Source: **SA1**

Title: **CRs to 22.978 with various subjects (Rel-7)**

Document for: **Approval**

Agenda Item: **7.1.3**

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers Current	Vers New	SA1 Doc
SP-28	SP-050223	22.978	001	-	Rel-7	F	Corrections to TR 22.978	7.0.0	7.1.0	S1-050496
SP-28	SP-050223	22.978	002	-	Rel-7	F	Improvements to Key Aspects of an AIPN	7.0.0	7.1.0	S1-050497
SP-28	SP-050223	22.978	003	-	Rel-7	F	Improvement of TR 22.978 Annexes	7.0.0	7.1.0	S1-050498
SP-28	SP-050223	22.978	004	-	Rel-7	F	Alignment and improvement of 'Recommended requirements' and 'Conclusions' of TR 22.978	7.0.0	7.1.0	S1-050499
SP-28	SP-050223	22.978	005	-	Rel-7	F	Content-based charging between operators	7.0.0	7.1.0	S1-050502
SP-28	SP-050223	22.978	006	-	Rel-7	C	More Flexible service adaptation under operator's control	7.0.0	7.1.0	S1-050503
SP-28	SP-050223	22.978	007	-	Rel-7	C	Multiple public addresses for single device/user	7.0.0	7.1.0	S1-050529
SP-28	SP-050223	22.978	008	-	Rel-7	F	Enabling integrated rich services in AIPN	7.0.0	7.1.0	S1-050538
SP-28	SP-050223	22.978	009	-	Rel-7	B	CR to improve multicast description in TR 22.978	7.0.0	7.1.0	S1-050539

CR-Form-v7.1

CHANGE REQUEST

⌘ **22.978** **CR** **001** ⌘**rev** **-** ⌘ Current version: **7.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☐

Title:	⌘	Corrections to TR 22.978
Source:	⌘	SA1 (AIPN Rapporteur (NTT DoCoMo Inc.))
Work item code:	⌘	AIPFS
Date:	⌘	04/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-7

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*
Rel-7 *(Release 7)*

Reason for change:	⌘	TR 22.978 contains some errors that need to be corrected.
Summary of change:	⌘	Re-organisation and correction of definitions and addition of abbreviations within Chapter 3; editorial modifications, removal of duplicated text, and alignment of terminology within chapters 4 and 5.
Consequences if not approved:	⌘	TR 22.978 will continue to contain errors which may make some parts of TR 22.978 ambiguous. This could result in confusion when TR 22.978 is referenced.

Clauses affected:	⌘	3.1, 3.2, 4.2, 4.2.1, 4.2.1.1, 4.2.2.4, 4.2.3.3. 4.2.3.4, 4.2.3.7, 4.2.3.8, .4.3.3, 5, 5.1, 5.4,

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
		X	Test specifications	
		X	O&M Specifications	

Other comments:	⌘	The AIPN Rapporteur apologises for missing these errors prior to approval of TR 22.978.

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

1st Modified Section

3.1 Definitions

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

~~**Ad-hoc Network:** An *Ad-hoc Network* is a dynamically organized network of mobile terminals that are able to communicate with each other via some means (e.g. using IEEE 802.15 or WLAN in ad-hoc mode). An Ad-hoc Network may contain terminals that are capable of connection to a variety of access systems. In the context of AIPN, it is assumed that every terminal in the Ad-hoc Network is under the control of a separate user, each able to independently access the AIPN. The Ad-hoc Network routes their consolidated traffic towards the AIPN, to an Access system through one or more terminals in the Ad-hoc Network. The Ad-hoc network may change the terminal carrying the consolidated traffic change dynamically according to rules set up by the users. The Ad-hoc network may move throughout the geographic coverage area. (See Annex E)~~

All-IP Network (AIPN): ~~-~~A collection of entities that provide a set of capabilities for the provision of IP services to users based on IP technology where various access systems can be connected. The AIPN provides a set of common capabilities (including mobility, security, service provisioning, charging and QoS) which enable the provision of services to users and connectivity to other external networks. An AIPN requires one or more connected access systems to allow users to access the AIPN.

Access system: An entity or collection of entities that provides the user the capability to connect to the AIPN.

AIPN operator: An operator of an AIPN. It is assumed that the AIPN operator will also be a network/PLMN operator as defined within [1].

IP service: A~~a~~ service using an IP bearer provided by an IP service provider. For IP services data traffic is routed according to the IP addresses of the sender and receiver.

IP service provider: A~~a~~ service provider that provides IP services. This may or may not be a network operator e.g. the operator of an IMS would be an IP service provider according to this definition.

IP service subscriber: A~~a~~ subscriber to an IP service provider that uses IP services.

~~**Moving Network:** A *Moving Network* is a group of user devices (terminals) that move together, for example, as part of vehicular network. The user devices (terminals) are interconnected in a way that their consolidated traffic towards the AIPN is routed through a well-defined system (gateway). The elements of the consolidated traffic may originate from PAN and Ad-hoc Networks within a Moving Network. (See Annex E)~~

~~**Personal Network:** A Personal Network, in the context of AIPN, consists of more than one device (terminal or server provided by the AIPN operator) under the control of one user providing access to the AIPN. These devices are interconnected by the AIPN such that the user perceives a continuous secure connection regardless of their relative locations. The user controls the PN using facilities provided by the AIPN. (See Annex E)~~

~~**Personal Area Network:** A Personal Area Network (PAN), in the context of AIPN consists of more than one device (terminal) controlled by, and physically close to, the same user (person). All the devices within a PAN use the same USIM. These devices are connected together using internal PAN means. The user obtains services from the AIPN using his multiple devices which all access the users USIM through the PAN to gain access to the AIPN. The user controls the PAN directly. (See Annex E)~~

Seamless: A user experience that is unaffected by changes in the mechanisms used to provide services to a user.

Note: The determination of whether something satisfies the requirement for being seamless or not is dependent on the user's (e.g., human end-user, protocol, application, etc.) perception of the service being received and not necessarily the technology used to provide the service.

Seamless s~~S~~ervice: S~~s~~ervices provided across access systems and terminal capabilities. Provisioning of this service is continued between and within access systems and between terminals with minimal degradation in the service as seen by the user.

Seamless session: A session that is maintained during a change in access system, with no perceivable interruption from a user perspective, while adapting to the capabilities of each access system.

End-user mobility: The ability for the subscriber to communicate using the device or devices of his/her choice

Terminal mobility: The ability for the same UE to communicate whilst changing its point of attachment to the network. This includes both handovers within the same access system, and handover from one access system to another.

Session mobility: The ability for a communication session to be moved from one device to another under the control of the user.

Ad-hoc Network: A dynamically organized network of mobile terminals that are able to communicate with each other via some means (e.g. using IEEE 802.15 or WLAN in ad-hoc mode). An Ad-hoc Network may contain terminals that are capable of connection to a variety of access systems. In the context of AIPN, it is assumed that every terminal in the Ad-hoc Network is under the control of a separate user, each able to independently access the AIPN. The Ad-hoc Network routes their consolidated traffic towards the AIPN, to an access system through one or more terminals in the Ad-hoc Network. The Ad-hoc Network may change the terminal carrying the consolidated traffic dynamically according to rules set up by the users. The Ad-hoc Network may move throughout the geographic coverage area. (For further details see use cases in Annex E)

Moving Network: A group of user devices (terminals) that move together, e.g. as part of a vehicular network. The user devices (terminals) are interconnected in a way that their consolidated traffic towards the AIPN is routed through a well-defined system (gateway). The elements of the consolidated traffic may originate from PAN and Ad-hoc Networks within a Moving Network. (For further details see use cases in Annex E)

Personal Network: In the context of an AIPN, a Personal Network (PN) consists of more than one device (terminal or server provided by the AIPN operator) under the control of one user providing access to the AIPN. These devices are interconnected by the AIPN such that the user perceives a continuous secure connection regardless of their relative locations. The user controls the PN using facilities provided by the AIPN. (For further details see use cases in Annex E)

Personal Area Network: In the context of an AIPN, a Personal Area Network (PAN) consists of more than one device (terminal) controlled by, and physically close to, the same user (person). All the devices within a PAN use the same USIM. These devices are connected together using internal PAN means. The user obtains services from the AIPN using his multiple devices which all access the users USIM through the PAN to gain access to the AIPN. The user controls the PAN directly. (For further details see use cases in Annex E)

For further definitions see [1].

3.2 Abbreviations

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

AAA	Authentication, Authorisation and Accounting
AIPN	All-IP Network
CAPEX	CAPital Expenditure
OPEX	OPerational Expenditures
~~CPE~~	~~Customer Premise Equipment~~
SSO	Single Sign-On
HSDPA	High Speed Downlink Packet Access
HSUPA	High Speed Uplink Packet Access
GAA	General Authentication Architecture
GBA	General Bootstrapping Architecture
MR	Mobile Router
PAN	Personal Area Network
PN	Personal Network
SC	Session Control

For further abbreviations see [1].

Next modified section

4.2 Motivations and Drivers

The current feasibility study aims at clarifying the notion of an "All-IP Network" (AIPN) within the context of 3GPP and to define requirements for an AIPN within 3GPP. There seems to be a common understanding in the mobile communications industry that the technical and commercial evolution of this industry sector points towards an AIPN. The term "All-IP Network"(AIPN), however, is not (yet) clearly defined and – depending on one's view of the future – can mean many different aspects of anticipated communication systems that are based on IP.

It should be noted that the 3GPP system standardised up to and including Rel-6 already provides the basis for introduction of an AIPN in 3GPP. Building on the foundations provided in previous 3GPP releases it is possible to leverage and build upon existing capabilities to evolve the 3GPP system towards an AIPN.

In order to justify the development and evolution of the 3GPP system it is essential to have an understanding of the motivations for evolving the 3GPP system in a particular direction.

In doing so it seems worthwhile to collect and list trends and drivers of the mobile telecommunications industry that now or in the future can be expected to have significant impact on the industry. This is provided in the following sub-clauses. An assessment of these trends and drivers with respect to the evolution of IP-based network and access systems, terminals and service provisioning will make it easier to create a vision of what an AIPN will look like.

4.2.1 User related and social drivers

4.2.1.1 Consumer trend demanding diversification of mobile services

Diversification as service specialisation:
As the market for mobile services grows there is an increased need to be able to offer diversified and flexible services to satisfy the varied needs of users. As the service market becomes more diversified services will become more specialised in order to satisfy the specific needs of users. With this there is a need for AIPN operators to be able to offer flexible services quickly without a large amount of capital expenditure.

Diversification in terms of usage patterns:
In addition to the current pattern of mainly server-to-person services there will be a diversification of mobile services to include person-to-person, person-to-server, server-to-server service scenarios with a variety of different subdivisions and combinations. Users will also desire the ability to be able to integrate the various services to which they subscribe. In the future mobile networks will need to be able to provide these varied and integrated service environments and enable this to be achieved in a flexible and efficient manner.

Diversification in terms of service quality:
Different services will have different user expectations placed upon them e.g. in terms of service quality. The demands for the same service may also differ according to specific user of that service at a given time.

Diversification regarding access to services:
With the increase in the diversity of the access systems available ~~and~~, as well as the increase in the number of terminals that a single user possesses it will be desirable to have the ability to use services seamlessly across different access systems and different terminals. Users will also desire the ability to use services `anywhere` at `anytime`. This leads to the conclusion that the provision of `seamless` and `ubiquitous` services will gain great prominence within future mobile services.

Deductions

- An AIPN would provide the ability to offer enhanced and flexible mobile services, quickly and cost effectively. An AIPN can also support the diversification of mobile network services, support service integration and would enable the provision of seamless and ubiquitous services across a variety of different access systems and terminals.

- IP technology that enables advanced service control (e.g. QoS/session control) is already used within 3GPP and elsewhere and could be further utilised and enhanced within and between mobile networks in order to enhance service provision.

Next modified section

4.2.2.4 Need for increased system efficiency leading to substantial cost reduction in terms of both equipment (CAPEX), and operational (OPEX) costs.

In the future it is foreseen that there will be increasing pressure to decrease the investment costs for mobile network equipment and the cost per bit for traffic carried by mobile networks. The reasons for this are twofold. Firstly, the increase in IP traffic carried by mobile networks will lead to a general need to further decrease the cost of handling this traffic both in terms of equipment and transmission costs. Secondly, in the future there will be increased competition for AIPN operators not only from mobile network operators using different radio access systems, but also from IP service providers providing broadband IP services using access and transmission technologies other than those of traditional mobile network operators, e.g. ISPs providing services using xDSL, Cable and/or WLAN without 3GPP inter-working. The business and charging models, e.g. flat-rate charging, deployed by these IP service providers are not those common to traditional network operators implementing the 3GPP system and will probably not be applied by AIPN operators. However, they do encourage heavy usage of IP services and as such AIPN operators need to be able to deploy a cost effective network for IP services in order to compete in the wider market place.

The cost of general-purpose equipment targeted for a wide-ranging general market is in general much less than that of specialised technology whose market is limited by specific criteria. An AIPN would enable the use of general-purpose IP technology with some modifications to tailor functionalities to the needs of network operators to provide mobile services. The ability to undertake large-scale deployment of general-purpose IP technology provided by an AIPN ~~are~~ is foreseen to enable significant improvements in system efficiency and overall reduction in the equipment (CAPEX) and operational (OPEX) costs for future mobile networks designed to handle a large amount of IP traffic.

CAPEX point of view:

- The adoption of a common network system enables capital investment to be made independent to the number of access systems supported. Also, when a new access is added, the equipment costs are suppressed to a necessary minimum.
- Over capacity can be avoided by sharing the system, and the equipment costs are reduced (including redundant equipment costs).
- The development and the equipment costs of mass produced general-purpose devices are generally lower compared to dedicated devices.

OPEX point of view

- The variety of maintained devices can be reduced by introducing a common system, hence maintenance costs are reduced.
  - The training costs of ~~the~~ maintenance engineers are reduced.
  - Due to the availability of general purpose platforms the cost ~~for~~ of replacement hardware can be suppressed.

Deductions

- The AIPN should be designed to enable AIPN operators to take advantage of the increased efficiency and OPEX/CAPEX reductions offered by IP technology.

