These differences are highlighted and discussed in the rest of the present document.

5.4 Service Capabilities (SC) and support for APIs

Both TIPHON and 3GPP IMS have adopted the approach not to standardize services, instead, both have standardized service capabilities. Service Capabilities (SC), are underlying technology independent building blocks that can be used independently or in a combination to develop a service. One of the reasons for adopting this approach is to allow for rapid service creation, allowing for standardized and unique services to be offered by the service providers. However, 3GPP system is divided into two parts:

- Circuit Switched (CS) part; and
- Packet Switched (PS) part.

The CS part inherits the standardized services from the 2nd generation systems such as GSM. The PS domain is a new domain which may initially utilize the support of services developed using service capabilities. TIPHON does not differentiate between CS and PS domains, and allows for service creation from its service capabilities irrespective of the TDM or IP based transport technology.

TIPHON and 3GPP define their SCs in object oriented methodology, defining classes, parameters and methods (SCs). However, there is a difference between the definition (clause 8.1) of service capabilities between TIPHON and 3GPP. 3GPP have adopted the approach of developing the SCs under the umbrella of open APIs, called OSA APIs. These APIs have been extensively defined for different Service Capability Features. There are several SC features such as Call Control, Charging, Data Transfer. The granularity of 3GPP SC features is different from TIPHON SCs, whose Service Capability Features are larger, more course grained blocks of functionality. The result is that 3GPP can support a rich set of services using these CS features. TIPHON has focused mainly on services related to telephony until Release 4, and has developed a smaller set of SCs compared to 3GPP.

A detailed comparison of TIPHON and 3GPP Service capabilities is provided in clause 8.

5.5 Conclusion

The TIPHON and UMTS IMS functional architectures are very similar, and there is a direct mapping available between the TIPHON and IMS functions. The main difference between the two architectures is that of approach adopted to develop these two architectures: IMS approach is specific to services to be supported in the UMTS environment, whereas, TIPHON approach is generic, to accommodate different underlying technologies and services. TIPHON functional architecture is flexible and can support different functions in IMS, e.g. the combination of Call Control, Bearer Control and Service Control functions in TIPHON architecture can support services provided by different types of CSCF including I-CSCF, P-CSCF and S-CSCF, as well as Signalling Gateway and Border Gateway (BG).

The service capabilities developed by TIPHON up to Release 4 are mainly focused on Telephony, whereas, 3GPP has focussed on a whole host of multimedia services. Consequently, there is a big gap between TIPHON and 3GPP in this area. It is recommended that in order to harmonize fully with 3GPP, TIPHON enhances its capability set to support the multimedia services, as supported by 3GPP.

Although TIPHON supports all the functions identified in IMS architecture, there is a need to show explicitly which of the TIPHON functions combine to provide the services offered by IMS functions. This should include the behaviour of the resulting TIPHON function. For example CC, BC, and MC combine to form the IMS MRF function, but it is not clear how the resulting function will behave in the context of TIPHON.

TIPHON has developed the "S" reference point, between the Service Control function and the Service (Application Server). This is considered equivalent to the ISC interface between the IMS Call Control and the Application server. However, a neither detailed behaviour of the "S" reference point nor a meta-protocol is defined in TIPHON. This should be addressed in subsequent release of TIPHON.

6 Mobility

This clause provides a comparison of concepts related to mobility between TIPHON and UMTS. Both the TIPHON and UMTS have developed functions, capabilities and procedures to support mobility and mobility management in their respective architectures. UMTS has inherited the concepts related to mobility from the second generation mobile systems such as GSM. Whereas, TIPHON has developed its architecture for fixed line users, whilst taking into consideration different aspects of mobility as shown in TS 101 315 [3]. These aspects include terminal mobility, user mobility and service mobility, and are described below:

- Terminal mobility includes out of session as well as in-session mobility where the user is merely registered with the network in the former scenario and registered and involved in a session in the latter scenario.

- User mobility encompasses terminal mobility scenarios as well as the scenario where a user does not have a mobile terminal. In the latter case, the user may be attached to terminals at different transport points of attachment.

- Service mobility encompasses both the terminal mobility and user mobility, as well as providing services from home domain or from the visited domain. The concept of service mobility can be further developed for the VHE.

To cover the above aspects, TIPHON has developed a mobility framework that encompasses the following:

- Mobility scenarios: Mobility within Home domain or visited domain (Roaming).

- Registration: This includes authentication, authorization, location update, and support to request specific services.

- Service execution environment that supports services executed in the Home or Visited domain, leading to the support of Virtual Home Environment.

The concepts related to mobility in IMS (TS 123 228 [2]) and the corresponding TIPHON response are described below:

- Connect to the core network using GPRS procedures and acquire the necessary IP address via activation of a Packet Data Protocol (PDP) context, which includes, or is followed by, the P-CSCF discovery procedure.

  - The mobility aspects of the transport network such as GPRS as well as IP address management have not been covered in TIPHON. The procedures to discover the RpoA (equivalent to P-CSCF) are similar to IMS.

- Register to the IM subsystem as defined by the IMS registration procedures.

  - Although the concept is similar, there are slight differences in the registration procedures in TIPHON: TIPHON has identified a "RE-Register" indicator in the re-registration requests, whereas, IMS re-registration requests are initiated and treated as an initial registration request. TIPHON should specify the behaviour of scenario where the 're-registration' indicator is not available in re-registration request. This would enable harmonization with IMS.

- If a User Equipment (UE) explicitly deactivates a PDP context that is being used for IMS signalling, it shall first de-register from the IMS (while there is no IMS session in progress).

  - TIPHON has not specified the procedures for terminating a transport connection with the user equipment. This is currently outside the scope of TIPHON. However, it is implicit that any disconnection from the transport network will be preceded by deregistration.

- If a UE explicitly deactivates a PDP context that is being used for IMS signalling while an IMS session is in progress, the UE must first release the session and de-register from the IMS and then deactivate the PDP context.

  - TIPHON has not specified the procedures for terminating a transport connection with the user equipment. This is currently outside the scope of TIPHON. However, it is implicit that any disconnection from the transport network will be preceded by deregistration.

- If an UE acquires a new IP address due to changes triggered by the GPRS/UMTS procedures, the UE shall re-register in the IMS by executing the IMS registration.

  - The scenario of change in terminal address whilst registered is not specified in TIPHON. However, this issue is not considered to have a major impact on harmonization, as this procedure can be adopted in TIPHON.

- In order to be able to deliver an incoming IMS session, the PDP context that is being used for IMS signalling need to remain active as long as the UE is registered in the IM Core Network (CN) subsystem.

  - TIPHON assumes that the connection to transport network will be available so that the calls can be delivered to a registered user.

TIPHON and UMTS have developed different scenarios, capabilities and procedures to support and manage the above concepts of mobility, which can be described generically as:

- Support for services from home or visited domain.
- Registration.
- User profile.

Clause 6.1 will compare in detail the procedures relevant to harmonization efforts related to the above concepts.

6.1 Support for services from home and visited domains

6.1.1 Local services provided from home or visited domain

TIPHON supports access to services provided either at Home or in a Visited domain. This concept is also supported in IMS (TS 123 228 [2]). This allows for the support of standardized or unique services to be provided by both the Home and Visited network leading to possible increase in revenues for service providers.

6.1.2 Support for OSA

IMS requires that it should be possible for an operator to offer access to services based on OSA for its IM CN subsystem subscribers. This should be supported by an OSA API between the Application Server (AS) and the network.

TIPHON has not yet specified the use of external APIs to support services offered by application servers. However, TIPHON has specified the "S", "SC" and "CC" reference points TS 101 314 [1] which can be used to register and gain access to services. This work could be furthered to map the OSP APIs (ES 201 915 [4]) to TIPHON metaprotocols, allowing TIPHON users access to services offered by OSA servers.

6.1.3 Service Control interface

IMS has specified a service control interface, ISC, between the Serving CSCF and the service platform(s), allowing services to be provided from platforms other than CSCF. The services platforms, also known as Application Servers (AS) offer value added IMS services. The ASs reside either in the user's home network or in a third party location. The third party could be a network or simply a stand-alone AS. The Serving-CSCF to AS interface is used to provide services residing in an AS.

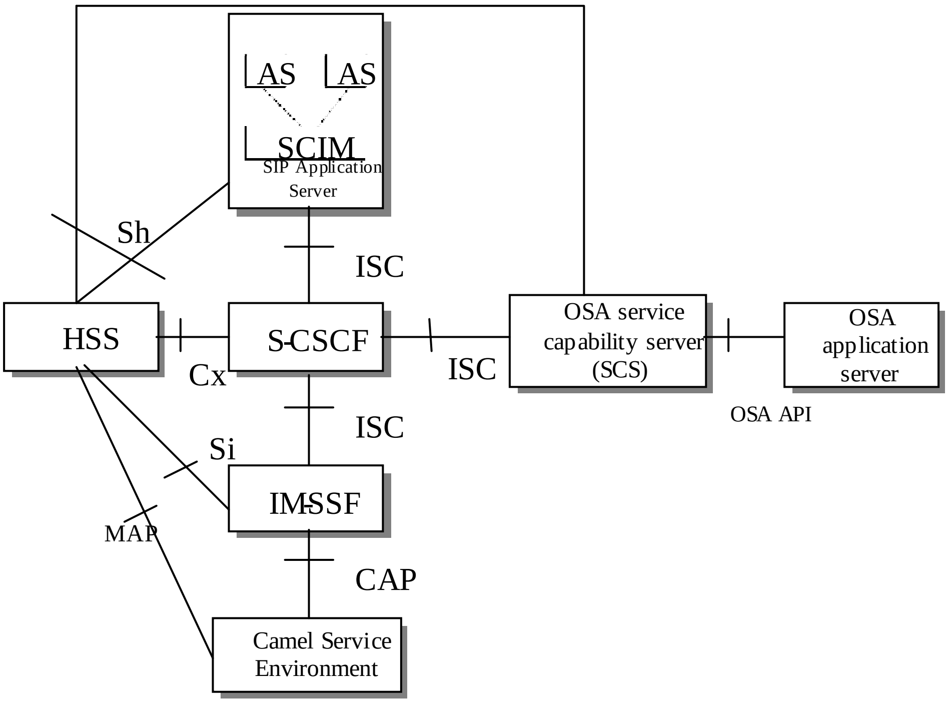

Figure 3

Figure 3 shows how different functions in IMS can provide services via S-CSCF.

TIPHON has specified the "S", "SC" and "CC" reference points (figure 1) that are used to access services from service platforms, or application servers in the serving, home, or another domain. However, "S" and "SC" reference points have only been specified for a limited set of services such as Registration.

6.1.4 Conclusion

Both TIPHON and UMTS IMS support the concepts of VHE, although the means of achieving are somewhat different. UMTS achieves this via the CAMEL framework, whilst TIPHON achieves this via its Registration and Service Preparation framework. TIPHON has not specified the use of standardized APIs such as OSA/PARLAY to develop and provide services from within or outside a service provider's domain. However, TIPHON has the capability to support APIs by mapping the OSA APIs to the TIPHON Service Capabilities Interfaces. This work should be considered in a subsequent TIPHON release.

6.2 Registration

The registration service allows a registrant to register with a registrar. This concept supports:

- the authentication of a user;
- authorization of user to ensure that a user is authorized to access the services requested by the user;
- informing the registrar of the contact details, such as IP address to ensure, e.g. incoming calls can be terminated to the user;
- update of contact details held by the registrar.