Next modified section

4.2.3.3 Progress in ad-hoc networking for user defined services.

Ad-hoc ~~n~~Networks denote particular kinds of networks that may establish themselves automatically - "ad-hoc" - (i.e. without explicit administration) between mobile terminals. From today's perspective, generally all the activity

concerning development in the field of ~~ad-hoc network~~Ad-hoc Networks (radio spectra, terminal communication and mechanisms to create ~~ad-hoc network~~Ad-hoc Networks) is happening outside 3GPP. However, AIPN operators may benefit from letting ~~ad-hoc network~~Ad-hoc Networks interact with the AIPN, thereby creating traffic in the AIPN; e.g. there could be ~~ad-hoc network~~Ad-hoc Network access to public networks via AIPN by at least one of the ~~ad-hoc network~~Ad-hoc Network members serving as a kind of wireless connectivity gateway.

Examples for such ~~ad-hoc network~~Ad-hoc Networks could be ~~personal network~~Personal Networks, as described later in the present document, or CB-type radio communications amongst listeners to a pop concert. In the case of ~~personal network~~Personal Networks an AIPN may provide connectivity to a server in an AIPN operator's network, in the pop concert example an AIPN may provide the capability for remote listeners to join.

Technically, an ~~ad-hoc network~~Ad-hoc Network is defined as a self-organizing and self-managing network of autonomous mobile terminals *without any infrastructure support*. In fact, it is this property which essentially characterizes ~~ad-hoc network~~Ad-hoc Networks, and as a consequence, no centralized radio resource management for ad-hoc networking necessarily exist.

Important aspects of ~~ad-hoc network~~Ad-hoc Networks which may impact an AIPN are:

- Identification, addressing and routing: If an ~~ad-hoc network~~Ad-hoc Network interacts with the AIPN, the AIPN may need to know about identities of individual members of the ~~ad-hoc network~~Ad-hoc Network (not only the "connectivity gateway"), be able to address them and route traffic to them.

- Authentication, security: in an ~~ad-hoc network~~Ad-hoc Network neither SIM resp. USIM/ISIM based identification and authentication nor ciphering on the air interface derived from authentication parameters can be assumed. In the case of at least one ~~ad-hoc network~~Ad-hoc Network member serving as a wireless connectivity gateway to the AIPN it should be ensured that this node can not compromise AIPN security.

Deductions

- Appropriate mechanisms for identification, authentication, addressing, ciphering and charging of members of an ~~ad-hoc network~~Ad-hoc Network inter-working with an AIPN have to be established.

4.2.3.4 Dawning of new, radio based services (e.g. ~~personal network~~Personal Networks, RFIDs, multi-hop access networks)

Currently there is a lot of activity (research projects) on new services that are utilizing different kinds of IP-based radio networks. Examples of such services could be:

- Personal (portable) N~~n~~etworks, that allow inter-working of different personal sensors/terminals

- RFIDs, that allow goods, to which a RFID is attached, to broadcast information about themselves,

- Multi-hop access networks, that allows a user's terminal to act as a radio relay station for another user

Many of these new services are capable to create revenue for an AIPN operator if they can easily inter-work with (or be integrated into) an AIPN

Deductions

- An AIPN would benefit from a capability to facilitate inter-working with (or integration of) these new radio based services.

4.2.3.5 Reconfigurable Radio (Software Defined Radio - SDR)

Reconfigurable radio interfaces allow terminals to adapt/optimise its radio properties to the currently available radio network. This could allow an increase of spectrum efficiency. However, the network would need to support such a functionality of the terminal.

Deductions

- An AIPN would benefit from a support of reconfigurable radio interfaces in the terminal.

4.2.3.6 Web services

While not being specific to mobile networks Web Services are becoming increasingly important as a standardised interface to provide IP-based services. There is a general trend towards Web services within the industry. For example, in OMA a working group is dedicated to the evolution of web services in mobile networks and in many respects they are seen as a replacement (rather than an addition) of traditional service enabler interfaces such as CAMEL and the CORBA version of OSA/PARLAY.

Deductions

- An AIPN will need to support Web Service interfaces for service provisioning.

4.2.3.7 Multi-access

The introduction of multiple access systems within the same coverage area raises new AIPN operator and user requirements; the user may wish to influence the selection of the access system for use based on such aspects as supported QoS, mobility, pricing, coverage, etc. and the AIPN operator may wish to influence the access system selection by setting policies. Optionally, a user may even wish to use simultaneous multi-access as well.

Note that the selection of the access system must be easy for the end-user, e.g. it could be based on some preferences and the actual process can be partly or completely hidden.

It is expected that users using multiple access systems will require an appropriate service continuity experience as they switch from one access system to another. This means that their sessions remain in operation, with minimal interruption. In addition, the services provided should be made access aware (e.g.~~,~~ choose video quality based on the available bandwidth).

Deductions

- An AIPN shall make use of the multiple access systems by providing support for appropriate handover between access systems, reachability over multiple access systems, access system-aware services, and optionally simultaneous multi-access.

- An AIPN shall provide support for access system selection based on combinations of AIPN operator policies, user preferences and access system conditions.

4.2.3.8 Progress of advanced Traffic Engineering Technologies

As the number of users accessing multimedia and data service[s] from 3G networks will continue to increase, huge amounts of IP traffic are expected to be handled by AIPN operators. Due to the increase of the IP traffic, network bottlenecks may also appear in an AIPN operator's IP backbone, therefore, new challenges will be faced by the AIPN to provide guaranteed QoS to end-users for different types of services (real-time, non real-time) and also ensure that the transport network resource is used efficiently. This would enable e.g. over-provisioning in IP transport network to be avoided in order to save CAPEX for AIPN operators.

Traffic engineering technologies, e.g. MPLS, advanced QoS routing algorithms, and dynamical load balancing among network entities are potential solutions to achieve this within an AIPN.

Deductions

- An AIPN will need to be able to guarantee QoS for different types of services (real-time, non real-time) and ensure efficient use of network resources. Traffic engineering technologies within the IP transport network may provide appropriate methods to achieve this within an AIPN.

Next modified section

4.3.3 Impacts to current service models

Impact on models for development and provisioning of services

Even if the 3GPP system already allows the flexibility of IP based services through the PS domain today, the introduction of AIPN may bring the model for ~~-~~the development and provisioning of services ~~-~~one step further. The current model for the introduction of new services ~~are introduced~~ into 3GPP systems, often comprising standardisation of capabilities within 3GPP, followed by development by vendors and deployment by network operators, is rather cumbersome and has difficulties in quickly responding to changing market trends. Whilst also maintaining the traditional aspects of the 3GPP service model, it should be important to leverage new possibilities for service provisioning which may be enabled by the introduction of an AIPN. There is a potential demand for an extremely wide variety of mobile services. To meet this demand new models for service provisioning are essential.

Historical side note: An interesting comparison is the evolution of software applications within the computer industry. Only two decades ago software applications were limited in variety and cost was high. The emergence of a few de facto standards for software application environment propelled an unparalleled explosion of all foreseeable and unforeseen kinds of software applications. The economy of scale has also made it possible for them to be provided at a much lower cost level.

Outlook on potential new models for development and provisioning of services

The introduction of AIPN can similarly be an enabling factor for developing new models for easier, more flexible and more cost efficient introduction of mobile services. Today there exist several good examples where simplified service models have brought forward a wide variety of mobile services. But to meet the potential demand of mobile services, models must continue to be developed that allow services to be jointly provided by multiple stakeholders. Most likely the broadest range of mobile services will be possible when responsibility for service provisioning is opened for third party service providers e.g. via web services. Using policy and control frameworks, applying flow based charging concepts, establishing the IMS framework, and providing different sorts of open interfaces, will be important tools for AIPN operators to control how third party providers can provide their services. Changed business models must go hand in hand with this to give all parties incentive to put efforts into it. As in the software application domain, it is by releasing the innovative force of a larger group of creative people and companies that we can meet the demand for mobile services in the coming decades.

New usage- and traffic patterns for mobile services

Different service models also need to exist for different categories of mobile services. Person-to-content, person-to-person, and machine-to-machine type of services should for example require different service models to enable faster, more flexible and more cost efficient service provisioning.

The work within 3GPP will allow an evolution of the 3GPP system to enable these more advanced service models and to keep AIPN operators in control at their selected level.

Next modified section

5 End-user and ~~network~~ AIPN operator aspects of an AIPN

5.1 AIPN Vision

An AIPN would enable the convergence of access systems and services onto a common network. In this emerging area users will demand more from their services and interaction with their technologies. Instead of the islands of capabilities that currently exist it is desirable to bring these capabilities under one umbrella whilst offering session continuity across multiple access systems. This seamless offering will be characterised by the provision of an effective management of mobility that consists of offering users a telecommunication service, continuously and transparently when the user's

terminal moves between various access systems or various services, whatever type of communication and wherever communication has been initiated. One of the key enablers within an AIPN will be the seamless mobility across terminals and access systems supported by a mobility manager that unobtrusively manages these interactions.

Delivering an AIPN will address these needs, extend the reach of 3G technologies and maintain a relationship with the user in each context. Multiple connected devices will enjoy interactivity, adopting principles including single sign on, seamless mobility, context sensing and the unobtrusive device management.

5.1.1 Key aspects of an AIPN

The following are the key aspects of an AIPN:

5.1.1.1 Common IP-based network

- IP-based network control
  - Non-access system specific mobility control equivalent to that provided by cellular networks i.e. mobility control within the AIPN under the control of the AIPN operator, across the same and different access systems, that is not dependent upon specific access or transport technologies or IP version.
  - IP-based routing and addressing
- IP transport
- Communication quality, i.e. QoS, equivalent to or greater than already provided
- Inter-working with IP networks
- Inter-working with legacy networks
- Functionality at the edge of the network to support different access systems, legacy equipment.

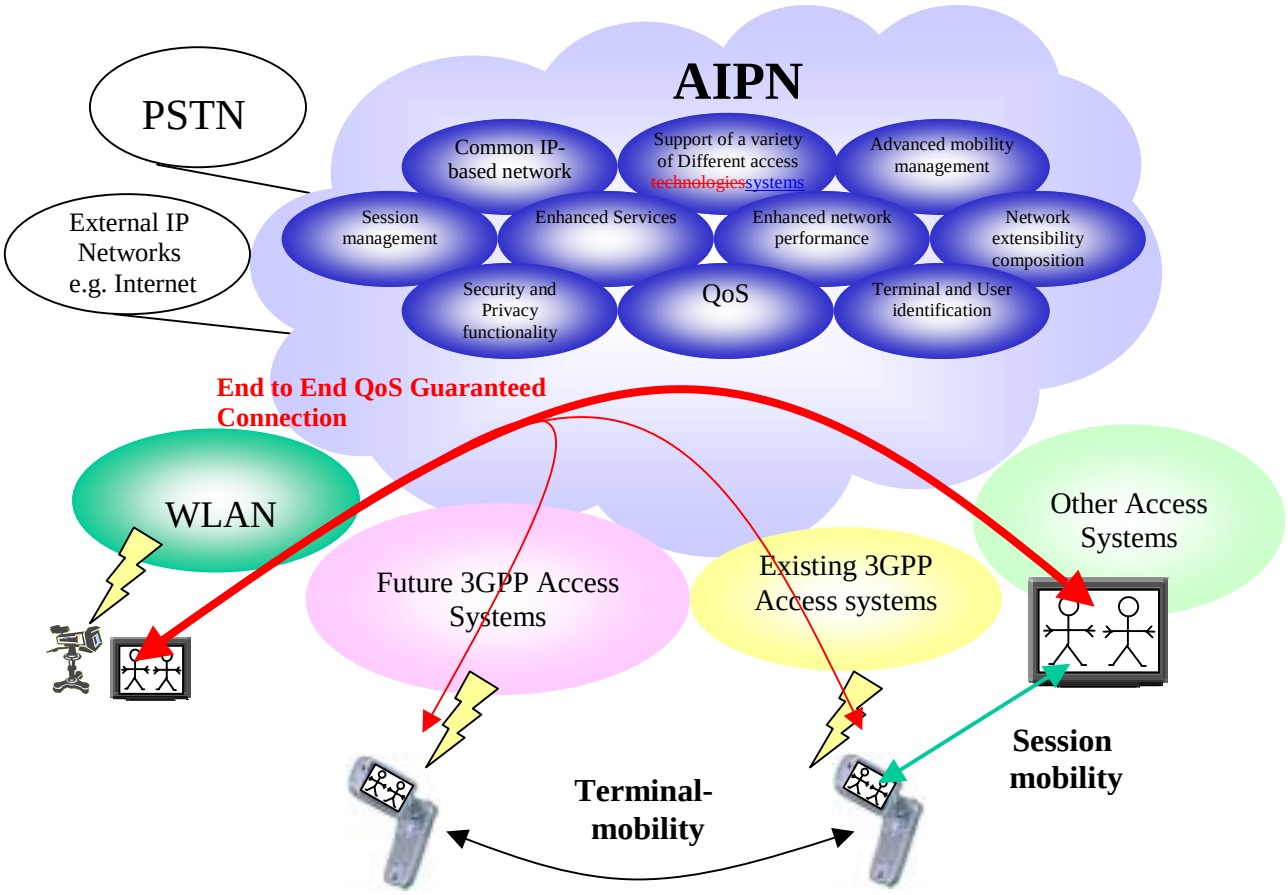


Figure 1: Visual representation of the key aspects of an AIPN

5.1.1.2 Support of a variety of different access systems (existing and future)

- Service provision across different access systems

5.1.1.3 Take advantage of convergence of telecommunications and IT industries towards IP technology

- An AIPN should aim to provide common capabilities independent to the type of service being provided (i.e. independent of whether it is a "traditional" telecomm service or a "traditional" data service).

- Convergence with IP technology should be considered within the AIPN system design from the perspective of the system as a whole (i.e. network and mobile terminals) to ensure that complexity is avoided within specific elements e.g. avoidance of complexity in mobile terminals due to a misalignment between technology convergence in the network and mobile terminals.

5.1.1.4 Advanced mobility management:

- Mobility across access systems.

  - Support fast handover and/or lossless handover across different access systems

  - Provision of Seamless services and handover across different access systems.

  - Support the capability to apply handover mechanisms based on quality of service requirements of applications and capabilities of the access systems involved.

- Multiple dimensions of mobility

  The AIPN shall support several dimensions to provide mobility:

  - An end-user shall be able to use different devices (“end-user mobility”).

  - The terminal shall be able to communicate while moving. This includes both handover from one radio cell to another in the same access system, or switching from one access system to another in a multi-access system environment. (“terminal mobility”).

  - The user may be able to move some or all of his active communication sessions from one of his devices to another. (“session mobility”) E.g., a user may wish to move a video streaming session from the handset to a car mounted TV screen.

Note that certain aspects of services may change as a result of mobility, but they must remain useful to the end-user.

To address these needs, advanced naming and addressing schemes are necessary that provide reachability for a given user or particular session.

Recommended requirements:

- An AIPN shall incorporate naming and addressing schemes that address a given user or session.

- The AIPN shall support end-user mobility.

- The AIPN shall support terminal mobility.

- The AIPN shall support session mobility.

5.1.1.5 Enhanced session management:

- Service adaptation to terminal capabilities.

  The services provided to users should be, as much as possible, independent of the terminal used. The network should be able to adapt the service (e.g. information rendering) to the capabilities of the terminal being used with minimum or no user interaction.

- Session mobility: seamless mobility of sessions between terminals.

It should be possible to move sessions from one terminal (or a set of terminals) to another according to the preferences of the user e.g. automatically with minimum user involvement or based upon a specific user request/pre-determined user preference settings.

Care needs to be taken to ensure there is no burden on the user to interact in a complex way.

5.1.1.6 Access system selection

In an AIPN the applications are based on IP and will evolve towards access system independence. An AIPN is expected to support multiple access systems.

The selection of the access system may need to take into account several aspects of an AIPN, e.g. service requirements of an application, load balance of the network, and charging & billing.

Recommended requirements:

- The AIPN should provide a means to enable access system selection based on a range of criteria e.g. user preferences, service requirements of applications, network conditions or other AIPN operator-defined criteria.

5.1.1.7 Enhanced services

- Support for advanced application services
- Provision of seamless services (e.g. transparent to access systems, adaptable to terminal capabilities, etc)

  Users should be able to move transparently and seamlessly between access systems and to move communication sessions between terminals.

  An AIPN will be able to adapt services as much as possible to the capabilities of the user's terminal, allowing the user to access services independently of which terminal they are using.

Note: this may not be feasible in all cases (e.g. some services will require "minimum terminal capabilities" to be able to be accessed, with these "minimum capabilities" being service dependent), but an AIPN will be designed to enable this property in as many cases as possible.

- Support ubiquitous services (e.g. associations with huge number of sensors, RF tags, etc.)

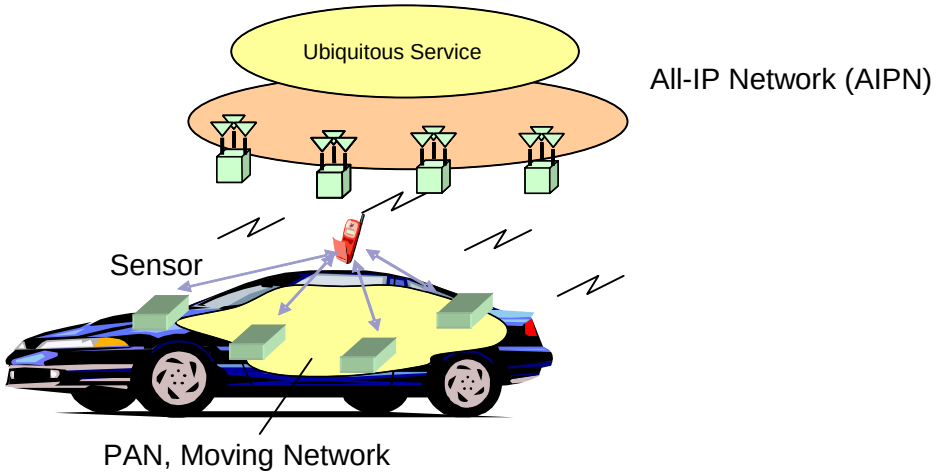


Figure 2: Support of ubiquitous services

- Improve disruption-prone situations when network connectivity is intermittent.

  Disruption-free network connectivity may not be cost effective, or even feasible, in all cases (e.g. cell planning for full radio coverage for all services, disruption-free inter-access system handovers, disruption-free IP connectivity in all network links). An AIPN should consider solutions for making services as resilient to temporary lack of connectivity as possible.

5.1.1.8 Enhanced network performance

- Ability to efficiently handle a variety of different types of IP traffic including user-to-user and user-to-multicast traffic models
- Optimized routing of IP traffic

5.1.1.9 Network extensibility/composition

- Facilitate integration of networks with different administrative domains (e.g. handle negotiation of administrative issues, security, trust, etc).
- Solutions should be studied for facilitating the integration of different networks of the same or different AIPN operators in order to enhance the services provided to their customers, and enable the introduction of new services. This includes, but it is not limited to, the sharing of some parts of the network.
- Allow dynamic and flexible integration of ~~"ad-hoc"~~" ~~networks~~Ad-hoc Networks at the edge (e.g. ~~personal area network~~Personal Area Networks, sensor networks, etc).

5.1.1.10 Network management

Introduction of self-managing technologies (e.g. Plug-and-Play) should be considered for faster deployment and reduction of operational cost. In particular, an AIPN should be designed from an early phase to include:

- Plug-and-play components to ease the setup and operation of the AIPN.

5.1.1.11 Maintenance and improvement of the level of security and privacy functionality

- Security equivalent to or greater than that already provided including the hiding of internal network elements
- Support for user privacy, e.g. location privacy, identity privacy

5.1.1.12 Quality of Service

- AIPN operators should be able to guarantee QoS within their networks.
- The QoS mechanisms used by an AIPN should be able to guarantee end to end QoS for a traffic flow when all network segments (including access, core network and inter-connecting networks) are able to provide the requested QoS.

Note: Business agreements for QoS guarantees between the parties (e.g. operators, national- and international carriers, corporate customers) are today regularly based on static agreements. These types of agreements may need to be re-considered in order to reflect the advanced means to guarantee QoS between AIPNs.

5.1.1.13 Terminal, Subscription and User identification

- Terminal identification in an AIPN should be scalable enough to cover a very large population of diverse terminals (e.g. huge number of mobile terminals which main purpose is to include a sensor or an RF tag, as well as more conventional mobile terminals).

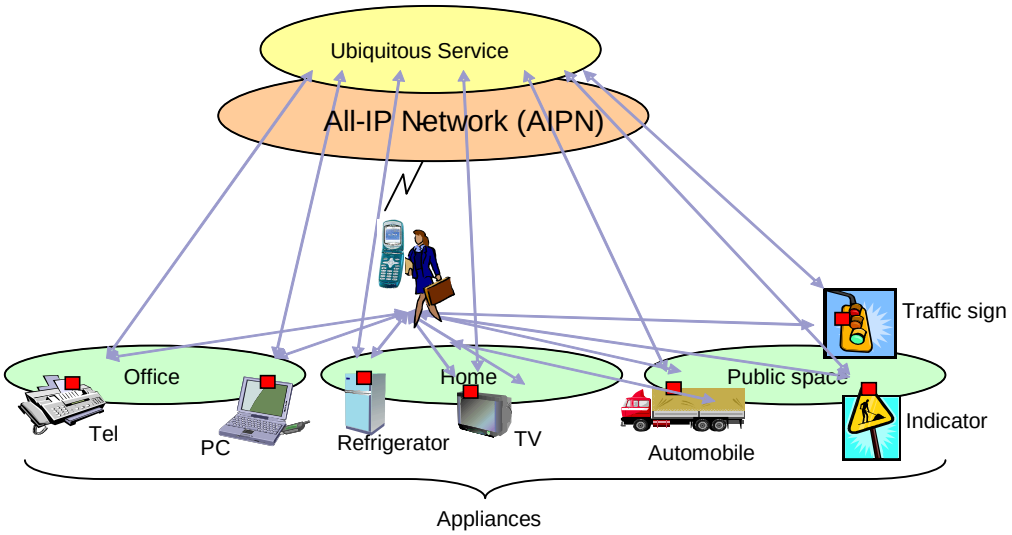


Figure 3: Terminal and User identification within an AIPN

- It should be possible to identify and address terminals, subscriptions, and users.
- It should be possible that more than one user can have active sessions on a single terminal at the same time (e.g. in the case of an ~~ad-hoc network~~Ad-hoc Network, several users may use a single terminal to gain access to the AIPN).

Note: It is for further study which of these identities are routable identities.

5.1.1.14 Flexible future development

- Extensibility
- Modularity of AIPN functions and commoditization of AIPN components. Open interfaces between appropriate network layers
- Ability to evolve individual AIPN entities independently
- Evolution path from previous releases of 3GPP specifications i.e. Rel-6

5.1.1.15 Identity Federation

In an AIPN a user may subscribe to services of many service providers. Accordingly he may hold several accounts (i.e. business agreements) with these service providers, some of these accounts providing the user with new identities. These identities are the means to authenticate the user to the service provider. Examples for identities could be the (U)SIM, username/password combinations, a credit/debit card number in combination with the PIN etc. Identity federation denotes the binding of two or more identities for a given user.

Identity federation for example enables a user, once he has been authenticated to a service provider through one identity, to be automatically authenticated to another service provider through a different identity if this different identity is federated to the first one. The latter process, the automatic authentication to several service providers through a single identity by means of identity federation, is often referred to as "Single Sign On".

Recommended requirement:

- An AIPN should support Identity Federation and Single Sign On for the end user. This would allow automatic authentication of the user to a multitude of service providers once the user has been authenticated by the AIPN.

5.1.2 Continued support of 3GPP system key aspects within an AIPN

Together with the introduction of new functionalities to realise an AIPN several key aspects of the existing 3GPP system need to be maintained in order to ensure that an AIPN is developed in accordance with the needs of the 3GPP community.

The following represent key aspects of the existing 3GPP system that are to be continually supported within an AIPN.

5.1.2.1 Efficiency of resource usage

- Effective usage of power resources within mobile terminals shall be maintained within an AIPN i.e. evolution to an AIPN should not have adverse effects on the battery life of mobile terminals.

- The scarcity of the radio resource shall be respected within an AIPN by ensuring that radio resources are utilised as efficiently as possible.

5.1.2.2 Charging

- The capability to maintain support of existing charging models shall be provided within an AIPN.

5.1.2.2 Roaming

- An AIPN shall provide functionality as appropriate to enable continued support of international roaming ~~between~~with other AIPNs and legacy 3GPP systems.

Next modified section

5.4 Security and Privacy considerations

User and network security and privacy issues, despite being a key concern in today's networks, tend not to be in the top list of priorities when evolving existing systems or designing new ones. The results of this tend to be that security is added to the system instead of being native in the system, which translates into insecure systems or unnecessarily complex security solutions which are often very user unfriendly. For this reason security and privacy considerations are considered within this Technical Report.

Note 1: The feasibility of "user issues" should be considered within the regulation for lawful interception that exists in some countries i.e. it may be required that some of the features above are disabled in some networks in order to comply with local lawful interception regulations.

Note 2: Further information regarding security issues is provided within Annex ~~E~~D.

5.4.1 Security Considerations

Transforming today’s 3GPP system into an AIPN will introduce changes in the threat environment, introducing new threats but also changes in risk levels of already identified threats. Threats previously seen as having low risks may need to be reassessed leading to new security requirements and the need for new and/or improved security mechanisms. The changes in the threat environment will mainly be due to qualitative and quantitative changes in e.g.

- Threat environment (more and more severe attacks) but also increased risks of particular threats (i.e., the impacts and probabilities that attacks occur may increase as a result of the changed threat environment).

- System heterogeneity and multi-access (GSM, UMTS, WLAN, new accesses, etc)

- Fragmentation of security solutions

- Usage patterns (many more users of existing services and many new services)

- Requirements on user convenience (e.g. SSO, etc)

- Use of trust establishment mechanisms (To counter threats and to enable trusted transactions)

The changes in these areas will certainly motivate a review and revision of currently employed security principles and solutions.

An important process will also be to collect the high-level principles and requirements. Examples of proposed high-level requirements for an AIPN are:

- Security shall be equivalent or better than with the current system i.e. 3GPP Rel-6.

  This includes support of:
  - easy portability of subscriber identities to different UEs
  - cost effective protection against unauthorized duplication of security related information such as keys for authentication purposes, key derivation purposes and protection of a session
  - the possibility for an AIPN operator to control security algorithms (and level of security) that apply for particular services e.g. for authentication purposes
  - AIPN operator controlled distribution of security information to devices used for the purpose ~~to~~ of giving~~e~~ cost effective protection of access to the AIPN.

- An AIPN shall be security-conscious from its early phase, not just have security added later on. The shift to AIPN provides an opportunity to introduce new security paradigms and enhancements/upgrades and optimizations of current security solutions.

- Usability: maximum transparency to the user i.e. high levels of security should be provided with minimum user involvement.

- Ensure authenticity so that the user can trust the information he is receiving. This should cover private user to private user communications as well as private user to service provider communications.

- Networks shall be protected against attacks such as Denial-of-Service attacks and unauthorised access.

- Networks shall be able to authenticate each other and authorize services that need signalling between servers.

- Fast re-authentication shall be possible.

- Hiding of internal network elements shall be provided by an AIPN.

- It should be possible for the AIPN operator to select among several levels of security (e.g. 3GPP Rel-6 equivalent security or better)

5.4.1.1 Threat environment

The Internet is rapidly becoming a very hostile environment. Unless proper countermeasures are installed, the threats found in the Internet will soon be prevalent in mobile networks.

With 3G and upcoming extensions of it, many new players will enter the scene. Small and very large AIPN operators and service providers will work together to offer the services the users expect in a competitive way. At the same time, the equipment of the end-users will become more complex and capable. Users will connect PANs over multi-access links to the AIPN and users will act as ~~ad-hoc network~~Ad-hoc Network extensions of the access system. In this environment, attacks may occur in many different places and in many different ways.

5.4.1.2 Network heterogeneity and traffic protection

AIPNs will become increasingly heterogeneous as more and more types of access systems are tied into the cellular environment. To be able to handle new and legacy systems in a uniform way some generic principles for traffic protection have to be established. It is assumed that the existing principle that the system should protect user traffic over the radio access and into the network still holds. It is also assumed that user payload traffic is forwarded in plaintext unless protection is provided as an application specific service.