Registration is a prerequisite for services: a successful registration would normally lead to access to services a user is entitled to, whereas, an unsuccessful registration would normally lead to refusal of service. The latter may not apply in exceptional circumstances such as request to access emergency services. The registration service supports mobility, as it allows a user to register from different terminals, as well as from different 'Transport points of attachment' in the home or visited domains.

6.2.1 IMS Requirements analysis

The following points are considered as requirements for the purpose of the registration procedures in IMS.

1) The architecture shall allow for the Serving-CSCFs to have different capabilities or access to different capabilities. E.g. a VPN CSCF or CSCFs in different stages of network upgrade.

   - The TIPHON architecture allows the flexibility to access different SpoA, offering different capabilities. The allocation of SpoA to a user is based on the user profile and the services requested by a user. Considering this is in line with the above IMS requirement, no issue for harmonization is foreseen.

2) The network operator shall not be required to reveal the internal network structure to another network. Association of the node names of the same type of entity and their capabilities and the number of nodes will be kept within an operator's network. However disclosure of the internal architecture shall not be prevented on a per agreement basis.

   - This requirement is related to the 'Topology Hiding' capabilities with in a domain. TIPHON does not mandate such a requirement on the system, instead, topology hiding is considered a policy matter for the network operator, and it can be imposed at the gateways interconnecting to adjacent domains. TIPHON has not yet defined explicit procedures for withholding the topology information, and is something it may consider in the subsequent releases.

3) A network shall not be required to expose the explicit IP addresses of the nodes within the network (excluding firewalls and border gateways).

   - This requirement is supported in TIPHON via the use of the Inter-connect function (ICF), as the addresses behind the ICF are hidden from external domains

4) It is desirable that the UE will use the same registration procedure(s) within its home and visited networks.

   - Although TIPHON differentiates between the scenarios where a user registers from within the home domain, and visited domain, the procedures are not different from IMS which assumes the user to be always roaming.

5) It is desirable that the procedures within the network(s) are transparent to the UE, when it registers with the IM CN subsystem.

  - The reference point visible to a TIPHON user is R1 for registration. Anything beyond R1 is not known to the user, Therefore, TIPHON supports this requirement.

6) The Serving-CSCF understands a service profile and the address of the functionality of the Proxy-CSCF.

  - TIPHON supports this requirement.

The following clauses discuss some of the above requirements in detail.

6.2.2 Scenarios

UMTS considers only one scenario for user mobility and assumes that a user is always roaming. Therefore, the procedures for registration whether a user is in the home or visited domain are same. TIPHON considers two scenarios for providing services to users: User at home and roaming user scenario. However, the procedures for registration for a user and network entities are similar to IMS.

6.2.3 Access to transport network

It is assumed in TIPHON that the terminal is provided with access to transport network. Since this access is out of the scope of TIPHON, no procedures are described. IMS requires establishment of PDP context after a mobile station has registered successfully with the serving network. Therefore, registration with IMS domain is considered a secondary registration. This difference has no impact on the harmonization between TIPHON and IMS.

6.2.4 Registrar discovery

Discovery is a mechanism by which the registrar is discovered prior to the actual registration. Both IMS and TIPHON support several mechanisms to discover a registrar such as DHCP, Multicast addresses, and provision of registrar identity in user agent/USIM. Because these mechanisms are common to both TIPHON and IMS, no issue for harmonization is foreseen in this area.

6.2.5 Pre-requisites and registration data

Both the TIPHON and IMS have identified data required to achieve successful registration. IMS has identified the holders (different entities involved in registration) of this data for the following states:

- Before registration.
- During registration.
- After registration.

The data identified as a prerequisite to Registration by both the TIPHON and IMS is:

- Registered Private and public identities, i.e. registrant ID.
- Home domain identity.
- Authentication credentials.

No harmonization issue foreseen in relation to this area.

6.2.6 Authentication and authorization

In TIPHON registration framework, a user is authenticated by providing its private identity and key. Private identity is used only once to reduce the chances of it being intercepted. Once the user is authenticated, authorization takes place to check if the user is allowed access to the requested services.

In IMS registration, private identity is also used to authenticate the subscriber. Unlike TIPHON, the private identity is used in all the registration, re-registration and de-registration requests. This increases the chances of the compromising the private ID. This could reduce the security of the system.

TIPHON recommends that IMS should NOT include the private ID in all the communications with registration.

6.2.7 Server assignment

In TIPHON, the server (SpoA) is assigned by the RpoA after successful authentication, based on the services a user requests or is entitles to, as described in the "user profile". The equivalent of SpoA in IMS is S-CSCF. The S-CSCF is assigned by the I-CSCF based on:

- The capabilities a user is entitled to, as described in the user profile, accessible to HSS and provided to I-CSCF.
- Operator preferences.
- Capabilities of individual S-CSCFs in the home network.
- Topological (i.e. P-CSCF) information of where the subscriber is locate.
- Availability of S-CSCFs.

The above policies for SpoA allocation are not specified in TIPHON, but TIPHON can accommodate these policies without an impact on the rest of the architecture. Therefore, no issue is foreseen in harmonizing with IMS in this area. It is, however, recommended that TIPHON aligns the policy framework for assigning SpoA as defined in IMS.

6.2.8 Multiple Identity registration

Multiple identity registration allows for more than one user identities to be registered for one user address. IMS allows the multiple ID registration to take place in one registration request, or separately on a need to do basis. Note that the multiple IDs are public IDs, and are bound to a private identity of a subscription.

TIPHON also supports multiple ID registration. This capability is supported in the Registration meta-protocol but the procedures for this capability are not described in any of the TIPHON documents. It is recommended that TIPHON updates its registration framework to show that it supports multiple identity registration.

6.2.9 Protocols

TIPHON is a technology independent framework, and different protocols can be mapped to its meta-protocol, including Registration meta-protocol. TIPHON currently supports SIP (RFC 3261 [5]) and ITU-T Recommendation H.323 [6] protocols to achieve registration. IMS supports only SIP as the protocol of choice. This limits the choice of protocol employed by the service provider and used by the end user.

A consequence of choosing just one protocol is that a TIPHON compliant user/terminal using a protocol other than SIP will not be able to utilize services offered by the IMS SIP network when roaming.

6.2.9.1 Communications between User Profile and SpoA

UMTS IMS uses MAP for communications between the HSS and S-CSCF. The communications that takes place between HSS and S-CSCF includes operations such as downloading user profile from the HSS to S-CSCF. TIPHON has also identified operations such as profile download between the Registrar and SpoA. Although the Registration meta-protocol supports these operations, a target standardized protocol has not been identified to map to the meta-protocol.

It is recommended that TIPHON addresses this issue to support the registration framework completely, using a standardized protocol.

6.2.10 Subscription update

IMS requires that whenever a modification occurs in the subscription data that constitutes the data used by the S-CSCF, the complete subscription data set shall be sent to the S-CSCF by the HSS. HSS shall use the Push model for downloading the subscription data to the S-CSCF.

TIPHON has to identify the capability TS 101 878 [7] that can be used to send subscription updates from the User Profile holder (Registrar) to the SpoA. However, a target standardized protocol has not been identified nor the procedures associated with the subscription update.

It is recommended that TIPHON defines procedures related to subscription update that are aligned with IMS to achieve harmonization.

6.2.11 Role of different functions in registration

IMS has identified different functions involved in IMS application level registration. These include CSCF and HSS. The role for a CSC Function includes:

- Proxy-CSCF, P-CSCF.
- Interrogating-CSCF, I-CSCF.
- Serving-CSCF, S-CSCF.

Each of the above CSCF functions performs a different role during registration. P-CSCF acts as the point of contact for the user to gain access to services including Registration. I-CSCF acts as an agent that identifies the suitable S-CSCF in consultation with HSS, and S-CSCF is the function that actually provides the user with the services it is entitled to. The details of the registration model are available in TS 123 228 [2].

TIPHON has also identified roles for RpoA and SpoA during registration, and when considering the "roaming user scenario", they perform the functionality that of IMS functions. Therefore, no issue is expected in harmonizing with IMS.

6.2.12 Conclusion

The following conclusion and recommendations are drawn from the comparison of TIPHON and IMS registration frameworks.

TIPHON and IMS registration frameworks are closely aligned, with slight differences. TIPHON supports most of the IMS requirements related to registration. There is slight difference in the scenarios considered by IMS and TIPHON: IMS always considers a user to be roaming, whilst TIPHON considers it either 'at home domain' or 'roaming' in another domain. The procedures are not different in either case, hence no issue for harmonization.

IMS has defined procedures for accessing the Transport network via establishment of PDP context as a pre-requisite. This is because IMS is designed mainly to serve a user with wireless access. TIPHON is access independent and can be used with any access technology. However, TIPHON should consider defining the procedures related to gaining access to transport network, referred to as 'Transport Point of Attachment', TpoA, prior to application level registration.

TIPHON recommends the use of a token to authenticate any communications with the service providers. This token is provided by the registrar after initial registration, when the user provides private identity and other credentials. However, IMS requires the private Identity to be provided in all communications with the server. This can lead to a higher probability of compromising a user's private identity. It is recommended that IMS adopt an alternative approach similar to TIPHON to minimize the risk of compromising a user's private identity.

TIPHON has specified procedures for communications between the user profile and the SpoA, and has developed a meta-protocol (registration) for this purpose, but it has not identified a target standardized protocol for implementation of this capability. IMS has inherited MAP from GSM for communications between the HSS and the CSCF. TIPHON should address this issue in the subsequent release.

6.3 User profile

This clause provides a comparison between the TIPHON and UMTS user profiles. The user profiles are considered important component of both the TIPHON and IMS systems. User profiles contain data related to a user which includes capabilities a user has access to, and services that are available to a user. This data can be accessed by different entities in the network such as Application servers, SpoA and S-CSCF. The following aspects of a user profile are covered:

- Description of user profiles.
- Data elements of user profile.
- Operations on user profile.
- Structure of user profiles.

Note that although the User Profile is covered under mobility, it is also required to support fixed users.

6.3.1 Description of user profiles

6.3.1.1 UMTS generic user profile, GUP

The objective of specifying the 3GPP Generic User Profile is to provide a conceptual description to enable harmonized usage of the user-related information located in different entities. The specification of the GUP shall also allow extensibility to cater for future developments.

The 3GPP Generic User Profile is the collection of User-related data which affects the way in which an individual user experiences services where a community of entities share this data. The 3GPP Generic User Profile can be stored in the home network environment and additionally storage can be extended to the UE and/or Value Added Service Provider equipment.

The 3GPP Generic User Profile will be accessed and managed by different stakeholders such as the user, subscriber, value added service provider and network operator by a standardized access mechanism. The 3GPP Generic User Profile allows intra-network usage (i.e. data exchange between applications within a mobile operator's network) and inter-network usage (between mobile operator's network and value added service providers) as illustrated in figure 4.