5.4.2 Privacy considerations

- User issues:

  - Location privacy. User location privacy should be guaranteed.

The location of a user has to be known by some instances in the AIPN to insure reachability and delivery of packets. But only these instances shall know the location to the necessary level of detail.

- Communication confidentiality. Privacy of content and origin/destination of information in all user communications should be guaranteed.

  The information sent and received by the user should be protected in a way that neither the content nor the origination or destination of this information is accessible to non-authorised parties.

- Non-disclosure of identity. Users should be allowed to hide their identities from non-authorised parties.

  Users should be able to have multiple identities from different providers with the relationship between the identities hidden from particular providers (thus supporting privacy).

Note: 2 use cases on this issue are described in Annex ~~D~~C.

End of changes

CR-Form-v7.1

CHANGE REQUEST

⌘ **22.978** **CR** **002** ⌘ **rev** **-** ⌘ Current version: **7.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☐

Title:	⌘	Improvements to Key Aspects of an AIPN
Source:	⌘	SA1 (AIPN Rapporteur (NTT DoCoMo Inc.))
Work item code:	⌘	AIPFS
Date:	⌘	04/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-7

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*
Rel-7 *(Release 7)*

Reason for change:	⌘	Text describing service adaptation appears in two chapters of TR 22.978 describing the 'Key Aspects of an AIPN'. In order to avoid duplication of essentially the same content it is necessary that these two pieces of text are combined.
Summary of change:	⌘	The text describing service adaptation within the chapters on 'Enhanced session management' (5.1.1.5) and 'Enhanced Services' (5.1.1.7) are combined into a single piece of text within chapter 5.1.1.5.
Consequences if not approved:	⌘	Duplicated text will remain within TR 22.978. This could result in an inappropriate understanding of the content of TR 22.978.

Clauses affected:	⌘	5.1.1.5, 5.1.1.7

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
		X	Test specifications	
		X	O&M Specifications	

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

1st Modified Section

5.1.1.5 Enhanced session management:

- Service adaptation to terminal capabilities.

  The services provided to users should be, as much as possible, independent of the terminal used. ~~The network~~An AIPN should be able to adapt the service (e.g. information rendering) to the capabilities of the terminal being used with minimum or no user interaction.

Note: this may not be feasible in all cases (e.g. some services will require "minimum terminal capabilities" to be able to be accessed, with these "minimum capabilities" being service dependent), but an AIPN will be designed to enable this property in as many cases as possible.

- Session mobility: seamless mobility of sessions between terminals.

  It should be possible to move sessions from one terminal (or a set of terminals) to another according to the preferences of the user e.g. automatically with minimum user involvement or based upon a specific user request/pre-determined user preference settings.

  Care needs to be taken to ensure there is no burden on the user to interact in a complex way.

Next modified section

5.1.1.7 Enhanced services

- Support for advanced application services
- Provision of seamless services (e.g. transparent to access systems, adaptable to terminal capabilities, etc)

  Users should be able to move transparently and seamlessly between access systems and to move communication sessions between terminals.

~~An AIPN will be able to adapt services as much as possible to the capabilities of the user's terminal, allowing the user to access services independently of which terminal they are using.~~

~~**Note**: this may not be feasible in all cases (e.g. some services will require "minimum terminal capabilities" to be able to be accessed, with these "minimum capabilities" being service dependent), but an AIPN will be designed to enable this property in as many cases as possible.~~

- Support ubiquitous services (e.g. associations with huge number of sensors, RF tags, etc.)

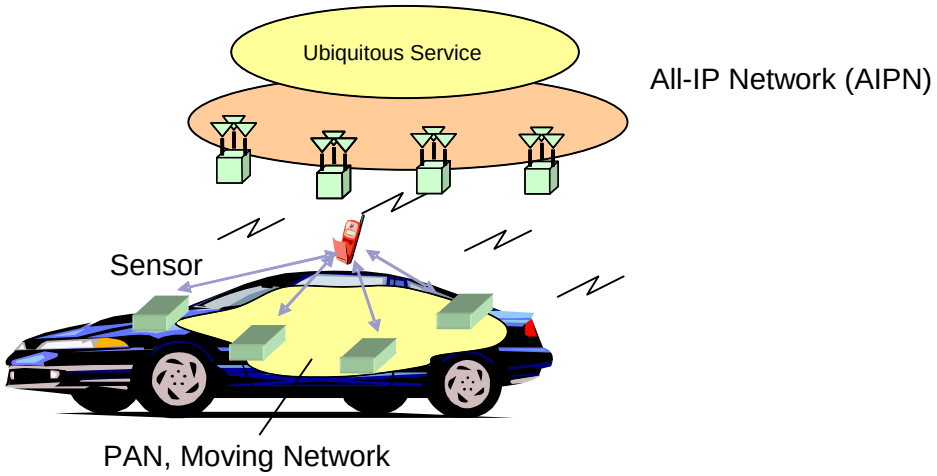


Figure 2: Support of ubiquitous services

- Improve disruption-prone situations when network connectivity is intermittent.

  Disruption-free network connectivity may not be cost effective, or even feasible, in all cases (e.g. cell planning for full radio coverage for all services, disruption-free inter-access system handovers, disruption-free IP connectivity in all network links). An AIPN should consider solutions for making services as resilient to temporary lack of connectivity as possible.

End of changes

CR-Form-v7.1

CHANGE REQUEST

⌘ **22.978** **CR** **003** ⌘ **rev** **-** ⌘ Current version: **7.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☐

Title:	⌘	Improvement of TR 22.978 Annexes
Source:	⌘	SA1 (AIPN Rapporteur (NTT DoCoMo Inc.))
Work item code:	⌘	AIPFS
Date:	⌘	04/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-7

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The annexes of TR 22.978 contains some errors that need to be corrected. Also, the formatting of the headers within the annexes is incorrect and should be rectified.
Summary of change:	⌘	Corrections are made throughout the annexes of TR 22.978 including the rectification of the heading format. Additionally, one use case is moved from Annex B to Annex F.
Consequences if not approved:	⌘	Errors within the annexes to TR 22.978 will remain and the format of the annexes will not be compliant to the format for 3GPP Technical Reports.

Clauses affected:	⌘	Annex B, Annex C, Annex D, Annex E, Annex F

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	The AIPN Rapporteur apologises for missing these errors prior to approval of TR 22.978.

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

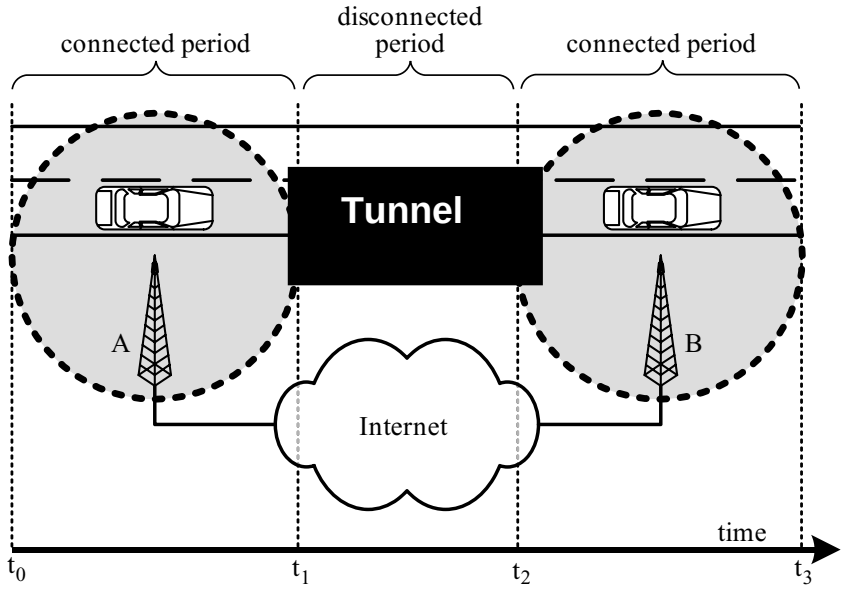
1st Modified Section

Annex B (Informative): Use cases for AIPN key aspects

B.1 Resilience in the presence of network disruptions and intermittent connectivity

Use case:

This use case is illustrated in the figure below.



The user is driving a car. While being under good radio coverage, he starts an IMS session with several media. The car goes through a tunnel where there is no radio coverage, and comes out of the tunnel into good radio coverage a minute later. Connections using disruption resilient transport protocols are automatically re-established and these protocols restore the communication to the point they w~~h~~ere before the interruption.

B.2 Service adaptation to terminal capabilities

Use case:

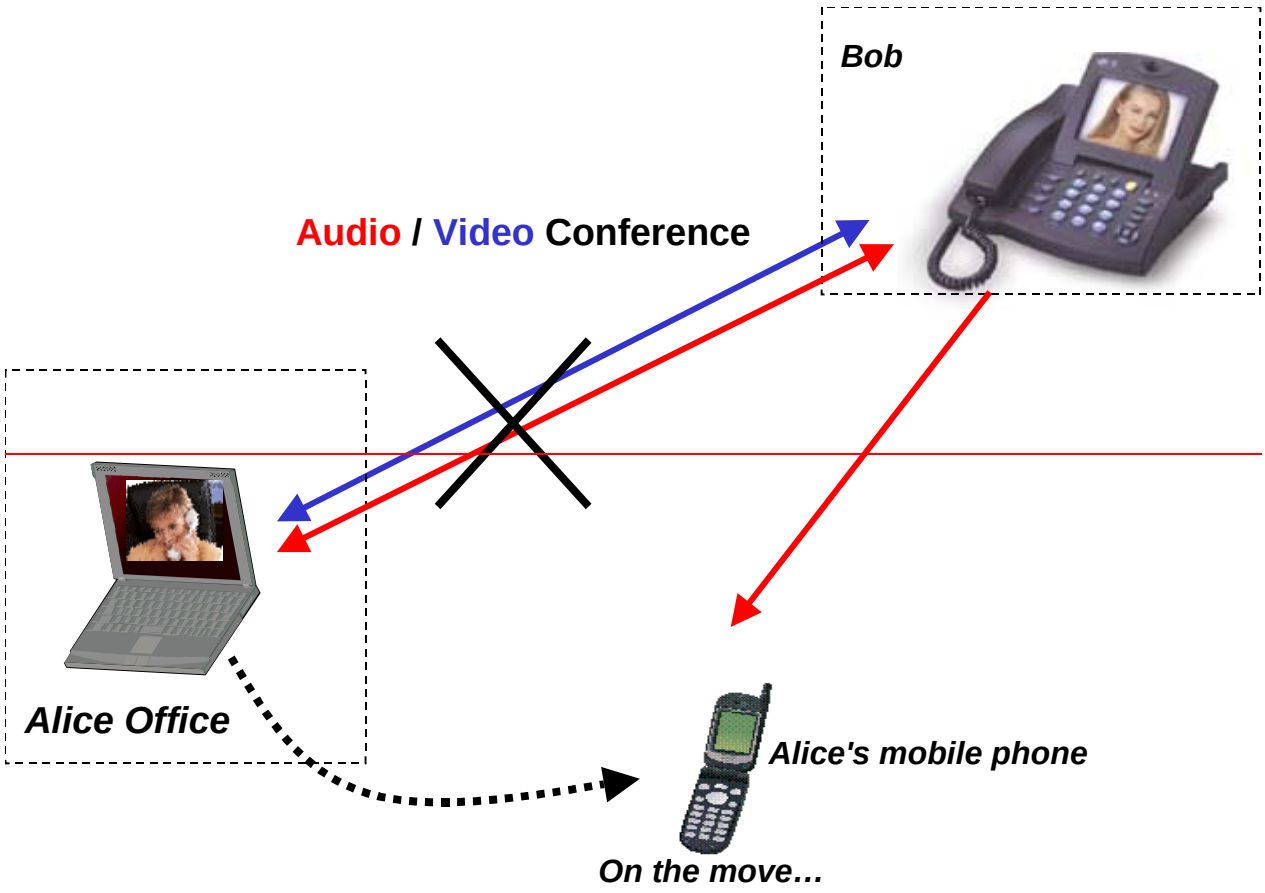
This use case is illustrated in the figure below.

Alice has a mobile device and Bob has a fixed one. Both devices have equal audio but different video capabilities in terms of screen size, number of colors and video codecs supported. Alice establishes a multimedia connection with audio and video components to Bob. The terminal capabilities are discovered and it is realized that Bob's terminal has better video capabilities than Alice. The terminal informs the network that it is unable to support new the new video codec and the AIPN then introduces a video transcoder in the path of the video media to adapt the video signal (stream, codec, format, etc) to the video capabilities and bit rates available on each side of the transcoder.

~~B.3 Session mobility: seamless mobility of sessions between terminals~~

~~**Use case:**~~

~~This use case is illustrated in the figure below.~~

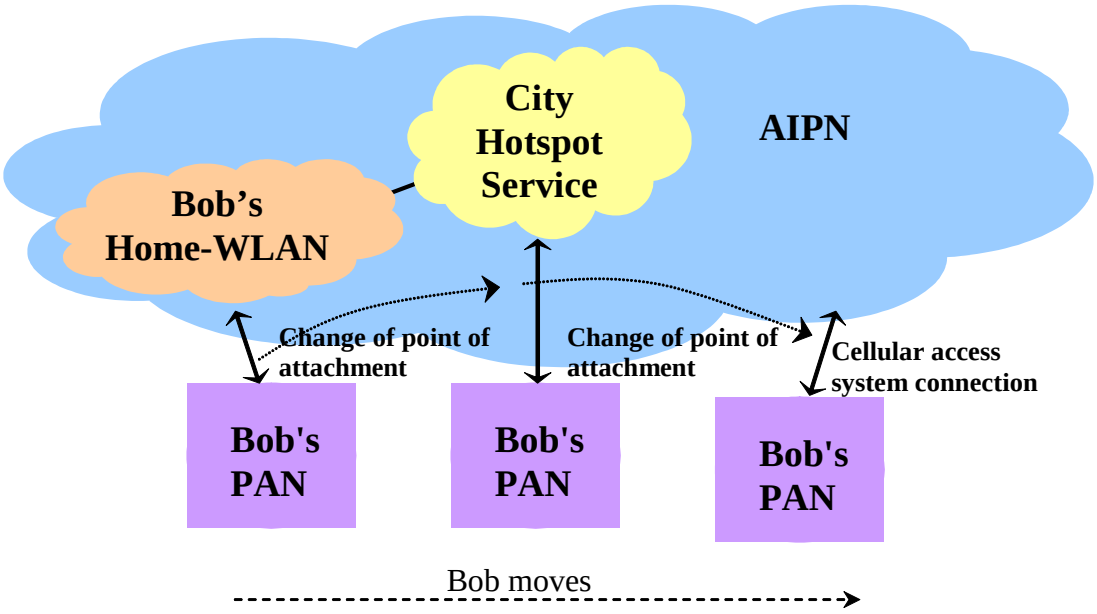


~~Alice and Bob are having a multimedia session with audio and video components using two high-end multimedia terminals in their offices. Alice needs to leave the office to take the car to visit a customer. She requests a session transfer. AIPN then transfers the session to her mobile phone.~~

B.43 Facilitate integration of networks with different administrative domains (e.g. handle negotiation of administrative issues, security, trust, etc)

Use case:

The following picture illustrates this use case.



Bob has his own ~~personal area network~~Personal Area Network (PAN). While at home, this network is composed with the Home Area Network using WLAN, which in turn connects externally with a local hotspot service, which in turn connects to a cellular network. Bob's PAN, Bob's Home-WLAN, the local hotspot service and the AIPN cellular access system are under different administrative domains. Still, if Bob moves outside coverage of his Home-WLAN, his PAN will communicate with the outside world via the local hotspot service. If he moves outside coverage from the hotspot service, his PAN will communicate with the outside world via the AIPN cellular access system.

Annex C (Informative): Use cases for Security

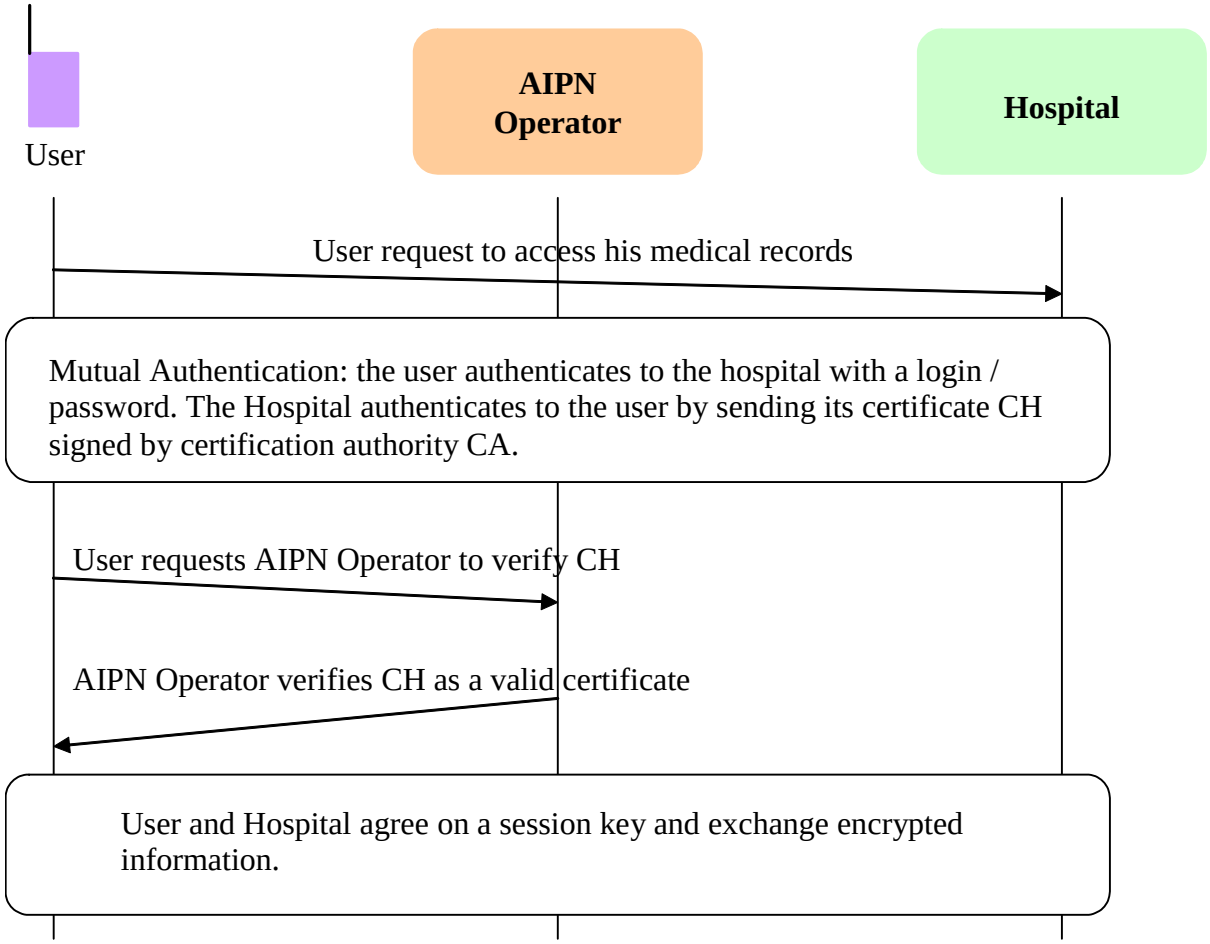
C.1 User issues

C.1.1 Ensure privacy and authenticity so that the user can trust the information he is receiving. This should cover private user to private user communications as well as private user to service provider communications

Use case:

~~u~~Using the AIPN operator as a certificate checking authority.

The figure below illustrates this case:



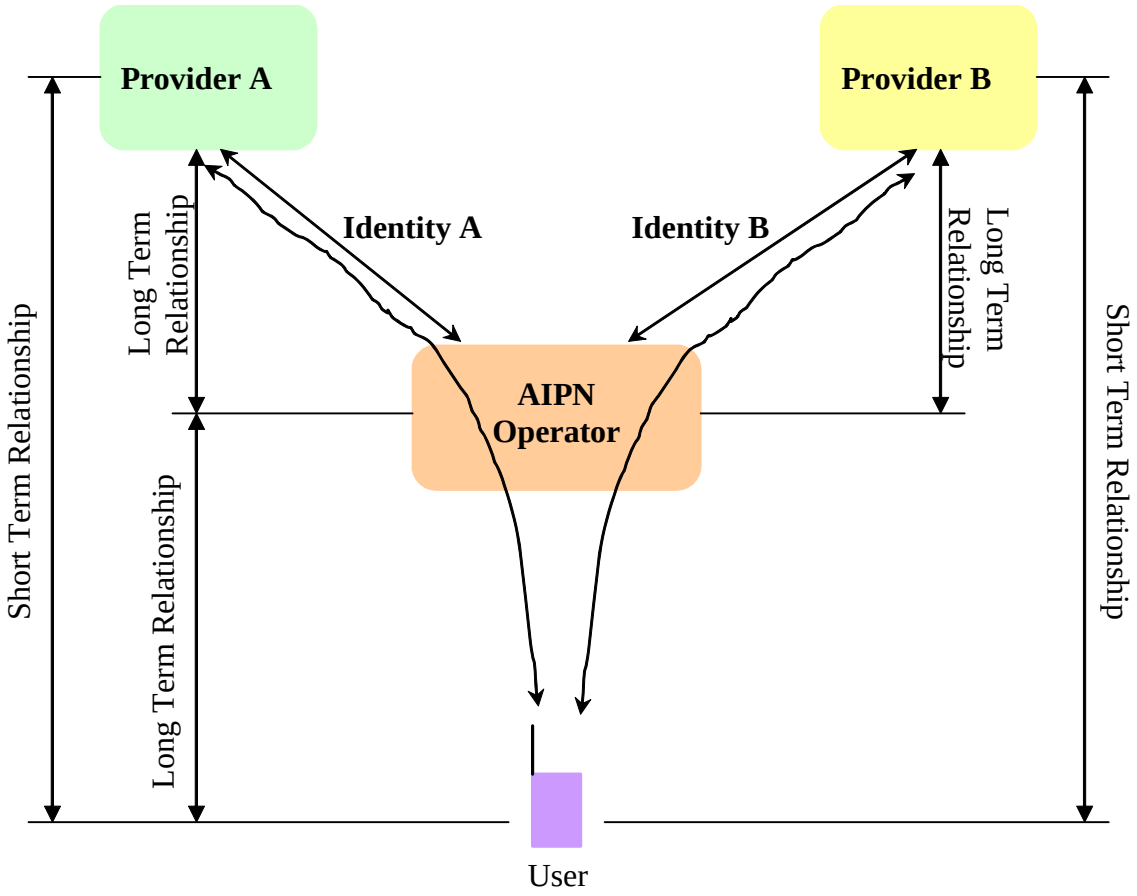
A user wants to access his medical records, stored in the hospital server, with his mobile terminal. The user connects with the hospital and authenticates itself. The hospital authenticates to the user by sending a certificate CH signed by certification authority CA. The user, however, does not recognize CA and asks the AIPN operator to check the validity of CH. The AIPN operator checks the validity of CH and informs the user about the positive result. At that point the user is sure that the information is really coming from the hospital.

C.1.2 Multiple user identities: Users should be able to have multiple identities from different providers, with the relationship between identities hidden to particular providers (thus supporting privacy)

Use case:

~~t~~The AIPN operator generates temporary identities for the user to be used towards different providers.

The figure below illustrates this case:



The user wants to connect to two providers but keeping full privacy. The AIPN operator enables this possibility by acting as a mediator. The AIPN operator allows the user to gain access to the two providers with completely different identities. Both identities are temporary ones and can not be correlated in any sense by just looking at log records in Provider A and Provider B.

In order to enable this type of service, the providers have to establish a "trust relationship" with the AIPN operator, so that he can perform accounting towards that AIPN operator for the services provided to the AIPN operator's subscribers.

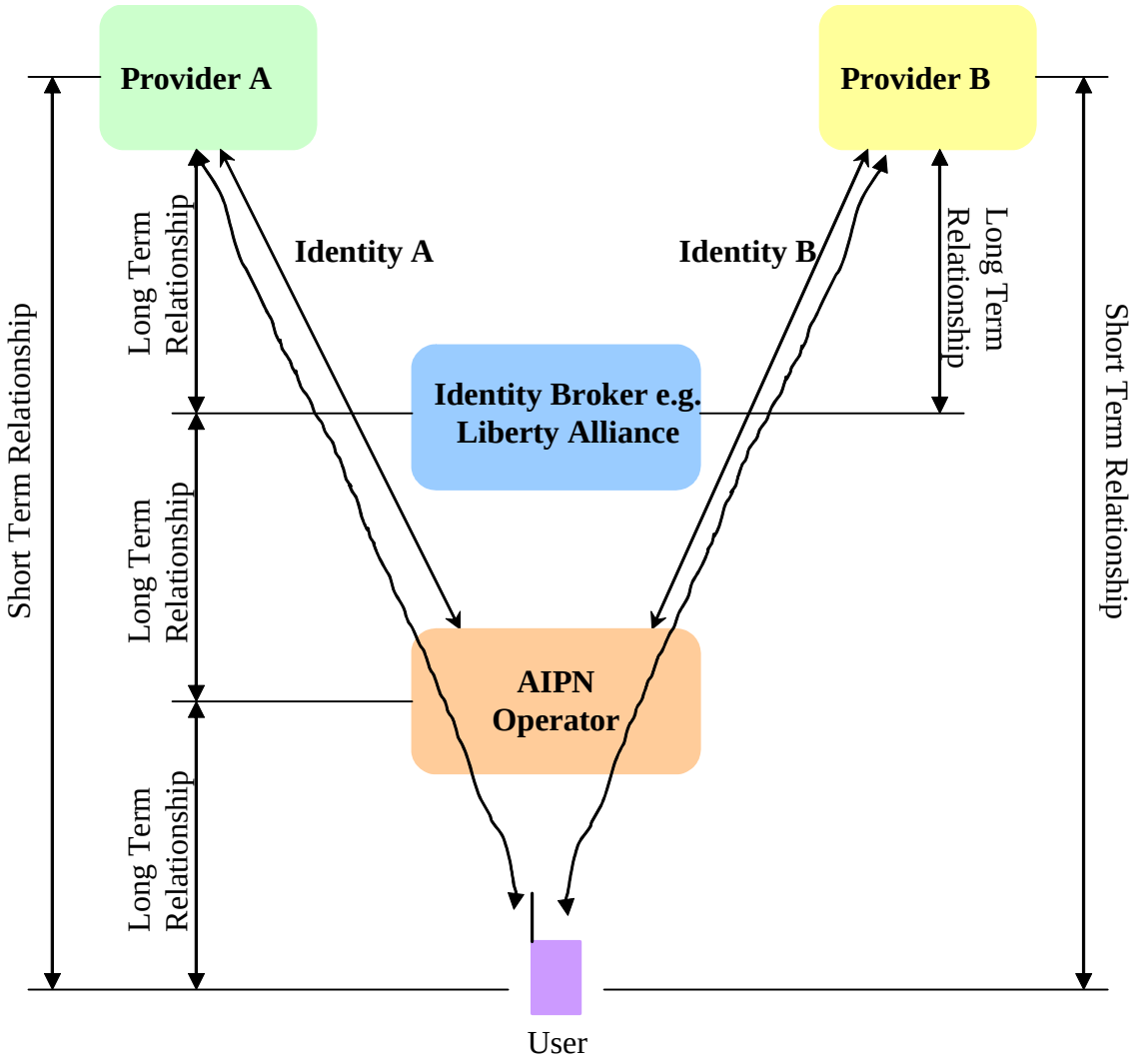
The user already has a long term relationship with the AIPN operator, and will be billed by the AIPN operator for services he accesses via external providers.

The AIPN operator does know the user's real identity and the temporary pseudonyms that he has given to the user to access services from external providers. The AIPN operator can then correlate the real and temporary identities for billing purposes.

Use case:

tThe AIPN operator generates temporary identities for the user to be used towards different providers. An identity broker, e., g., Liberty Alliance, acts as the long term trust relation centre.