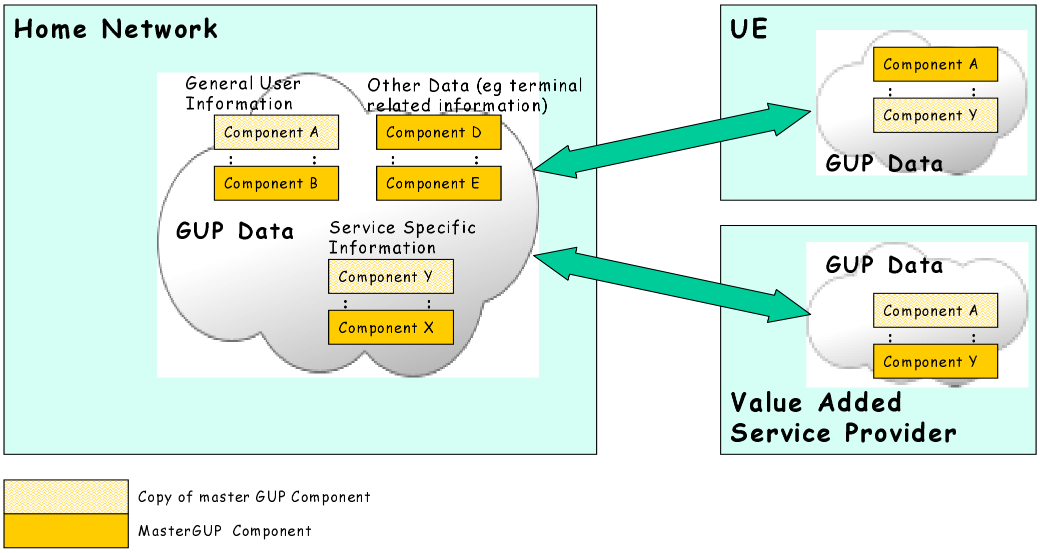

Figure 4: GUP use scenarios

The 3GPP Generic User Profile may be also be used by different applications in a standardized way.

The 3GPP Generic User Profile will help to create and manage the user data in each entity and on the other hand to make it easier to find all user related data as a whole in the home network environment.

Technically the 3GPP Generic User Profile provides an architecture, data description and interface with mechanisms to handle the data.

6.3.1.2 TIPHON User profile

TIPHON user profile contains user specific data. This data can be used to provide access to the services subscribed by a user, or to restrict access to the services. TIPHON user profile can be accessed by different entities inside or outside the user's home domain, depending on the access granted to access different types of data.

The users of TIPHON user profile have not been clearly defined, nor where the data is stored. This should be addressed in TIPHON.

6.3.2 Operation on user profile

6.3.2.1 GUP operations

The intended usage of the 3GPP generic user profile is a critical factor driving its detailed specification e.g. architecture and data model. In general, user profile data can be shared between different stakeholders to facilitate the following:

- **User preference management:** Enable applications to read and utilize a limited set of user preference information.
- **User service customization:** Enable applications to read and utilize personalized service information i.e. individual settings for a particular service.
- **Terminal capability management:** Enable applications to access terminal-related capabilities.
- **User Information sharing:** Enable applications to read and utilize application level information e.g. address book information.
- **Profile key access:** Enable applications to use a unique identity as a key to access profile information, e.g. any public user identity or an alias.

It is intended that the 3GPP GUP, in particular, will address all of the above. As can be inferred, a user's identity can serve as the unique common key into the profile.

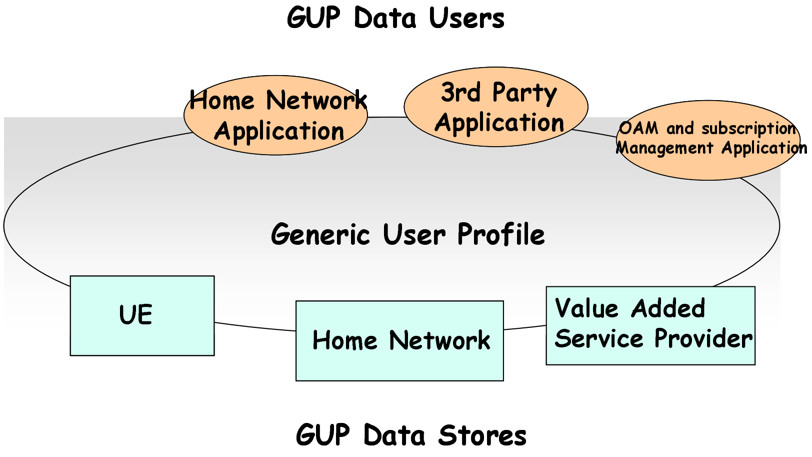

Figure 5: GUP data stores

6.3.2.2 TIPHON user profile operations

The following operations can be performed on a TIPHON user profile:

- **register:** allows a user to register for a service from a set of subscribed services.
- **attach:** allows a user to explicitly attach to a service provider (service node inside or outside the home domain).

- **authenticate:** invokes authentication of a user based on credentials provided, and data stored in the user profile.
- **authorize:** invokes authorization of a user to use a service based on credentials provided.
- **deregister:** terminates a specific registration and mark the user as not available as not-available in the profile.
- **detach:** allows a user to detach from a previously service provider attachment.
- **getStatus:** allows an application to request the status of the user from the related elements in the user profile.
- **setStatus:** allows an application or user to update the status of a user.
- **setCondition:** allows triggers and actions to be set against certain events.
- **clearCondition:** allows the cancellation of an active setCondition.
- **transfer:** allows some or all of the user profile data to be transferred from one entity to another.

The operations performed on user profiles by UMTS GUP TUP are described differently; nevertheless, they achieve similar results. Therefore, no issues of harmonization have been identified.

6.3.3 User Profile structure

6.3.3.1 GUP structure

The structure recommended by the GUP is decomposed as follows:

- **General information:** This includes general information related to a subscriber, e.g. Address, billing information.
- **Capability description:** Contains data on capabilities available and supported by a subscriber, e.g. Terminal capability, communications capability.
- **User's preference:** This contains the user preferences, e.g. user interface preference.
- **Parameters:** This includes setting of parameters related to different services, e.g. parameters related to security and supplementary services.

6.3.3.2 TIPHON User Profile Structure

The structure of user profile is not defined in TIPHON.

TIPHON should define a standardized TUP structure so as to facilitate the download of data between different domains allowing, for example, 3rd party services to be supported. It is recommended that TIPHON considers the user profile structure adopted by UMTS, allowing a close alignment between UMTS and TIPHON.

6.3.4 User Profile data

6.3.4.1 GUP data

UMTS GUP has not specified any data yet [GUP]. However, there is an example of the type of data that could be available in GUP. This example is included in Annex A for illustration only.

6.3.4.2 TIPHON User Profile (TUP) data

TIPHON User Profile (TUP) data may be distributed in different parts of the TIPHON architecture. This information has been included in annex A for illustration purpose only.

It is recognized that the data elements for a user profile in UMTS and TIPHON will be specific to the corresponding systems. Therefore, no issues for harmonization have been identified.

6.3.5 Conclusion

TIPHON has not yet developed a structure for user profile. It is recommended that TIPHON develops a structure for the user profile data. TIPHON can adopt the structure developed by UMTS, which will allow an alignment between the two user profiles. TIPHON should also identify the data stores for the user profile data, along with authentication levels, allowing different functions to access user related data.

7 Session control

7.1 General

7.1.1 Access to transport domain

IMS requires establishment to GPRS PDP context before an IMS session can exist. Here, GPRS acts as the access technology to the packet switched network. TIPHON, however, does not mandate the use of any particular technology for the purpose of accessing the network providing the desired services.

7.1.2 Requirements for session control

The requirements for session control presented below have been derived from 3GPP IMS architecture (TS 123 228 [2]), and forms a basis for comparing the founding principles of session control. A comparison with TIPHON is provided for each of the requirement to identify any gaps in principles behind the capabilities supported by both the TIPHON and IMS.

7.1.2.1 Resource reservation during call establishment

Both end points of the session shall be able to negotiate (according to service / UE settings) which resources (i.e. which media components) need to be established before the destination party is alerted. The session signalling shall ensure that these resources (including (UMTS) IP-Connectivity Network resources and IP multimedia backbone resources) are made available or reserved before the destination UE rings. This should nevertheless not prevent the UE from offering to the end-user the choice of accepting or rejecting the components of the session before establishing the bearers.

The call control capabilities in TIPHON follow a similar behaviour, therefore, no issue is foreseen with regards to resource reservation during call establishment.

7.1.2.2 Charging and reverse charging

Depending on regulatory requirements, the IP multimedia service shall be able to charge the originating party for the Access IP-connectivity service of both originating and destination side or when reverse charging applies to charge the terminating party for the Access IP-connectivity service of both originating and terminating side. This implies that it should be easy to correlate CDR held by Access IP-connectivity service (e.g. GPRS) with a session.

TIPHON has not yet developed a framework for charging the originating party for the usage of transport resources for both the calling and called party. This area is for further study in TIPHON.

7.1.2.3 Control over sessions

The session control function of IP multimedia network of an operator (CSCF) shall be able (according to operator choice) to have a strict control (e.g. on source /destination IP address, QoS) on the flows associated with session established through SIP entering the IP multimedia bearer network from Access IP-connectivity service. This does not mean that CSCF is the enforcement point (which actually is the Gateway between the Access IP-connectivity service and the IP multimedia network, i.e. the GGSN in UMTS case) but that the CSCF may be the final decision point for this control.

The TIPHON architecture strictly requires access control to be observed for all the sessions originating or terminating in a TIPHON domain. This access control is currently the responsibility of the SpoA serving both the originating and terminating party. The exertion of access control via the transport network is limited to the media flowing through the ICFs, which are under the control of Call Control function. This behaviour is in line with the above requirement.

7.1.2.4 Relationship between session control and synchronization for charging

The session control and bearer control mechanisms shall allow the session control to decide when user plane traffic between end-points of a SIP session may start/shall stop. This allows this traffic to start/stop in synchronization with the start/stop of charging for a session.

TIPHON is fully compliant with this requirement.

7.1.2.5 Transport connectivity management

The Access IP-connectivity service shall be able to notify the IP multimedia session control when Access IP-connectivity service has either modified or suspended or released the bearer(s) of an user associated with a session (because e.g. the user is no longer reachable).

TIPHON has not yet specified the concept of connectivity management. This area is for further study.

7.1.2.6 Architectural rules for logical separation of Session, Bearer and Service Control

The solution shall comply with the architectural rules relating to separation of bearer level, session control level, and service level expressed in TS 123 221 [8].

TIPHON is fully compliant with this requirement and has specified functions in architecture that logically differentiate between the Call, Bearer and Service Control, along with several other logical planes.

7.1.3 Session path information

IMS has identified the need to store the session paths. A Session Paths is determined during the session initiation request in order to route the subsequent session requests through this determined path. This is needed in order to route these session requests through certain nodes, e.g. the ones performing Service Control.

The use of session path capability is implicit in TIPHON architecture. It is a state-full architecture that requires all the relevant nodes in the path of initial session request to be informed of any subsequent information flow. This behaviour satisfies the above requirement.

7.1.4 End user preferences and user terminal capabilities

Due to different capabilities of the originating and terminating terminals, it might not be possible to establish all the media suggested by the originator for a particular session. In addition, the destination user may have different preferences of type of media depending on who is originating and on the situation e.g. being in a meeting or driving the car etc. The detailed examples of user preferences and terminal capabilities are given in TS 123 228 [2], and include preferences for media type, QoS, outgoing calls, incoming calls.

TIPHON has not yet included the user preferences or terminal capabilities in releases up to Release 4. This area is for further study.

7.1.5 Mechanism for bearer establishment

This mechanism refers to the pre-alerting capability that IMS has specified. Pre-alerting allows the called party to choose the media streams and codecs before the PDP context is established, and resources are reserved for a call. This helps to preserve these resources in the case where the called party cannot support the requested bearer capabilities.

The concept of pre-alerting is may be supported in TIPHON as it is an implementation option.

7.1.6 Numbering and addressing

IMS mandates the use of SIP URLs to identify IMS related network nodes such as I, P, S-CSCF, MGCF and BGCF.

TIPHON does not mandate the use of a particular addressing technology for use inside a network domain to identify network nodes, and can support SIP URLs, along with other identification mechanisms.