This use case is similar to the previous one, but in this case the AIPN operator does not have a long term trust relationship with the providers, instead the AIPN operator has a long term relationship with an identity broker, e.g. Liberty Alliance, and the identity broker has a long term trust relationship with the external providers. This case is illustrated in the figure below:



The user wants to connect to two providers but keep full privacy. The AIPN operator enables this possibility by acting as a mediator. The AIPN operator allows the user to gain access to the two providers with completely different identities. Both identities are temporary ones and can not be correlated in any sense by just looking at log records in Provider A and Provider B.

The AIPN operator however, does not have a trust relationship with the providers but has one with an identity broker e.g. Liberty Alliance. The providers also have a trust relationship with the identity broker. So the identity broker is used as the common trust point to for the providers to offer services to the AIPN operator's subscribers. The AIPN operator can offer these services fully protecting the privacy of its subscribers.

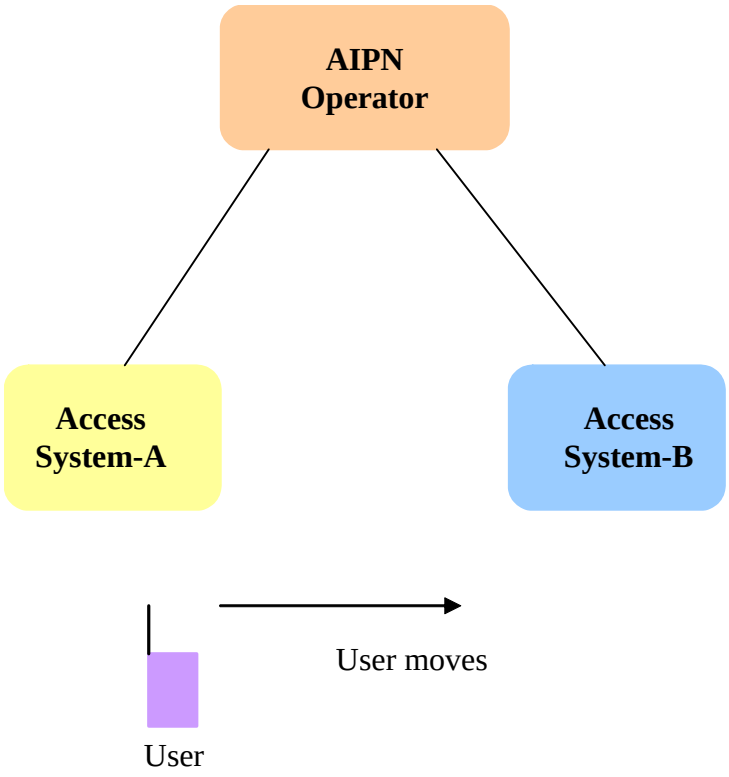
C.2 Network issues

C.2.1 Fast re-authentication shall be possible

Use case:

F~~f~~ast re-authentication in handovers between access systems.

The figure below illustrates this case:



The user is initially connected to Access System-A and has a session with several media established. He moves towards Access System-B, which may be under a different administrative domain than Access System-A. In this case there are mechanisms for fast authentication to continue communication across Access System-A and Access System-B.

Note: In this case the user's terminal needs to support each of the access systems

Annex D (Informative): Security Issues

These issues are very high level and many aspects need to be investigated further to be able to specify them more clearly. This could e.g., include:

- Investigating how and where to realize policy enforcement functionality to get the most general, efficient and secure solution to protect the end-users and the AIPN operators' networks.
- Reviewing architectural and protocol features to get a better understanding of how to protect the network against attacks such as denial-of-service.
- Investigate how to develop a homogenous SSO concept taking privacy and anonymity requirements into account.
- Investigating the need for end-to-end security solutions.

In summary, the challenges will be in understanding the new risks to identify any new or lacking security requirements, and of course finally ensuring that the right mechanisms are in place.

To mitigate the problems and protect users and systems and to deter from attacks different types of policy enforcement functions are needed to build trusted domains. Policy enforcement should cover

- Available network services. General purpose IP access may be restricted or tunneled securely through the network.
- Traffic/content inspection in the AIPN to stop download of malware and intrusive content.
- Spam control
- Blocking of no~~t~~n-~~-~~trusted services and service providers
- Traffic separation
- Traffic origin (e.g. prohibit source IP address spoofing).

There will be a need for policy enforcement controlled by end-users and by AIPN operators and a need to investigate how and where to realize policy enforcement functionality to get the most general, efficient and secure solution.

End-user policy enforcement will become a very important function, which AIPNs will have to provide. One particularly important area is to control distribution of location information. However, presence information in general could be just as sensitive.

For protection against denial-of-service attacks, architectural and protocol features have to be reviewed**.**

D.1 Trust domains

Often, the only means to deter attackers and mitigate threats are to build logging and detection systems to make the risk of getting caught sufficiently high. Thus, it will be critical to define trust domains, means to establish trust, authenticate and authorize users and systems, and put requirements on trusted hardware (especially end-user equipment). A key issue is if monolithic mobile phones can become the trusted devices in which AIPN operators can enforce different policies.

A specific issue is how to design the trust model when ad-hoc extensions of access systems are offered by ordinary end-user equipment. Should all such traffic just be tunneled through the ad-hoc extension or should there be some policy enforcement performed. There is also the question of who is responsible for the traffic from the ~~ad-hoc network~~Ad-hoc Network. Either the originating device of the traffic or the relaying device (or both) has to be responsible. Since they belong to different end-users, maybe having different AIPN operators, this may pose a problem.

Another issue is how to enforce policies in multi-access system environments. One threat scenario is that a user connects his device to two different domains with different “trust levels”.

D.2 Trust establishment

There is a need for different trust establishment mechanisms e.g. for end-users towards AIPN operators, end-users towards service providers, between end-user and between service providers. These mechanisms may be identical but could also be based on different principles if that would make them more efficient.

The natural choice for authentication of end-users towards AIPN operators is of course (X)SIM based. However, public key based systems may have advantages for other situations. The DRM solutions also show the need for secure authentication of trusted hardware.

A basic end-user requirement is that security mechanisms should be automatic and invisible to the end-user. User authentication and authorization should be able to be performed with a minimum of user interaction. At the same time, legitimate requirements on user privacy and even anonymity should be able to be catered for. Current work in SA3 (GAA/GBA) and Liberty show that there is a need for simple and uniform trust establishment mechanisms for service provisioning at different levels.

To increase user convenience, make systems less complex, simplify application development a common, standardized, homogenous SSO system taking privacy and anonymity requirements into account is needed. Today, we are moving towards a situation in which we have a set of diverse user authentication and authorization mechanisms tailored for different services.

D.3 Network heterogeneity and traffic protection

Specific issues that need to be reviewed are

- Location of the network point of trust. Network point of trust means the first network point at which user payload traffic is available in plaintext format. Simultaneous multi-access should be taken into account.
- Should user authentication and key agreement be performed on layer 3 (IP-layer) to enhance “portability”.
- Layer 2 protection is needed to protect system signaling and protect against Denial of service attacks. How to establish keys?
- How to handle the situation that in the future user payload traffic and end-user equipment control signaling traffic may have different endpoints in the AIPN
- New means to derive and distribute keys based on an initial user authentication.

D.4 End-to-end protection

With the introduction of IP based conversational multi-media over an AIPN, many users could feel a need for better end-to-end protection of their communication. A natural first step would be to introduce end-to-end integrity protection to guarantee the authenticity of data. Confidentiality of data may also be required (e.g. government agencies). Thus, the AIPN should be designed to allow efficient end-to-end protection of multimedia sessions. Here it might be beneficial to deploy (new) generic protocols for key management and data protection to limit signaling and computational load in the terminals. Lawful intercept requirements have also to be considered.

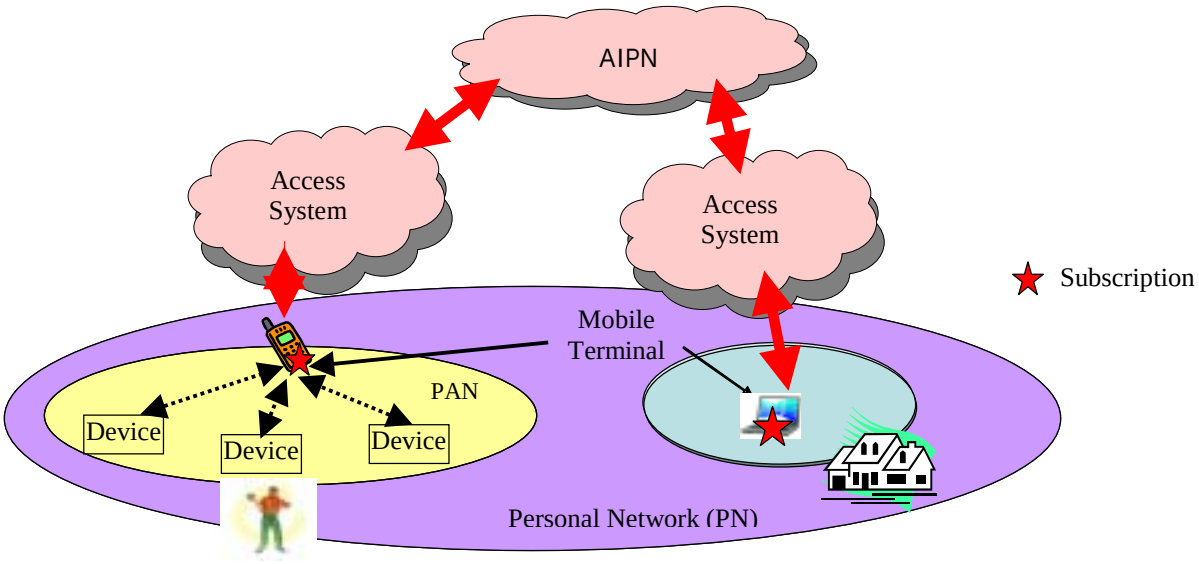
Annex E (Informative): Use cases for Personal Network (PN), Personal Area Network (PAN), Ad-hoc Network and Moving Network Support

The following use cases are intended to provide some examples of how the AIPN is impacted by major categories of user networks. This should not be considered an exhaustive list of possible use cases~~,~~. ~~the d~~Detailed consideration of the networking of user terminals is for further study.

E.1 Personal Network (PN)

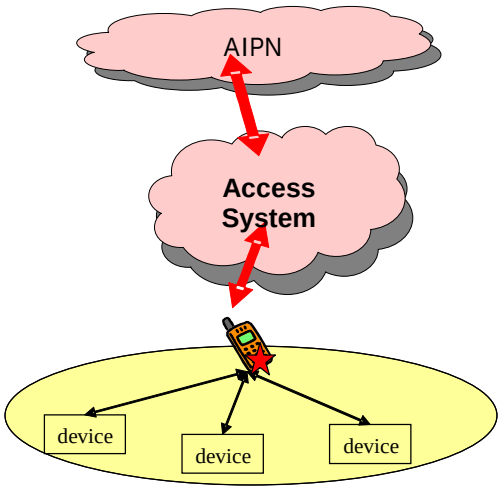
E.1.1 Use case 1: PN with the terminal away from the user

The AIPN provides a connection between the user's personal terminal and a terminal connected to the PC in his home such that the user is provided with a virtual secure ~~personal network~~Personal Network. Through this secure link, a user is able to synchronise his 3GPP terminal with data contained on his PC at home or monitor his heating or burgular alarm system while away from his home. Additional devices would enable connection to the user's car or holiday home.



Use case 1: PN with the terminal away from the user

E.2 Personal Area Network (PAN)



Connection of PAN devices to an AIPN via a mobile terminal

E.2.1 Use case 2: Multiple devices held by the same user

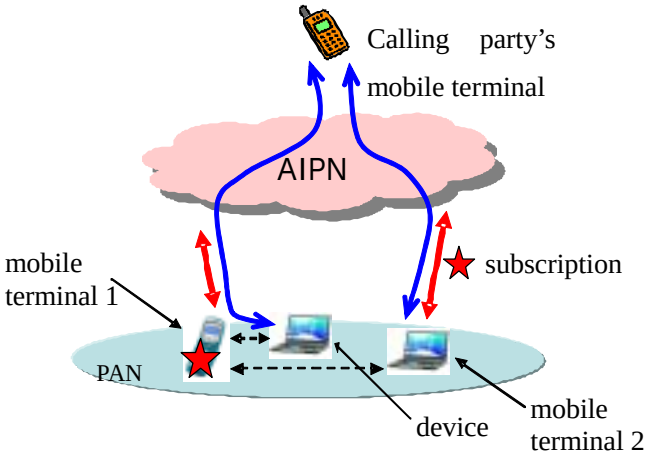
A user will carry a plurality of devices (PDA, music player, laptop, camera, headset, etc.) as well as mobile terminals with him/her. Each of them has a demand to access services provided by the AIPN or to communicate with another entity through the AIPN, but they might lack a USIM and/or a means to directly access to the AIPN.

A mobile terminal, containing a USIM, with short-range wireless connectivity (e.g. IEEE 802.15) can connect to other devices with wireless access when they are close to each other to form a small network called a *Personal Area Network (PAN)*, which is controlled by the user of the mobile terminal.

A calling party may request a call indicating the particular terminal/device within the PAN subject to service attributes and terminal/device capability.

E.2.1.1 Use case 2a: Subscription data within one device only

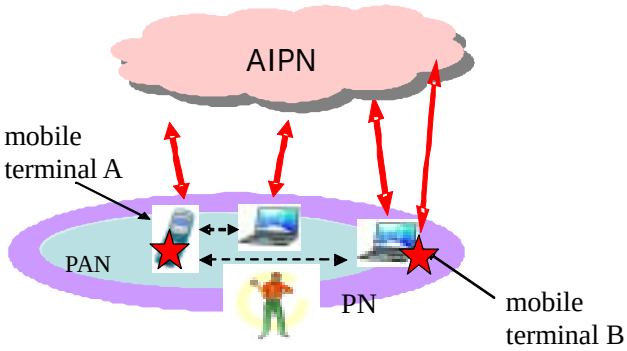
When only one device (~~i.e.~~ mobile terminal 1) holds a USIM and another device (~~e.g.~~ mobile terminal 2) does not hold a USIM but has a means to access the AIPN, mobile terminal 2 will be authorized to access the AIPN using the USIM in mobile terminal 1. The data transfer channel (i.e. transport and session) can be established and maintained through the access means of mobile terminal 2 ~~itself for~~ as long as mobile terminal 2 can access the USIM through the PAN. If the mobile containing the USIM is removed from the PAN all service sessions, other than those on the mobile containing the USIM, will be terminated immediately.



Use Case 2a: Subscription data within one device only

E.2.1.2 Use case 2b: Relationship between Personal Network and Personal Area Network

Devices close to the user are connected using internal PAN means and share a USIM authority for the devices so connected. ~~-~~A device containing an independent USIM may be removed from the PAN yet still remains connected to the user's Personal Network ~~of the user~~ through the AIPN.



Use case 2: Relationship between PAN and PN

A user has a PAN consisting of a number of devices, including a personal device, mobile terminal A, and a device that remains in the user's vehicle, mobile terminal B. Mobile ~~T~~terminal A and mobile ~~T~~terminal B each contain a USIM. While close to the user, and connected using the internal PAN means, communication between mobile terminal A and B (e.g. synchronisation of a database) is achieved directly via the PAN. When the user leaves his vehicle, the PAN connection is lost and mobile ~~T~~terminal B continues to connect to the Personal Area Network (e.g. to continue the synchronisation process) through the users Personal Network by connecting through the AIPN using the USIM contained in Terminal B.

E.2.3 Impact on an AIPN:

For reliable billing information ~~for~~ in all the PAN use cases it is essential that the appropriate USIM is correctly associated with every request for ~~S~~services from the AIPN. Possible causes of double counting, attributing a service request to the wrong user, or other causes of incorrect billing, must be eliminated.

E.3 Ad-hoc Network

E.3.1 Use Case 1: Formation of an Ad-hoc Network

In this use case, a number of users interconnect their terminal devices to form an Ad-hoc Nnetwork. These terminal devices may be capable of connecting to different access systems. The Ad-hoc Network enables its members to access the AIPN through any of the terminal devices that are able to connect to a suitable access system. Each member of the Ad-hoc Network uses their own USIM to obtain whatever services they are individually entitled to use.

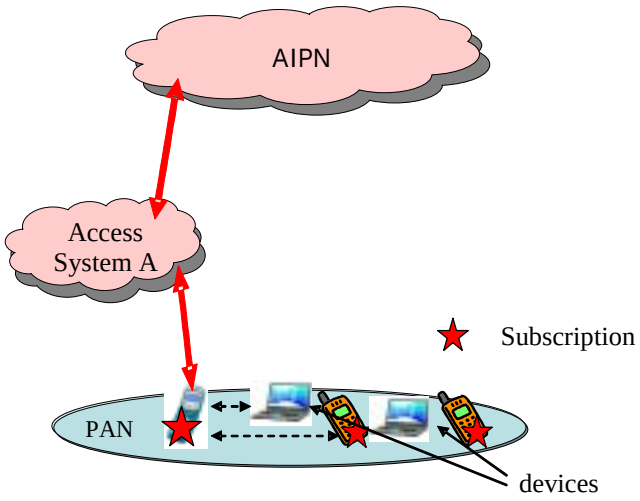
E.3.2 Use Case 2: Movement of an Ad-hoc Network

The Ad-hoc Network may change the terminal device used to forward the consolidated traffic to the AIPN as required. Reasons for change could be;

1) Movement of the connected terminal device within the Ad-hoc Network causing it to loose service while another terminal device gains service (not necessarily using the same access system).

2) It may be financially advantageous to the group of users for their consolidated traffic to be routed through one particular access system depending on their location or time of day. -The users of the Ad-hoc network Network may cause their Aad-hoc Nnetwork to change access system simply to maintain their fiscal advantage rather than for reasons of access system coverage etc..…

E.3.3 Use case 3: Multiple users within the home

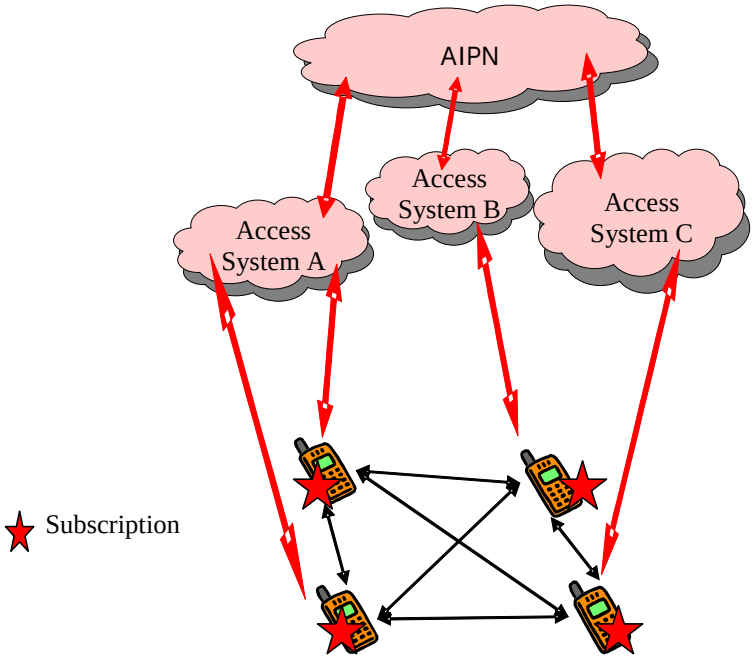


It is possible for a home network to have multiple users. For example, a family may consist of a group of users who share the various devices on a home network through the mechanisms described in Use Case 1 & 2. From an AIPN perspective they should be seen as independent users, each with capabilities as defined in the use cases above. The AIPN need not be aware that they share the same home network.

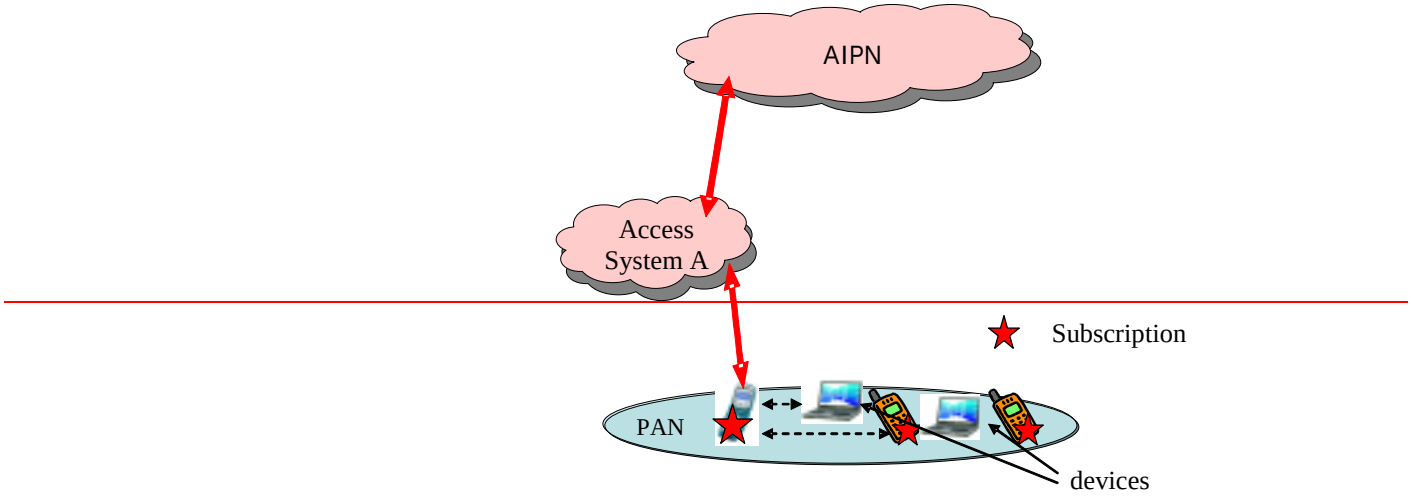
Note: The demands of this use case on the individual terminal devices is considered beyond the scope of this document.

E.3~~.3~~.4 Impact to an AIPN

The AIPN will see consolidated traffic from a group of separate users arriving through an access system. The access system bearing the consolidated traffic may change at any time with no warning to the AIPN. Elements of the consolidated traffic could originate from a PAN.



~~E.3.4 Use case 3: Multiple users within the home~~



~~It is possible for a home network to have multiple users. For example, a family may consist of a group of users who share the various devices on a home network through the mechanisms described in Use Case 1 & 2. From an AIPN~~

~~perspective they should be seen as independent users, each with capabilities as defined in the use cases above. The AIPN need not be aware that they share the same home network.~~

~~Comment: The demands that this places on the individual terminal devices is for further study and is considered beyond the scope of this work item.~~

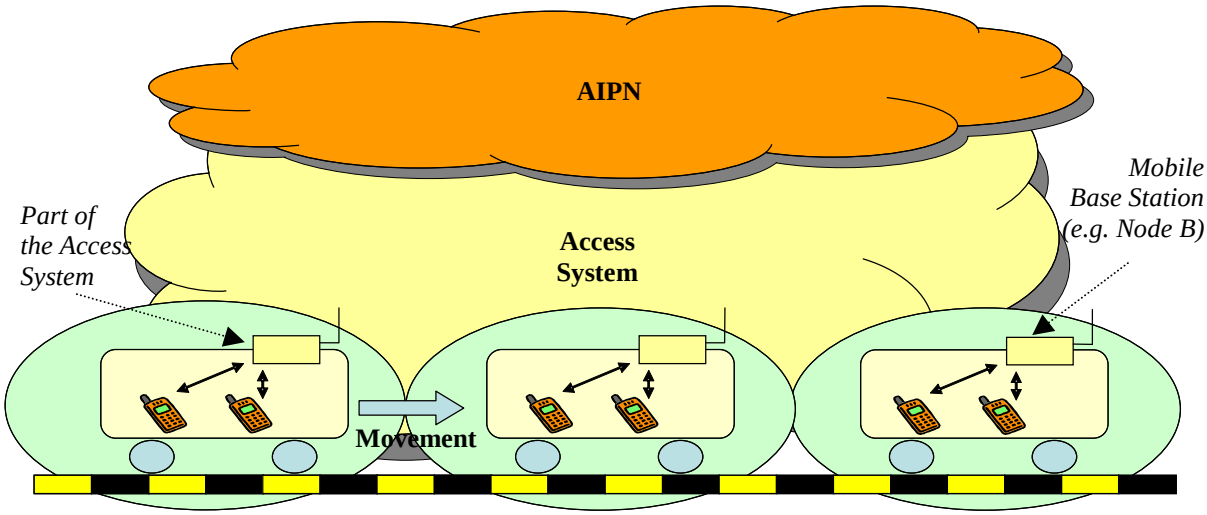
E.4 Moving Network

A Moving Network provides access to AIPN for a group of users that move together (e.g. as part of a vehicular network). The devices (terminals) of a M~~m~~oving N~~n~~etwork are connected to a well-defined system (gateway) through which the user devices (terminals) in the M~~m~~oving N~~n~~etwork gain access to the AIPN.

Note: This is a key difference to ~~a~~Ad-hoc N~~n~~etworks, where access to the AIPN can be gained through any device (terminal) that has access.

E.4.1 Use case 1: Moving Base Station

A moving base station (e.g. a pico cell) is responsible to provide radio access to user terminals in a ~~m~~Moving ~~n~~Network. The moving base station is part of an access system and is owned by the AIPN operator providing the access network. As the access system fully accommodates the M~~m~~oving N~~n~~etwork, it dominates the wireless technology that can be used to connect the user terminal to the AIPN.



In this use case, mobility for the ~~moving network~~Moving Network is provided by the access system only.

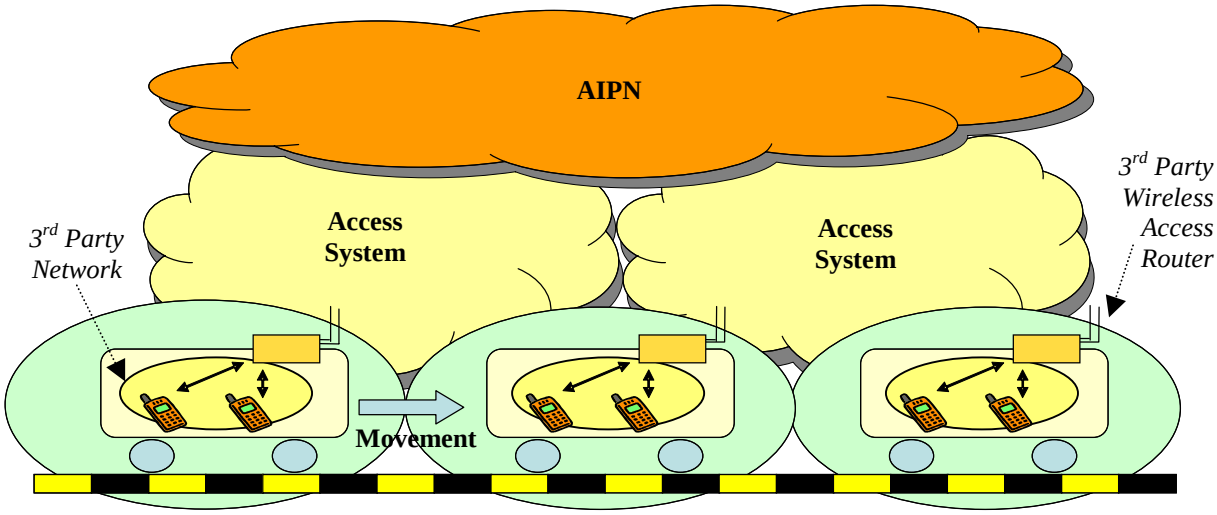
Note: ~~As t~~The AIPN may not see any impact resulting from a handoff of a ~~moving network~~Moving Network in this use case. The particular impacts of ~~, it is for further study whether~~ this use case upon the AIPN are for further study.~~should be included in this document.~~

Advantages of this approach:

- Low or potentially zero impact on the AIPN as mobility is completely handled by the access system (which accommodates the ~~moving network~~Moving Network)

E.4.2 Use case 2: Wireless Access Router

A wireless access router (e.g. a WLAN router), owned by a 3rd party network provider (e.g. the train company), is equipped with a means to connect to an AIPN~~-~~. This connection can be established via any access system that is supported by the wireless access router and for which the wireless access router has a subscription. The wireless access router consolidates traffic from users of the ~~moving network~~Moving Network towards the AIPN. A variety of wireless or wired access technologies can be used to connect user terminals to the wireless access router.