IMS requires the support for ITU-T Recommendation E.164 and SIP URLs to identify and address users. Whilst TIIPHON only supports E.164 (in Release 4), non-E.164 based User Names need to be supported.

7.1.7 Address resolution

IMS requires the support to translate the E.164 address contained in a Request-URI in the non-SIP URL "tel:" format to a SIP routable SIP URL using an ENUM DNS translation mechanism with the format as specified in RFC 2916 [9], (E.164 number and DNS). If this translation fails, then the session may be routed to the PSTN or appropriate notification shall be sent to the mobile.

TIPHON does not support the use of the ENUM translation service.

7.1.8 Conclusion

TIPHON supports most of the general IMS requirements related to session control. There are some differences to note. IMS requires resource negotiation before alerting the user, which is not supported explicitly in TIPHON. TIPHON has not shown the support for charging and reverse charging capabilities explicitly. However, it is believed that TIPHON has developed most of the capabilities required to achieve charging related services.

TIPHON has not developed the concept of connectivity management at transport level. This is useful, e.g. when a user is disconnected from the transport network whilst in a session, to inform the serving SpoA to take appropriate actions. This capability should be considered in the subsequent release of TIPHON.

TIPHON has mainly concentrated on telephony service until Release 4, and does not support the use of "terminal capabilities" and "user preferences". This should be considered in subsequent release when TIPHON supports the multimedia services, in line with IMS.

TIPHON does not support the ENUM service for address resolution which IMS does. TIPHON should clarify the address resolution scheme to translate E.164 addresses to other formats including URLs.

7.2 Quality of Service (QoS)

7.2.1 Support for End-to-End QoS

TIPHON requires and specifies a mechanism to support QoS End-to-End (E2E). E2E in TIPHON context means from user to user, whether the users are in the same domain or in different domains.

UMTS also requires the QoS to be supported on the E2E basis. The E2E in UMTS context is user to user if in the same domain, or user to border gateway if the session traverses out of the user's domain. The QoS support for external bearer services is out of scope of UMTS QoS architecture.

7.2.2 QoS Class

TIPHON has specified three QoS classes, which are based on three performance matrix TS 101 329-2 [10]. These matrix are:

- Over all Transmission Quality rating (R).
- Listener Speech Quality (one way non interactive speech quality).
- End-to-End (mean one way) delay.

The TIPHON QoS classes of service based on the above matrix are:

- Class 1: best effort.
- Class 2: 3 sub classes:
  - 2A: Acceptable.
  - 2M: Medium.
  - 2H: High.
- Class 3: Best (broadband).

UMTS has specified four QoS classes of service for UMTS bearer service (TS 123 107 [11]), which are:

- Conversational class.
- Streaming class.
- Interactive class.
- Background class.

The UMTS QoS classes have not been classified in the same way as TIPHON. The UMTS QoS classes are defined for different traffic types carried over UMTS bearer service. Examples of applications carried over different UMTS classes are telephony, web access, email download. All TIPHON QoS classes are currently defined for telephony only. Therefore, all the three TIPHON QoS classes would fall in the Conversational class of UMTS.

The main distinguishing factor within the TIPHON and UMTS QoS classes is how delay and error/packet loss sensitive the traffic is. In UMTS, the conversational class is meant for traffic which is very delay sensitive while Background class is the most delay insensitive traffic class. In TIPHON, speech quality (minimum packet loss) is also considered in addition to E2E delay.

A comparison of TIPHON and UMTS QoS classes for delay is provided in tables 2 and 3

Table 2: Boundary conditions for TIPHON QoS classes

	3 (WIDEBAND)	**2 (NARROWBAND)**			**1 (BEST EFFORT)**
		2H (HIGH)	**2M (MEDIUM)**	**2A (ACCEPTABLE)**	
End-to-end Delay	< 100 ms	< 100 ms	< 150 ms	< 400 ms	< 400 ms
NOTE: The delay for best effort class is a target value.					

Table 3: Boundary condition for UMTS traffic classes

Class	**Conversational**	**Streaming**	**Interactive**	**Background**
Delay	< 100 ms	< 250 ms	Not defined	Not defined

7.2.3 The QoS requirements for an IM CN subsystem session

The selection, deployment, initiation and termination of QoS signalling and resource allocation shall consider the following requirements so as to guarantee the QoS requirement associated with an IM CN subsystem session.

7.2.3.1 Independence between QoS signalling and session control

The selection of QoS signalling and resource allocation schemes should be independent of the selected session control protocols. This allows for independent evolution of QoS control and the session control in the IM CN subsystem.

The TIPHON QoS signalling is specified at the meta-protocol level so is, by definition, independent of session control protocols.

7.2.3.2 Necessity for end-to-end QoS signalling and resource allocation

End-to-end QoS indication, negotiation and resource allocation during the session set-up in the IM CN subsystem should be enforced for those services and applications that require QoS better than best-effort services or the Background QoS Class.

TIPHON QoS signalling is specified as an end-to-end meta-protocol.

7.2.3.3 QoS signalling at different Bearer Service control levels

During the session set-up in a IM CN subsystem, at least two levels of QoS signalling/negotiation and resource allocation should be included in selecting and setting up an appropriate bearer for the session.

7.2.3.3.1 The QoS signalling/negotiation and resource allocation at the IP Bearer Service (BS) level

The QoS signalling and control at IP BS level is to pass and map the QoS requirements at the IP Multimedia application level to the UMTS BS level and performs any required end-to-end QoS signalling by inter-working with the external network. The IP BS Manager at the UE and the GGSN is the functional entity to process the QoS signalling at the IP BS level.

TIPHON QoS keeps the application level distinct from the transport level and there is communication vertically to pass QoS requirements downwards, as well as horizontally to inform the next node of the QoS requirements.

7.2.3.3.2 The QoS signalling/negotiation and resource allocation at the UMTS Bearer Service level

The QoS signalling at the UMTS BS Level is to deliver the QoS requirements from the UE to the RAN, the CN, and the IP BS manager, where appropriate QoS negotiation and resource allocation are activated accordingly. When UMTS QoS negotiation mechanisms are used to negotiate end-to-end QoS, the translation function in the GGSN shall co-ordinate resource allocation between UMTS BS Manager and the IP BS Manager.

QoS negotiation takes place at the application level in a TIPHON system, not in the transport plane. That is not to say that there is not QoS related signalling in transport but it is purely related to setting up transport connections with particular QoS parameters.

7.2.3.3.3 QoS signalling interaction

Interactions (QoS class selection, mapping, translation as well as reporting of resource allocation) between the QoS signalling/control at the IP BS Level and the UMTS BS Level take place at the UE and the GGSN which also serve as the interaction points between the IM CN subsystem session control and the UMTS Bearer QoS control.

UMTS specific QoS signalling, negotiation and resource allocation mechanisms (e.g. RAB QoS negotiation and PDP Context set-up) shall be used at the UMTS BS Level. Other QoS signalling mechanisms such as RSVP at the IP BS Level shall only be used at the IP BS Level.

This is not precluded by TIPHON.

7.2.3.3.4 Aggregate bearer

It shall be possible to negotiate a single resource allocation at the UMTS Bearer Service Level and utilize it for multiple sessions at the IP Bearer Service level.

Currently, the meta-protocol assumes that that QoS is established on a call-by-call basis but there is no reason why the UMTS approach (QoS allocation for multiple sessions) could not be mapped onto the meta-protocol.

7.2.3.4 Restricted resource access at the IP BS level

Access to the resources and provisioning of QoS at IP BS Level should be authenticated and authorized by applying appropriate QoS policies via the IP Policy Control element.

In the TIPHON QoS model, the policy control element is in the application layer and supports this requirement.

7.2.3.5 Restricted resource access at the UMTS BS level

Access to the resources and provisioning of QoS at the UMTS BS Level should be authenticated and authorized by using existing UMTS registration/security/QoS policy control mechanisms.

This can be done through the QoS Policy control unit or by separate use of the security service capabilities.

7.2.3.6 Co-ordination between session control and QoS signalling/resource allocation

- In establishing an IMS session, it shall be possible for an application to request that the resources needed for bearer establishment be successfully allocated before the destination user is alerted.
  - This is implicit in the TIPHON QoS model as the call will not reach the destination if the en route resources are not available.
- In establishing an IMS session, it shall be possible, dependent on the application being offered, to prevent the use of the bearer until the session establishment is completed.
  - The TIPHON meta-protocol assumes that resources can be reserved during the initial stages of call setup and then either connected or discarded on successful or unsuccessful completion of the setup request.
- In establishing an IMS session, it shall be possible for a terminating application to allow the destination user to participate in determining which bearers shall be established.
  - To the extent that the terminating application can make the final selection of the codec to be used (assuming there is still more than one codec in the received list), this requirement is met in TIPHON. However, there is no explicit negotiation between the originating and terminating applications on the bearers to be used.
- Successful bearer establishment shall include the completion of any required end-to-end QoS signalling, negotiation and resource allocation
  - This requirement and is supported in the TIPHON model.

The initiation of any required end-to-end QoS signalling, negotiation and resource allocation processes at different network segments shall take place after the initiation and delivery of a session set-up request.

TIPHON QoS signalling is based on a parallel setup model i.e., the QoS negotiation and allocation takes place in parallel with the basic call setup. The difference between IMS and TIPHON exists because IMS supports pre-alerting allowing a destination application to indicate if it can support the bearer requirements such as codec. Pre-alerting is not supported in TIPHON, hence only the parallel setup model is supported.

7.2.3.7 The efficiency of QoS signalling and resource allocation

The sequence of end-to-end QoS signalling, negotiation and resource allocation processes at different network segments should primarily consider the delay in negotiating end-to-end QoS and reserving resources that contributes to the session set-up delay. Parallel or overlapping QoS negotiation and resource reservation shall be allowed where possible.

TIPHON supports the parallel QoS reservation model.

7.2.3.8 Dynamic QoS negotiation and resource allocation

Changes (upgrading or downgrading) of QoS provided to an active IMS session shall be supported based on either the request from the IM application or the current network loads or radio link quality.

In theory, this should be possible in TIPHON but Release 4 ties QoS signalling closely to Simple Call. This can be broken into a number of Service Capabilities which can be used at any time to modify QoS settings, in subsequent TIPHON releases.

It shall be possible to maintain a resource allocation in excess of the resources needed for current media flows (but within the restrictions imposed by clauses 7.2.3.4 and 7.2.3.5), in order to e.g. switch to different media flow characteristics without risk of admission control failure.

This is a network resource issue and it should not affect (or affected by) the QoS signalling model.

7.2.3.9 Prevention of theft of service

The possibility for theft of service in the IM CN subsystem shall be no higher than that for the corresponding GPRS and circuit switched services.

This requirement has no direct relation with the QoS model.

7.2.3.10 Prevention of denial of service

The system unavailability due to denial of service attacks in the IM CN subsystem shall be no greater than that for the corresponding GPRS and circuit switched services.

This requirement has no direct relation with the QoS model.

7.2.4 Bearer interworking concepts

Voice bearers from one domain need to be connected with the voice bearers to other domains. IMS has identified elements such as Media Gateway Functions (MGW) to support such bearer interworking. One of the functions of the MGW may be to support transcoding between a codec used by the UE in the IM CN subsystem and the codec being used in the network of the other party.

TIPHON supports the concept of bearer interworking. It has developed a Media Control (MC), function to perform transcoding from one media format to another.

7.2.5 Interaction between QoS and session signalling

IMS has specified capabilities and procedures that ensure admission control for traffic flow in the transport network, based on the interaction between the QoS and Session Control signalling. The GGSN contains a Policy Enforcement Function (PEF) that has the capability of policing packet flow into the IP network, and restricting the set of IP destinations that may be reached from/through a PDP context according to a packet classifier. This service-based policy "gate" function has an external control interface that allows it to be selectively "opened" or "closed" on the basis of IP destination address and port. When open, the gate allows packets to pass through (to the destination specified in the classifier) and when closed, no packets are allowed to pass through. The control is performed by a PDF, which is a logical entity of the P-CSCF.

NOTE: If the PDF is implemented in a separate physical node, the interface between the PDF and the P-CSCF is not standardized.

There are eight interactions defined for service-based local policy:

1) Authorize QoS Resources.

2) Resource Reservation with Service-based Local Policy.

3) Approval of QoS Commit for resources authorized in (1), e.g. "open" the "gate".

4) Removal of QoS Commit for resources authorized in (1), e.g. "close" the "gate".

5) Revoke Authorization for GPRS and IP resources.

6) Indication of PDP Context Release from the GGSN to the PDF.

7) Authorization of PDP Context Modification

8) Indication of PDP Context Modification from the GGSN to the PDF.

The first five of the interactions are relevant to the comparison between IMS and TIPHON and will be discussed further.

7.2.5.1 Authorize QoS resources

The Authorize QoS Resources procedure is used during an establishment of a SIP session. The P-CSCF(PDF) uses the SDP contained in the SIP signalling to calculate the proper authorization. The PDF authorizes the required QoS resources to GGSN.

7.2.5.2 Resource Reservation with Service-based Local Policy

The GGSN serves as the Policy Enforcement Point that implements the policy decisions for performing admission control and authorizing the GPRS and IP BS QoS Resource request, and policing IP flows entering the external IP network. Resource reservation is done at the GGSN based on the information provided by PDF in interaction in clause 7.2.5 (1).

7.2.5.3 Approval of QoS Commit for resources authorized in clause 7.2.5 (1)

The PDF makes policy decisions and provides an indication to the GGSN that the user is now allowed to use the allocated QoS resources for per-session authorizations

7.2.5.4 Removal of QoS Commit for resources authorized in clause 7.2.5 (1)

The PDF makes policy decisions and provides an indication to the GGSN about revoking the user's capacity to use the allocated QoS resources for per-session authorizations. Removal of QoS Commit for GPRS and IP resources shall be sent as a separate decision to the GGSN corresponding to the previous "Approval of QoS commit" request.

7.2.5.5 Revoke Authorization for GPRS and IP resources

At IP multimedia session release, the UE should deactivate the PDP context(s) used for the IP multimedia session. In various cases, such as loss of signal from the mobile, the UE will be unable to perform this release itself. The Policy Decision Function provides indication to the GGSN when the resources previous authorized, and possibly allocated by the UE, are to be released. The GGSN shall deactivate the PDP context used for the IP multimedia session.

TIPHON model contains functions such as CC and ICF that support the admission control, and allows for transport resources to be provided only to authorized users. The behaviour related to authorization, reservation, approval, removal, and revocation of resources is covered in TS 101 885 [12] and TS 101 882-2 [17].

7.2.6 QoS assured precondition

IMS has developed the concept of precondition, which is a set of constraints about the session, which are introduced during the session initiation. The recipient of the session generates an answer, but does not alert the user or otherwise proceed with session establishment until the preconditions are met. This can be known through a local event (such as a confirmation of a resource reservation), or through a new set of constraints sent by the caller. This concept is introduced in IMS so as to preserve the much valued radio interface.

A "QoS-Assured" session will not complete until required resources have been allocated to the session. In a QoS-Assured session, the UE must succeed in establishing the QoS bearer for the media stream according to the QoS preconditions defined at the session level before it may indicate a successful response to complete the session and alert the other end point.

The concept of pre-condition is not supported in TIPHON.

7.2.7 Codec and media flow negotiation

UMTS IMS allows a user to negotiate and renegotiate media and bearer capabilities. The session initiator includes an SDP in the SIP INVITE message that lists every codec that the originator is willing to support for this session. The list of codecs may be reduced by the network entities due to the network policies. When the message arrives at the destination endpoint, it responds with the subset that it is also willing to support for the session. Media authorization is performed for this common subset by the serving CSCF. The session initiator, upon receiving the common subset, determines the codec (or set of codecs) to be used initially.

Bearer negotiation and renegotiation in TIPHON is based on the session initiator sending a list of codecs in the bearer setup message that it is willing to support. The codec list is ordered in preference of the session initiator. This means that the single codec chosen by the destination should be the one most favoured by the initiator. The process is effectively the same as IMS.

7.2.8 Conclusion

The following conclusions and recommendation have been drawn from the comparison of QoS models.

The meaning of E2E in TIPHON and UMTS is not the same. TIPHON requires that sessions be supported for the required QoS through all the transit domains. This ensures that the QoS is maintained E2E, and not just in part. UMTS may rely on SLAs with adjacent domains to provide a certain level of QoS. TIPHON should consider the scenario where application level signalling cannot be used to request the required QoS for a session, and its impact on a session.

Currently, all the TIPHON QoS classes fall in the Conversational Class of UMTS. There may be scenarios in TIPHON Release 5 where media types other than telephony are used. For such cases, additional QoS classes may be useful to support traffic types such as Interactive or streaming media types.

There is a difference in approach between TIPHON and UMTS IMS for performing bearer negotiation: UMTS uses a three stage codec negotiation, whereas, TIPHON uses a two stage codec selection. The UMTS approach allows more flexibility for the users to select the codecs, whereas, TIPHON restricts the codec negotiation to one. However, the UMTS approach requires a higher degree of negotiation management than TIPHON, due to the flexibility, whereas, TIPHON approach simplifies the call set up and management. This difference in approach on deciding which codec to use will not have an affect on the harmonization of TIPHON and IMS.

TIPHON does not support the concepts of "assured-QoS" and "pre-condition". Both these capabilities require a change in behaviour of a TIPHON terminal. This area is for further study.

7.3 Event and information distribution

IMS requires that the S-CSCF and Application Servers (SIP-AS, IM-SSF, OSA-SCS) shall be able to send service information messages to endpoints. This should be done based on a SIP Request/Response information exchange containing the service information and/or a list of URI(s) pointing to the location of information represented in other media formats. The stimulus for initiating the service event related information message may come from e.g. a service logic residing in an application server.

In addition, the end points should also be able to send information to each other. This information shall be delivered using SIP based messages. The corresponding SIP messages shall be forwarded along the IMS SIP signalling path. This includes the S-CSCF but may also include SIP application servers. The information may be related or unrelated to any ongoing session and/or may be independent of any session. Applicable mechanisms (for e.g. routing, security, charging, etc) defined for IMS SIP sessions shall also be applied for the SIP based messages delivering the end-point information. The length of the information transferred is restricted by the message size (e.g. the MTU), so fragmentation and re-assembly of the information is not required to be supported in the UE. This information may include e.g. text message, http url, etc.

TIPHON has developed service capabilities in 'Message' class in Release 4. These capabilities include the ability to set events, and send notifications between functions that support this capability. This capability supports information flow between network elements, user to network and network to user. It does not support user to user signalling and messaging at this stage. This should be introduced in subsequent release.

7.4 Signalling and protocol

TIPHON has identified several reference points on its architecture (figure 1) that help establish a relationship between different functions. Protocols can be mapped on these reference points to transfer information from one function to another, and provide services across different functions. The 'C' reference point is used for Call Control signalling and can be mapped to H.323 suite of protocols, SIP and ISUP etc. Similarly 'R' reference point supports the registration service and can be mapped to different protocols supporting registration. 3GPP IMS has adopted SIP as the protocol of choice for session management. TIPHON has also developed a SIP profile based on mapping SIP to TIPHON Call Control Meta-Protocol. The main capabilities between TIPHON and IMS session control are compared in Annex B. This clause compares the context and behaviour of SIP protocol in IMS and TIPHON.

7.4.1 Comparison between TIPHON and IMS SIP protocol

The detailed comparison between TIPHON and IMS SIP is given in annex B. The analysis of the comparison shows that there is a big gap between the capabilities supported by TIPHON and IMS SIP protocols. IMS has a lot more capabilities than TIPHON. The main reason for this gap is the type of services supported by both the IMS and TIPHON: TIPHON supports mainly telephony (until Release 4), whereas, IMS supports many more services in addition to telephony, including multimedia, messaging and data transfer services.

7.4.2 Inter-connecting with other systems

Both the TIPHON and IMS can interconnect with other network systems and each other via a Call Control protocol interconnection. In the case of IMS, interworking is performed via SIP, whereas, in the case of TIPHON it could be SIP, H.323, ISUP or BICC. The interworking between TIPHON and IMS will take place via a call control gateway, such as a SIP gateway, that will interconnect a TIPHON domain to an IMS domain. The interconnect capabilities of SIP will be subject to either the national regulations or SLA between the interconnecting network operators.

7.4.3 Conclusion

Several gaps have been identified in comparison between TIPHON and IMS SIP annex B. When the TIPHON is enhanced with the multimedia service in Release 5, it should adopt the capabilities identified as missing in annex B. These enhancements in the SIP protocol should also be reflected in the Call Control Meta-protocol.

8 Services and service capabilities

TIPHON specifies service capabilities, and not services. The philosophy behind this approach is that any of the parties involved in providing services can develop services from the service capabilities. The service capabilities can be used to develop standardized services or unique services. The services developed from TIPHON service capabilities can be deployed on any underlying technologies including circuit switched or packet switched networks.

The UMTS framework is divided into two domains: Circuit switched domain, and Packet switched domain. The circuit switched domain has inherited most of the supplementary services introduced in the 2nd generation GSM systems. UMTS has also agreed not to standardize any more services, instead service capabilities will be standardized which will allow for unique and value added service to be developed. The initiative to develop service capabilities is mainly related to the APIs based on OSA that can be used to develop and provide value added services either by the service provider or a 3rd party service provider.

UMTS has also defined a subsystem in the PS domain, called the IMS. It is an IP based multimedia system which utilizes the transport technologies in the access and core networks provided by the UMTS, and serves as an application plane to support user specific services. IMS supports several IP based services including telephony, and supports SIP for this purpose. IMS has also identified a set of capabilities that will be supported in UMTS Release 5 and Release 6.

8.1 Comparison of terminology

Both TIPHON and 3GPP share a number of common terms including "Service" and "Service Capability". However, although "Services" are similar, "Service Capabilities" have different definitions. This clause identifies the differences in terminology and provides a mapping between the two.

8.1.1 3GPP Terminology

In 3GPP documents the following relationships between services and service capabilities are defined:

- **Services:** Services are made up of different service capability features (TS 122 105 [18]).
- **Service Capabilities:** Bearers defined by parameters, and/or mechanisms needed to realize services. These are within networks and under network control (TS 122 105 [18]).
- **Service Capability Feature:** Functionality offered by service capabilities that are accessible via the standardized application interface (TS 122 105 [18]).

- **Services Capability Features:** are open, technology independent building blocks accessible via a standardized application interface. This interface shall be applicable for a number of different business and applications domains (including besides the telecommunication network operators also service provider, third party service providers acting as HE-VASPs, etc.) (TR 122 121 [19]).

IP multimedia applications shall, as a principle, not be standardized, allowing operator specific variations. It shall be possible to enable rapid service creation and deployment using service capabilities.

To date, the only service capability features in 3GPP have been defined for use at of Open Services Access (OSA) Interface.

8.1.2 TIPHON Terminology

TIPHON have chosen UML notation to describe Service Capabilities. In TIPHON Documents the following relationships between services and service capabilities are defined (TS 101 878 [7]) as follows:

- **Service:** set of telecommunication related tasks performed for a customer by a Service Provider and supplied in a business context.

- **Service Capability:** specified set of functionalities that are used to provide a component part of a service application.

8.2 Comparison of terms and concepts

Both 3GPP and TIPHON provide for the creation of non-standard services. Both 3GPP and TIPHON aim to support Service Providers ability to create services from standardized building blocks. However the building blocks in 3GPP are Service Capability Features but in TIPHON are Service Capabilities.

It should be noted however that the granularity adopted for in 3GPP for Service Capability Features and in TIPHON for Service Capabilities are different.

Service Capability Features are larger, more course grained, blocks of functionality.

The 3GPP service capabilities and features are developed as OSA which is based on Parlay APIs. TIPHON has developed its own methodology to develop its service capabilities, and although it is not the same as 3GPP, it is similar. The service capability features developed by 3GPP and service capability classes developed by TIPHON are listed below. A mapping of TIPHON classes to OSA Capability features is also provided where applicable.

Table 4: Comparison of TIPHON and OSA service capabilities

3GPP OSA capability features	TIPHON Service capabilities classes
Call Control	Call, Bearer, Media
User Interaction SCF	
Mobility SCF	Profile
Terminal Capabilities SCF	
Data Session Control SCF	
Generic Messaging SCF	Messaging
Connectivity Manager SCF	
Account Management SCF	
Charging SCF	
Policy Management SCF	
Presence and Availability Management SCF	Profile

8.3 Enhanced IMS services

In addition to the OSA service capabilities and those described in clause 7, 3GPP has developed a set of services specific to IMS. These services are referred to as 'Enhanced Multimedia Services'. This clause describes these enhanced services and provides a comparison with TIPHON.

8.3.1 Session Hold and Resume

IMS requires the support for placing sessions on hold that are established, and resuming the session afterwards. Two cases are presented:

- mobile-to-mobile (UE-UE); and
- a UE-initiated hold of a UE-PSTN session.

For a multi-media session, it shall be possible to place a subset of the media streams on hold while maintaining the others.

TIPHON has the capabilities under the Call and Bearer Classes to support the session hold and resume that cover both the cases identified by IMS. However, TIPHON has not yet specified this service for session that has more than one media flows/bearers. This may be specified in the next TIPHON release.

8.3.2 Anonymous session establishment

IMS requires the support for anonymous session establishment. However, sessions are not intended to be anonymous to the originating or terminating network operators.

TIPHON supports this service using Call class, and has specified the signalling flows for this service. In addition to anonymity at session (application) level, TIPHON has specified anonymity at transport level too.

8.3.3 Codec and media negotiation

Covered in clause 7.2.7.

8.3.4 Providing or blocking user identity

IMS requires the support for providing or blocking the authenticated public user identity and the optional display Name information of the originating party to the terminating party, if requested by the originating party.

TIPHON supports this service.

8.3.5 Session Redirection services

IMS requires the support for session redirection services. The decision to redirect a session to a different destination may be made for different reasons by a number of different functional elements, and at different points in the establishment of the session.

Three cases of session redirection prior to bearer establishment are considered, as well as the case of session redirection after bearer establishment. These cases enable the typical services of "Session Forward Unconditional", "Session Forward Busy", "Session Forward Variable", "Selective Session Forwarding", and "Session Forward No Answer", though it is important to recognize that the implementation is significantly different from the counterparts in the CS domain.

TIPHON supports the session redirect services with a combination of "Profile", "Call" and "Bearer" Classes. Different flavours of session redirect supported include blind and assured transfer, as well as a three-way session. Note that the cumulative transfer (TS 123 228 [2]) is not supported.

8.3.6 Emergency session

IMS Release 5 does not require the support for emergency services. It is expected that this will be required in subsequent releases.

TIPHON supports the emergency services.

8.4 Comparison of General Capabilities

This clause identifies the general capabilities applicable to both the CS and PS domains of UMTS and their support in TIPHON.

Table 5: Comparison of General Capabilities

UMTS Service	TIPHON Releases 3 and 4
Location Services (LCS)	PS
Presence service	PS
Push service	S
New events for triggered location reports	N
Generic user profile	PS (see clause 6.3)
Priority service	S
Enhanced emergency call	PS
Lawful Interception	PS

8.5 Supplementary Services (SS)

In addition to the above listed services, TIPHON supports a large set of supplementary services. Those service which are relevant to UMTS are listed below, along with the indication whether or not they are supported by TIPHON.

Table 6: Supplementary Services supported by TIPHON and UMTS

3GPP Service	TIPHON Releases 3 and 4
Advanced addressing	S
Advice of Charge (AoC) supplementary services	S
Automatic establishment of roaming relationships	S
Basic Call Handling	S
Broadcast and multicast services	NS
Call Barring (CB)	S
Call Deflection (CD)	S
Call Forwarding (CF)	S
Call Waiting (CW) and Call Hold (HOLD)	S
Cell Broadcast Service (CBS)	NS
Charge Advice Information (CAI)	NS
Closed User Group (CUG)	S
Completion of Calls to Busy Subscriber (CCBS)	S
Dual Tone Multi Frequency (DTMF) signalling	S
Enhanced Multi-Level Precedence and Pre-emption service (eMLPP)	PS (see note 1)
Enhanced support for user privacy in Location Services (LCS)	NS
Explicit Call Transfer (ECT)	S
Facsimile Group 3 service	S
Follow Me Service	S
Global text telephony	NS
Mobile Number Portability (MNP)	S
Line Identification supplementary services	S
Multicall supplementary service	S
MultiParty (MPTY) service	S
Multiple Subscriber Profile (MSP)	NS
Name identification supplementary services	NS
Network Identity and Time Zone (NITZ)	NS
Numbering, addressing and identities	S
Operator Determined Barring (ODB)	S
Support Optimal Routeing (SOR)	S
Quality of Service (QoS) and network performance	(see note 2)
Routeing of calls to/from Public Data Networks (PDN) and the GSM Public Land Mobile Network (PLMN)	S
Security Mechanisms	S
P-P Message Service	NS
Teletex	NS

3GPP Service	TIPHON Releases 3 and 4
User-to-User Signalling (UUS)	PS
Videotex	NS
Virtual Home Environment	S
Voice Broadcast Service (VBS)	NS
NOTE 1: Yes for MLP; No for pre-emption. NOTE 2: Yes but different.	

8.6 Conclusion

The principles adopted by TIPHON and 3GPP IMS to define service capabilities and not standardized services are the same, although the granularity of the capabilities themselves is somewhat different. There are opportunities for alignment of service capabilities to facilitate the production of services by service providers which can be deployed and interwork with either technology.

However, 3GPP have developed a few services specific to the IMS including session hold and resume, anonymous session establishment, providing or blocking user identity and session redirection. The TIPHON Release 4 service capabilities may need to be modified if these services or service features need to be realized.

The services that have been standardized by 3GPP for the CN has been used as the basis for a service set that may be applicable to TIPHON or 3GPP IMS. It is shown from this analysis that there are some general capabilities e.g. location service, presence service and some supplementary services that are not fully supportable by TIPHON Release 4 capabilities. These additional requirements are being addressed in TS 102 283 [16].

9 Security

9.1 General

In the security area both UMTS (as developed within the 3rd Generation Partnership Project (3GPP)) and TIPHON have been designed with a view to achieving compliance to the following objectives:

a) to ensure that information generated by or relating to a user is adequately protected against misuse or misappropriation;

b) to ensure that the resources and services provided by serving and home functional groups are adequately protected against misuse or misappropriation;

c) to ensure that the security features standardized are compatible with world-wide availability (i.e. there should be at least one ciphering algorithm that can be exported on a world-wide basis (in accordance with the Wassenaar agreement 2 (see bibliography));

d) to ensure that the security features are adequately standardized to ensure world-wide interoperability between different serving functional groups;

e) to ensure that the implementation of security features and mechanisms can be extended and enhanced as required by new threats and services.

The basic security features employed in existing fixed and mobile systems will be retained, or, where needed, enhanced. These include:

- subscriber authentication;
- encryption;
- subscriber identity confidentiality;
- use of removable subscriber module;
- secure application layer channel between subscriber module and home network;

- transparency of security features;
- minimized need for trust between home and serving functional groups.

The above objectives together can be met by provision of methods to achieve the following goals:

- Confidentiality:
    - The avoidance of the disclosure of information without the permission of its owner.
- Integrity:
    - The property that data has not been altered or destroyed in an unauthorized manner.
- Accountability:
    - The principle whereby individuals are held responsible for the effect of any of their actions that might lead to a violation.
- Availability:
    - The property of being accessible and usable upon demand by an authorized entity.
- Non-repudiation:
    - A property by which one of the entities or parties in a communication cannot deny having participated in the whole or part of the communication.

In addition the areas of concerns outlined in the succeeding clauses have been addressed equally in UMTS and in TIPHON.

9.1.1 Privacy

Privacy legislation is of increasing importance; there are strong restrictions in many countries with regard to storage and visibility of data. Therefore, when offering a service within UMTS or TIPHON, or when designing data processing functions and defining the kind of data being generated or stored within UMTS or TIPHON systems, UMTS and TIPHON service providers shall consider the relevant national data protection laws.

The definition of privacy includes:

- privacy of information: keeping information exchanged between service functions away from third parties;
- limitations on collection, storage and processing of personal data: personal data may only be collected, stored and processed if there is a relationship between the data and the actual provision of services;
- disclosure: the obligation of a network and service providers to keep information concerning customers away from third parties;
- inspection and correction: the right of the customer to inspect and correct information about himself stored by the service and/or network provider.

Privacy legislation will mostly concern the security objectives regarding "data confidentiality" and "data integrity". For UMTS and TIPHON special concern in this respect shall be paid to the contents of personal data in the UMTS/TIPHON service profile. These data and the access conditions to it for the service provider's personnel, the subscriber and the user himself shall be limited, in accordance with the relevant European guidelines and national laws.

9.1.2 Security order

National laws concerning the security order:

- demand proper protection of information and infrastructure to ensure the availability and the integrity of the telecommunication network;
- may restrict the usage of cryptographic methods.

This legislation will mostly concern the security objectives regarding "data confidentiality", "data integrity" and "availability".

9.1.3 Lawful Interception

Lawful interception means the obligation of the network operator to co-operate and provide information in case of criminal investigations (see TS 101 331 [13]).

This legislation will mostly influence the security objectives regarding "data confidentiality".

9.1.4 Contract

It shall be possible to use information concerning the contract for communication services between two entities in case of a dispute in a court of law.

This legislation will mostly influence the security objectives regarding "accountability" and "data integrity".

9.2 Threat analysis

Both UMTS and TIPHON have identified those areas of their systems most vulnerable to attack through the development of a threat analysis.

Here we describe the main threats but with the observation that only intentional non-physical threats are taken into account. The following threats are partly derived from ETR 336 [14]. These threats are:

- Masquerade ("spoofing"):
  - The pretence of an entity to be a different entity. This may be a basis for other threats like unauthorized access or forgery.
- Unauthorized access:
  - An entity accesses data in violation to the security policy in force.
- Eavesdropping:
  - A breach of confidentiality by unauthorized monitoring of communication.
- Loss or corruption of information:
  - The integrity of data (transferred) is compromised by unauthorized deletion, insertion, modification, reordering, replay or delay.
- Repudiation:
  - An entity involved in a communication exchange subsequently denies the fact.
- Forgery:
  - An entity fabricates information and claims that such information was received from another entity or sent to another entity.
- Denial of service:
  - An entity fails to perform its function or prevents other entities from performing their functions.

These threats counteract the identified main objectives as shown in table 7.

Table 7: Threats to security objectives

Threat	Objective			
	Confidentiality	**Integrity**	**Accountability**	**Availability**
Masquerade	X	X	X	X
Unauthorized access	X (within a system)	X (within a system)	X	X
Eavesdropping	X (on the line)			
Loss or corruption of information		X (on the line)	X	X
Repudiation			X	
Forgery		X	X	
Denial of service				X

9.2.1 Actors and roles

In both TIPHON and in UMTS only technical security countermeasures are considered, which means that relevant actors to consider are *TIPHON users* or *UMTS users*. The present document uses a TIPHON user as the example in the text but in all cases the UMTS user can be substituted. A TIPHON user is defined as a person or process using TIPHON in order to gain access to some TIPHON service. TIPHON users can further be categorized dependent on whether they belong to the organization running the TIPHON services (internal users) or whether they access the TIPHON services as external users.

Each time a TIPHON user accesses a TIPHON service, the TIPHON user will take on a role. In some cases there will be a one-to-one relationship between a TIPHON user and a role, i.e. the TIPHON user will always stay in the same role. In other cases there will be a one-to-many relationship between a specific TIPHON user and the possible roles the TIPHON user can play. This latter case is the normal TIPHON case in which the same user may act as a call initiator, call receiver, registrant, etc.

The following gives a high level classification of the most common roles:

- network operators (*private or public*);
- service providers (*Bearer Service Providers or Value Added Service Providers*);
- service subscribers/service customers;
- service end users;
- equipment/software vendors.

Some security measures may require actors to enforce the role of a Trusted Third Party (TTP). An important security issue is how these actors should be allowed to interact with TIPHON.

9.2.2 Security domains

A *security domain* is defined as a set of entities and parties that is subject to a single security policy and a single security administration. A security domain may encompass many functional domains as defined in TS 101 314 [1].

9.2.3 Threat analysis and risk assessment

The purpose of a threat analysis is to measure the risk to a system and ultimately it is the intention to design a system where the risk when countermeasures have been implemented that is low.

A potential threat is doing no harm unless there is a corresponding weakness in the system and until the point in time when a weakness is exploited by the intruder. Thus, the threats must be evaluated, i.e. it should be attempted to characterize them according to cost/effort involved (occurrence likelihood) and according to potential benefit/damage that can be done (impact value).

For the risk assessment, the occurrence likelihood of threats is estimated with values from "1" to "3". The meaning of a certain value associated to the occurrence likelihood of a particular threat is explained as follows.

Table 8: Occurrence likelihood

1	For "unlikely"	According to up-to-date knowledge, a possible attacker needs to solve strong technical difficulties to state the threat, or the motivation for an attacker is very low.
2	For "possible"	The technical requirements necessary to state this threat are not too high and seem to be solvable without big effort; furthermore, there must be a reasonable motivation for an attacker to perform the threat.
3	For "likely"	There are no sufficient mechanisms installed to counteract this threat, and the motivation for an attacker is quite high.

The impact of a threat is also estimated with values from "1" to "3". The meaning of a certain value associated to the impact is explained as follows.

Table 9: Impact

1	for "low impact"	The concerned party is not harmed very strongly; the possible damage is low.
2	for "medium impact"	The threat addresses the interests of providers/subscribers and cannot be neglected.
3	for "high impact"	A basis of business is threatened and severe damage might occur in this context.

The product of occurrence likelihood and impact value gives the risk which serves as a measurement for the risk that the concerned management function is compromised. The result is classified into the following three categories.

Table 10: Risk

1, 2, 3	for "minor risk"	Minor risks arise, if either no essential assets are concerned, or the respective attack is unlikely. Threats causing minor risks have no primary need for counter measures.
4	for "major risk"	Major risks are represented by threats on relevant assets which are likely to occur, even if their impact is less fatal. Major risks should be handled seriously and should be minimized as soon as possible.
6, 9	for "critical risk"	Critical risks arise, when the primary interests of the providers/subscribers are threatened and when a potential attacker's effort to harm these interests is not high. Critical risks shall be minimized with highest priority.
NOTE: The values 5, 7 and 8 cannot occur.		

9.3 Authentication mechanisms

The definitions of TIPHON and UMTS diverge very slightly in the use of authentication mechanisms. In both cases authentication is achieved by secret keying (symmetric) methods, with the UMTS methods going somewhat deeper into implementation using a variation of the AES (Rijndael) algorithm as the core mechanism.

TIPHON identifies a set of 7 authentication measures of which 6 are defined in TS 102 165-2 [15].

- Authentication:
  - A1 = Authentication of the terminal by the registrar (home of the user profile);
  - A2 = Authentication of the registrar by the terminal;
  - A3 = Authentication of the terminal by the Service point of Attachment (SpoA);
  - A4 = Authentication of the SpoA by the terminal;
  - A5 = Authentication of the SpoA by the registrar;
  - A6 = Authentication of the registrar by the SpoA;
  - A7 = Authentication of the User to the TIPHON terminal device.

The TIPHON countermeasures are broadly equivalent to those specified in UMTS (IMS) and may be implemented using the specific mechanisms of UMTS (IMS).

9.4 Authorization mechanisms

Both TIPHON and UMTS offer authorization mechanisms in which the right to access service is contained within the user profile. In practice this enforces access control and the broad outline of thee services in TIPHON are listed below:

- Access Control:
  - C1 = Access control to services;
  - C2 = Access control to data;
  - C3 = Access control to data in terminal;
  - C4 = Access control to software;
  - C5 = Access control to hardware.

In the UMTS (IMS) implementation post authorization access control requires opening of specific "pinholes" on gateway devices. TIPHON does not delve this deep.

9.5 Other security measures

Whilst authentication and access control are the most prevalent mechanisms TIPHON has also identified a set of additional measures that are required. In common with other measures the UMTS (IMS) systems provide further detail on the implementation of these measures.

- Confidentiality:
  - E1 = Confidentiality of user communication on the access interface (terminal to TpoA);
  - E2 = Confidentiality of signalling on the access interface (terminal to SpoA);
  - E3 = Confidentiality of signalling between SpoA entities;
  - E4 = Confidentiality of signalling between SpoA and TpoA;
  - E5 = Confidentiality of communication between transport domains;
  - E6 = Confidentiality of TIPHON-id on signalling interfaces;
  - E7 = Confidentiality of communication between SpoA and Registrar (registration services)
- Integrity:
  - I1 = Signalling data integrity;
  - I2 = Bulk data transfer data integrity.
- General Security Policy:
  - P1 = Bill limitations;
  - P2 = Secure billing administration;
  - P3 = Subscriber and terminal management;
  - P4 = Hotline;
  - P5 = Security related reports to the user;
  - P6 = Secure dialogue between operators;

- P7 = Contractual agreements between operators;
- P8 = Contractual agreements between service providers and subscribers;
- P9 = Security related reports to the service providers;
- P10 = Secure subscription process.

9.6 Topology hiding

In both TIPHON and UMTS specific details of the network topology are invisible to the user. However, UMTS IMS requires topology hiding of a domain to be supported to protect it from external entities. TIPHON does not explicitly support topology hiding: It is implicit in TIPHON.

9.7 Conclusion

The principles behind security frameworks in TIPHON and UMTS IMS are identical. The main differences between the two are limited to the implementation of these mechanisms. A more obvious difference is on the authentication algorithms: although the authentication mechanisms are similar, IMS mandates the use of digest authentication mechanism using MD5 algorithm for SIP, whereas, TIPHON has made no recommendation on algorithms.

Another area where TIPHON differs slightly with UMTS is of Topology Hiding. UMTS explicitly requires the topology of a domain be hidden from another domain, when, for example, call control signalling traverses from one domain to another. TIPHON has not made such an explicit requirement and considers this capability implicit, i.e. the information related to the topology of a domain will not traverse across to another domain. In order to fully harmonize with UMTS, TIPHON should consider to explain this capability explicitly in the relevant documents.

Access control to network resources is another area where TIPHON differs from UMTS. In UMTS, a separate PDP context is established for the media/bearer, which is different from the PDP context used for signalling. This ensures that only authorized media flows through the network. This is access control at the transport level, i.e. requires establishment of a transport connection between the user device and the serving node. In TIPHON, it is assumed that access to the transport network is already available. When a user requests bearer for a service, the request for bearer establishment is authorized by SpoA, and an authorization is sent to the ICF, which acts as the point of enforcement for access control, and opens and closes the pinholes allowing or barring traffic to flow through it. This access control is at Service level. Therefore, TIPHON should consider the capability to restrict access to transport network.

Annex A (informative): User Profile

A.1 Recommended Generic User Profile content (3GPP)

- General Information:
  - Not controlling functions.
  - General User Information (Name, address, age, sex, ID).
  - General Subscriber Information (Name, bill info, users).
- Capability description:
  - Describe capacity. Normally not settable.
  - Terminal capability.
  - User interface capabilities.
  - Communication capabilities.
  - Synchronization capabilities.
  - MExE capabilities.
  - WAP Browser capabilities.
- User's preferences:
  - User's "wishes". Sent to servers. Used for "content selection".
  - User interface preferences (language, event notifications, etc.).
  - Browser appearance (User's preference for displaying frames).
  - Preferred memory usage.
  - IPMM preferences.
  - User preferences (The preferred access technology, second preferred access technology, etc.).
- Parameters:
  - User interface (Ring volume, Vibrating alert, Ring signals, Melodies, Key sound).
  - WAP Parameters (Bookmarks; Gateway: Internet account, Gateway IP address, User ID, Password, Datamode, Security, Show images, Response timer).
  - User security policy (application download, ciphering, positioning).
  - User Security data (Secret keys, user name).
  - Supplementary Services settings.
  - IPMM settings (QoS profile, max nob sessions, roaming restrictions).
  - Identifiers/addresses/references (IMSI, IMEI, MSISDN, etc.).
  - User preferences (access technologies).

A.2 TIPHON user profile data

This clause presents the data that could be used for TIPHON user profile. This data has been gathered from different TIPHON documents. Note that this data has been presented in the form of 3GPP GUP, allowing a close alignment between the two. The data can, however, be organized in another format.

- General information:
    - Public ID:
        - Public name(s).
    - Private ID:
        - User Id with SP.
    - Subscription data.
    - Contact details.
    - Roaming user's address (new).
    - Terminal ID (to bind the capabilities with a terminal).
- Capability description [as in service (capabilities) offered]:
    - Registration.
    - Simple Call.
    - Number portability.
    - Terminal capabilities.
    - Addressing information (including address allocation and translation):
        - Binding information for private and public addresses.
        - Binding of internet addresses to E.164 addresses.
    - Billing/Accounting data.
- User preferences:
    - Subscribed services.
    - Authorized services (possibly includes service barring data).
    - Service availability.
    - QoS profile:
        - QoS subscribed.
        - QoS requested.
        - QoS promised/negotiated/provided.
    - Service Class (QoS profile).
    - Codecs related data (preference/order).
    - Alerting preferences (ring tone type - part of Release 4).
    - Privacy preferences: e.g. hide privacy for all calls.

- Parameters:
  - Domain/network ID.
  - Routing Information.
  - Forwarding number.
  - New address/destination number (for number portability).
  - Authentication info (provided in e.g. Register message; service request to SpoA).
  - Security information (Keys etc).
  - Duration of Registration.
  - Duration of Service availability.
  - Home service provider/Domain ID.
  - Serving service provider/Domain ID.
  - Home Registrar ID.
  - Serving Registrar ID.
  - Home SpoA ID.
  - Serving SpoA ID.
  - Media and service proxy Ids.
  - Location information.
  - User/Service priority.

Annex B (informative): Comparison of 3GPP IMS and TIPHON SIP

B.1 Comparison of SIP METHODS supported in IMS and TIPHON

NOTE: 3GPP specific extensions are referred to as 3GE.

Table B.1: Comparison of Methods supported by TIPHON and IMS SIP

Method	3GPP IMS	TIPHON	Comments
ACK	S	S	
BYE	S	S	
CANCEL	S	S	
COMET	S	NS	To be supported in Release 4
INFO	S	NS	To be supported in Release 4
INVITE	S	S	
NOTIFY	S	NS	To be supported in Releases 4 and 5
OPTIONS	S	S	
PRACK	S	NS	To be supported in Release 4
REFER	S	NS	To be supported in Release 4
REGISTER	S	S	
SUBSCRIBE	S	NS	Should be supported in Releases 4 and 5
UPDATE	S	NS	To be supported in Release 4

B.2 Comparison of HEADERS supported in IMS and TIPHON

Table B.2: Comparison of HEADERS supported in IMS and TIPHON

Header	3GPP IMS	TIPHON	Notes
Accept	S	S	
Accept Encoding	S	S	
Accept Language	S	S	
Alert Info	S	NS	This should be introduced in Release 4
Allow	S	NS	For Release 5
Allow-Events	S	NS	For Release 5
Anonymity	S	NS	This should be introduced in Release 4
Authentication Info	S	S	
Authorization	S	S	
Call-ID	S	S	
Call Info	S	NS	FFS
Contact	S	S	
Content-Disposition	S	NS	For Releases 4 and 5
Content-Encoding	S	NS	For Release 5
Content-Language	S	NS	For Release 5
Content-Length	S	S	
Content-Type	S	S	
Cseq	S	S	
Date	S	S	
Error Info	S	NS	Required in Release 4
Expires	S	S	
From	S	S	
In Reply To	S	NS	For Release 5
Max-Forwards	S	NS	Not required

Header	3GPP IMS	TIPHON	Notes
MIME-Version	S	NS	
Min-Expire	S	NS	Required in Release 4
Organization	S	NS	FFS
Priority	S	S	
Proxy Authenticate	S	S	
Proxy-Authorization	S	S	
Proxy Media Authorization	S	NS	Required in Release 4
Proxy-Require	S	NS	FFS
RAck	S	NS	Required in Release 4
Record Route	S	S	Although supported in TS 101 884 [20], Concept not supported in TIPHON
Remote Party Id	S	NS	FFS, May support this in Release 4
Reply To	S	NS	Required in Release 4. equivalent to return address for calling pty
Require	S	NS	FFS. Concept not supported in TIPHON
Retry After	S	NS	FFS. Concept not supported in TIPHON
Route	S	NS	Concept not supported in TIPHON
RSeq	S	NS	
Server	S	NS	To be supported in Releases 4 and 5
SIPFrag	S	NS	
Subject	S	NS	May be supported in Release 5
Subscription state	S	NS	To be supported in Releases 4 and 5
Supported	S	NS	See 'Require'
Timestamp	S	?	Required in Release 4
To	S	S	
Unsupported	S	NS	See 'Require'.
User-Agent	S	NS	To be supported in Releases 4 and 5
Via	S	S	
Warning	S	NS	FFS.
WWW Authenticate	S	S	
P-Called-Party-ID header	3GE		
P-Access-Network-Info header	3GE		
P-Visited-Network-ID header	3GE		This should be introduced in Release 4
P-Charging-Function-Addresses header	3GE		
P-Charging-Vector header	3GE		
P-Original-Dialog-ID header	3GE		
P-Service-Route header	3GE		This should be introduced in Release 4
P-Asserted-Identity header	3GE		This should be introduced in Release 4
NOTE: OSP header to be included in SIP.			

B.3 Comparison of response CODES supported by IMS and TIPHON SIP

Table B.3: Comparison of supported response CODES

Item	Header	Sending			Comments
		Profile status	RFC status	TIPHON status	
1	100 (Trying)	c1	c1	S	Release 4 will support '100Rel'.
2	180 (Ringing)	c3	c3	S	
3	181 (Call Is Being Forwarded)	c3	c3	NS	To be supported in Release 4
4	182 (Queued)	c3	c3	NS	FFS - may be required for ETS etc.
5	183 (Session Progress)	c3	c3	S	
6	200 (OK)			S	
7	202 (Accepted)	c4	c4	NS	
8	300 (Multiple Choices)			S	
9	301 (Moved Permanently)			S	
10	302 (Moved Temporarily)			S	
11	305 (Use Proxy)				FFS

Item	Header	Sending			Comments
		Profile status	RFC status	TIPHON status	
12	380 (Alternative Service)				FFS
13	400 (Bad Request)			S	
14	401 (Unauthorized)			S	
15	402 (Payment Required)			NS	
16	403 (Forbidden)			NS	
17	404 (Not Found)			S	
18	405 (Method Not Allowed)			NS	
19	406 (Not Acceptable)			S	
20	407 (Proxy Authentication Required)			NS	
21	408 (Request Timeout)			NS	
22	410 (Gone)			S	
23	413 (Request Entity Too Large)			NS	
24	414 (Request-URI Too Large)			NS	
25	415 (Unsupported Media Type)			NS	
26	416 (Unsupported URI Scheme)			S	
27	420 (Bad Extension)			NS	
28	421 (Extension Required)			NS	
29	423 (Registration Too Brief)	c5	c5	NS	
30	480 (Temporarily not available)			S	
31	481 (Call Leg/Transaction Does Not Exist)			NS	
32	482 (Loop Detected)			NS	
33	483 (Too Many Hops)			NS	
34	484 (Address Incomplete)			S	
35	485 (Ambiguous)			NS	
36	486 (Busy Here)			S	
37	487 (Request Cancelled)			NS	
38	488 (Not Acceptable Here)			NS	
39	489 (Bad Events)	c4	c4	NS	
40	491 (Request Pending)			NS	
41	493 (Undecipherable)			NS	
42	500 (Internal Server Error)			NS	
43	501 (Not Implemented)			NS	
44	502 (Bad Gateway)			NS	
45	503 (Service Unavailable)			S	
46	504 (Server Time-out)			NS	
47	505 (SIP Version not supported)			NS	
48	513 (Message Too Large)			NS	
49	580 (Precondition Failure)			NS	
50	600 (Busy Everywhere)			NS	
51	603 (Decline)			S	
52	604 (Does Not Exist Anywhere)			NS	
53	606 (Not Acceptable)			NS	

B.4 Comparison of CAPABILITIES supported by IMS SIP and TIPHON SIP

B.4.1 Comparison of capabilities of User Agent

Table B.4: Comparison of supported User Agent capabilities

Item	IMS Capabilities	RFC status	Profile status	TIPHON SIP R3	Notes
1	Client behaviour for registration?	M	c3	S	
2	Registrar?	O	c4	NS	
3	Client behaviour for session requests?	M	o	S	
4	Server behaviour for session requests?	M	o	S	
5	Session release?	M	c1	S	
6	Timestamping of requests?	O	o	S	
7	Authentication between UA and UA?	O	o	NS	User to user auth not supported in TIPHON yet
8	Authentication between UA and registrar?	O	n/a	S	
9	Server handling of merged requests due to forking	M	m	NS	Not supported in TIPHON. May be supported in Release 5
10	Client handling of multiple responses due to forking	M	m	NS	See item 9
11	Insertion of date in requests and responses?	O	o	S	
12	Downloading of alerting information?	O	o	NS	SC not supported in TIPHON. Need 'alerting type' capability
Extensions					
13	The SIP INFO method?	O	n/a	NS	To be supported in Release 4
14	Reliability of provisional responses in SIP?	O	m	S	
15	The REFER method?	O	o	S	To be included in Release 4
16	Integration of resource management and SIP?	O	m	NS	
17	the SIP UPDATE method	c5	m	NS	
18	SIP extensions for caller identity and privacy?	O	m	NS	This capability does not satisfy TIPHON req, another extension required
19	SIP extensions for media authorization?	O	m	NS	
20	SIP specific event notification	O	o	NS	This could be supported if TIPHON has a notification SC
21	The use of NOTIFY to establish a dialog	O	n/a	NS	See item 20
22	Acting as the notifier of event information	c2	c2	NS	See item 20
23	Acting as the recipient of event information	c2	c2	NS	See item 20
24	Path Extension Header for Establishing Service Route with SIP REGISTER	O	c6	NS	This capability is not supported in TS 101 884 [20] uses 'record-route' for this purpose
25	Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks	O	m	NS	This should be supported in TS 101 884 [20]
26	A Privacy Mechanism for the Session Initiation Protocol (SIP)	O	m	NS	This should be supported in TS 101 884 [20]

B.4.2 Comparison of capabilities for Proxies/B2BUA

Table B.5: Comparison of capabilities for Proxies/B2BUA

Item	Does the implementation support	RFC status	Profile status	TIPHON SIP R3	
Capabilities within main protocol					
1	client behaviour for session requests?	m	M	S	
2	server behaviour for session requests?	m	M	S	
3	session release?	m	M	S	
4	Stateless proxy behaviour?	o.1		NS	TIPHON does not support stateless behaviour
5	Stateful proxy behaviour?	o.1		S	
6	forking of initial requests	c1	n/a	NS	Forking is not supported in TIPHON
7	support of TLS connections on the upstream side	o	n/a	?	FFS
8	support of TLS connections on the downstream side	o	n/a	?	FFS
9	insertion of date in requests and responses	o	O	S	
10	suppression or modification of alerting information data	o	O	NS	This is not supported in TIPHON. Need an "Alerting type" parameter in TIPHON.
11	reading the contents of the Require header before proxying the request or response	o	O	NS	Require method may be supported in Release 4
12	adding or modifying the contents of the Require header before proxying the REGISTER request or response	o	M	NS	See item 11
13	adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER	o	O	NS	See item 11
14	the requirement to be able to insert itself in the subsequent transactions in a dialog	o	c2	S	
15	the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing	c3	c3	S	
16	reading the contents of the Supported header before proxying the response	o	O	NS	See item 11
17	reading the contents of the Unsupported header before proxying the 420 response to a REGISTER	o	M	NS	See item 11
18	reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER	o	O	NS	See item 11
19	the inclusion of the Error-Info header in 3xx - 6xx responses	o	O	NS	To be supported in Release 4

Item	Does the implementation support	RFC status	Profile status	TIPHON SIP R3	
Extensions					
20	The SIP INFO method?	o	O	NS	To be supported in Release 4
21	Reliability of provisional responses in SIP?	o	M	S	
22	the REFER method?	o	O	NS	To be supported in Release 4
23	Integration of resource management and SIP?	o	M	NS	To be supported in Release 4
24	the SIP UPDATE method	c4	M	NS	To be supported in Release 4
25	SIP extensions for caller identity and privacy?	o	M	NS	Could support this Release 4 for application level anonymity
26	SIP extensions for media authorization?	o	M	NS	To be supported in Release 4
27	SIP specific event notification	o	O	NS	Should support in Releases 4 and 5
28	the use of NOTIFY to establish a dialog	o	n/a	?	FFS
29	Path Extension Header for Establishing Service Route with SIP REGISTER	o	c5	NS	FFS
30	extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks	o	M	NS	Should be supported in Release 4
31	a Privacy Mechanism for the Session Initiation Protocol (SIP)	o	M	NS	FFS

Annex C (informative): Bibliography

- Wassenaar agreement 2 (http://www.wassenaar.org/)

History

Document history		
V1.1.1	November 2003	Publication