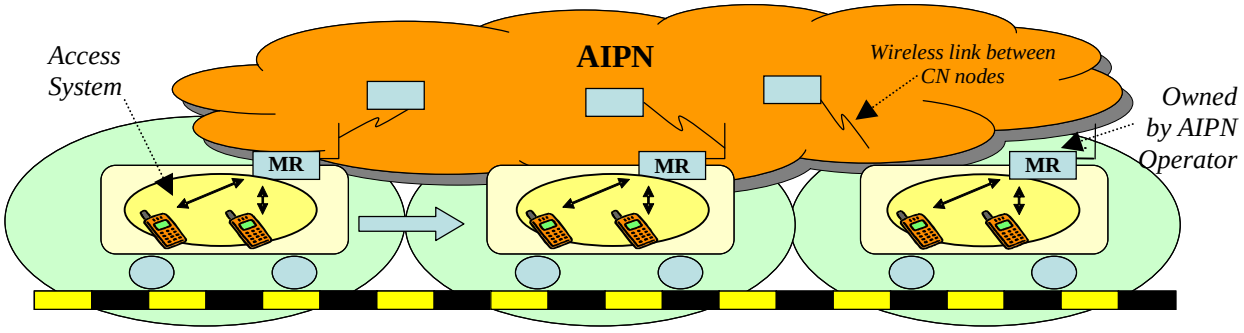
In this use case, mobility management is split between the AIPN and the access systems. While the AIPN takes care of the ~~network~~ handover when the ~~moving network~~Moving Network changes the access system, the access system provides mobility for handoffs between different cells of the access ~~network~~system.

Advantages of this approach:

- The ~~moving network~~Moving Network is not tied to a single access system; i.e. this approach provides more flexibiltye, as it allows the ~~moving network~~Moving Network to choose the best (e.g. most reliable, fastest, cheapest) access system at any time.
- It enables 3rd parties~~y network providers~~ to offer access to an AIPN ~~access~~.

E.4.3 –Use Case 3: Mobile Router

A mobile router, which travels together with a ~~moving network~~Moving Network, is equipped with some wireless technology that connects itself with the rest of the AIPN. In contrast to the above use cases, the mobile router is considered a component of the AIPN itself. The purpose of the mobile router is to provide the user terminals access to the AIPN. As such it serves as gateway between the ~~moving network~~Moving Network and the AIPN. A variety of wireless or wired access technologies can be used to connect the user terminals to the mobile router.



In contrast to the above use cases, here mobility of the mobile router is handled solely by the AIPN. The access system does not require any mobility functions.

Advantages of this approach:

- It allows simplification of the access system (i.e. single cell access network)
- Only a single mobility management component is required (i.e. mobility is only handled by the AIPN – not the access system)
- The access system does not require support for ~~moving network~~Moving Networks

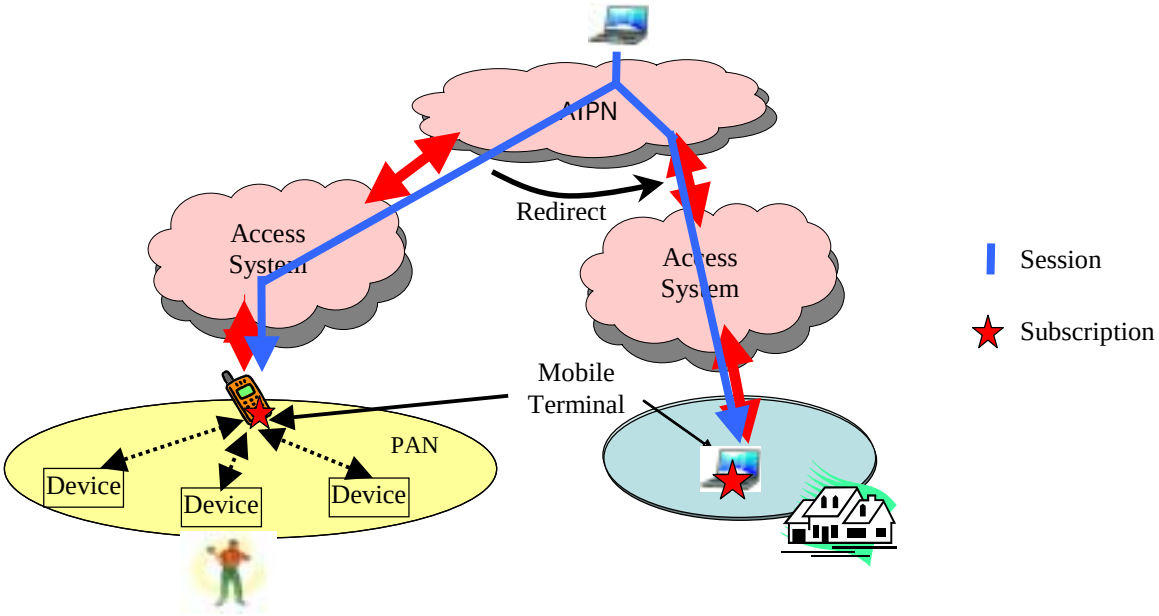
E.4.4 Impact to an AIPN

The access system for the consolidated traffic may change with time (e.g. as the train moves) in a manner that can reasonably be anticipated by the AIPN. Elements of the consolidated traffic from a ~~moving network~~Moving Network may originate from PANs or Ad-hoc ~~networks~~ Networks covered by the ~~Moving Network~~Moving Network.

Annex F (Informative): Use Cases for Session Mobility

F.1 Use Case 1: Redirection of a video stream to the terminal away from the user

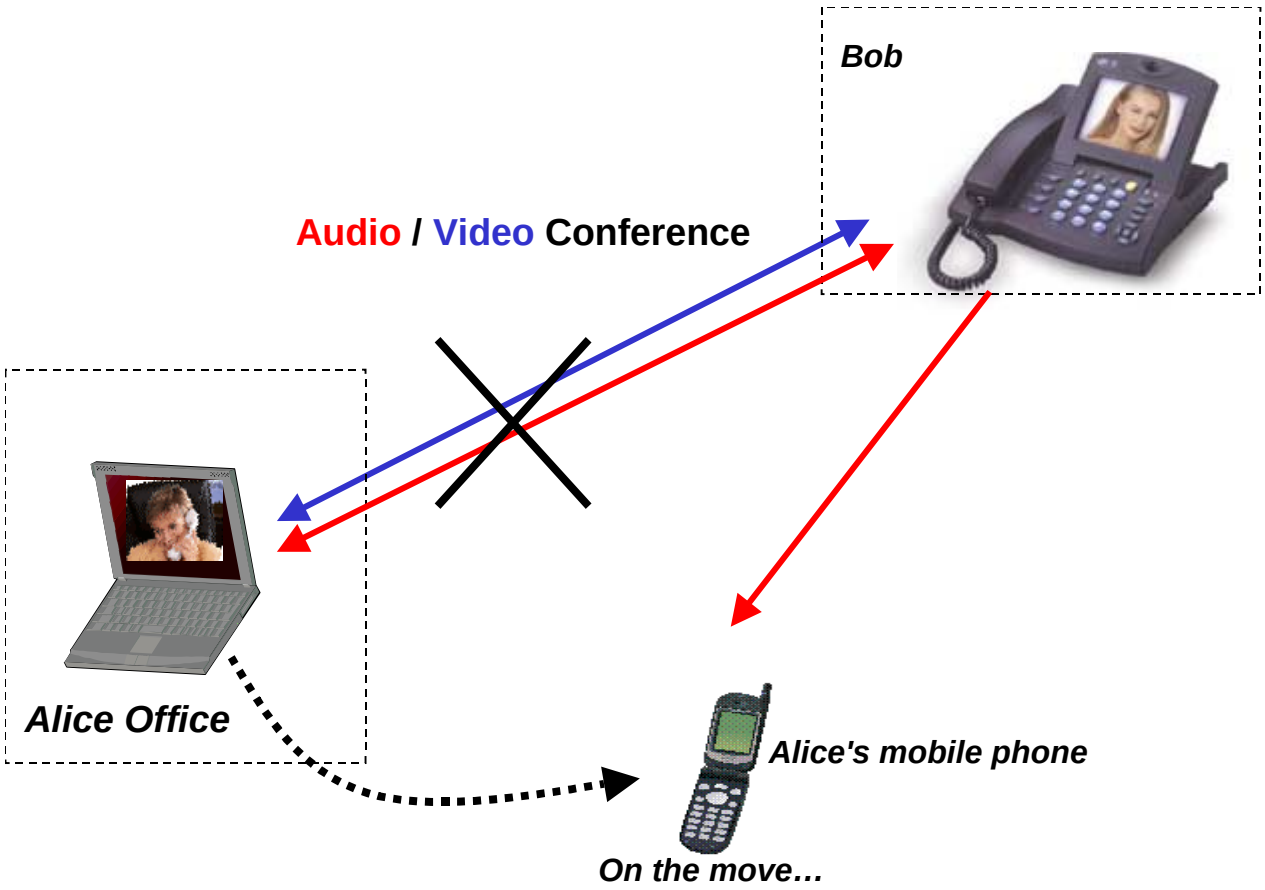
A user has ~~the~~ a PAN in ~~the~~ close proximity~~area to the user~~ and ~~the~~ another terminal in his/her home some distance away ~~from the user~~. A user can use any of their devices (terminals) ~~for his/her use~~. In this use case~~,~~ the AIPN manages multiple devices (terminals) in different locations as belonging to the same user, and can redirect a session to another terminal. Then, for example, when the user receives a video streaming session but does not have enough storage resource in ~~his/~~her terminal, the user is able to redirect the session to ~~be~~ the terminal in his/her home and store the video stream in ~~his/~~her PC.



Use case: Redirection to ~~the~~ a terminal some distance away from the user

F.2 Use case 2: Seamless mobility of sessions between terminals

This use case is illustrated in the figure below.



Alice and Bob are having a multimedia session with audio and video components using two high-end multimedia terminals in their offices. Alice needs to leave the office to take the car to visit a customer. She requests a session transfer. AIPN then transfers the session to her mobile phone.

End of changes

CR-Form-v7.1

CHANGE REQUEST

⌘ **22.978** **CR** **004** ⌘ **rev** **-** ⌘ Current version: **7.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☐

Title:	⌘	Alignment and improvement of recommended requirements and conclusions of TR 22.978
Source:	⌘	SA1 (AIPN Rapporteur (NTT DoCoMo Inc.))
Work item code:	⌘	AIPFS
Date:	⌘	04/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-7

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*
Rel-7 *(Release 7)*

Reason for change:	⌘	Although the conclusions of TR 22.978 should list all the recommended requirements identified throughout the Technical Report this is not the case at present. This Change Request aligns the identified recommended requirements' with the conclusions of TR 22.978. Additionally, two similar recommended requirements are contained within two different sections of TR 22.978. Therefore, it is necessary to merge these into a single recommended requirement.
Summary of change:	⌘	Alignment of the identified recommended requirements with those listed within the conclusions of TR 22.978. Combination of recommended requirements within chapter 5.1.1.6 and 6.2.2.1 into a single recommended requirement within chapter 6.2.2.1. Further corrections to the content of Chapters 6 and 7 to improve readability.
Consequences if not approved:	⌘	The conclusions of TR 22.978 will be incomplete and duplicated/ambiguous text will remain. This could result in confusion when TR 22.978 is referenced and an inappropriate understanding of the conclusions and content of TR 22.978.

Clauses affected:	⌘	5.1.1.6, 5.2.1.4, 6, 7

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	

	X	O&M Specifications

Other comments: ⌘

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

1st Modified Section

5.1.1.6 Access system selection

In an AIPN the applications are based on IP and will evolve towards access system independence. An AIPN is expected to support multiple access systems.

The selection of the access system may need to take into account several aspects of an AIPN, e.g. service requirements of an application, load balance of the network, and charging & billing.

~~Recommended requirements:~~

- ~~The AIPN should provide a means to enable access system selection based on a range of criteria e.g. user preferences, service requirements of applications, network conditions or other AIPN operator defined criteria.~~

Next modified section

5.2.1.4 Network and mobility

- An AIPN shall be designed as a common IP-based network system, hence evolution of the 3GPP system to an AIPN shall be realised with minimum duplication of network functionality wherever possible.
- Evolution of mobility mechanisms

  In the evolution towards an AIPN, the integration of the telecom and datacom worlds, which has been discussed for a long time, materializes. The integration of WLAN into 3GPP systems is already a good example of this. As part of this trend, the mobility mechanisms must be evolved.

  Nevertheless, new mobility mechanisms of AIPN must be introduced in such a way that there is a migration path from current 3GPP systems (i.e., Rel-6). New features, nodes or protocols should be introduced such that an incremental introduction is facilitated.

  Specifically, the large installed base of UTRAN and GERAN based access systems must continue to be supported. In the AIPN, mobility mechanisms must be able to co-exist with current PS core network mobility mechanisms in a cost-efficient way.

Recommended requirements:

- An AIPN mobility solution must support UTRAN and GERAN based systems as possible access systems besides supporting alternative existing accesses such as WLAN and other emerging new technologies.
- An AIPN mobility solution must be able to co-exist with the current 3GPP PS core network in a cost-efficient way.
- An AIPN mobility solution should support seamless terminal mobility across various access systems.
- AIPN should support services handover between 3GPP CS services (e.g. CS telephony) and AIPN equivalent services (e.g. V~~v~~oice over IP).

Next modified section

6 Capability expansion required for the introduction of an AIPN

The AIPN vision provided in chapter 5 of this Technical Report lists the desired capabilities of an AIPN. This chapter provides a detailed gap-analysis between the existing capabilities of the 3GPP system and the capabilities of an AIPN. Based on this analysis it will be possible to obtain a clear picture of the work that needs to be undertaken within 3GPP to evolve to an AIPN.

6.1 Existing capabilities suitable for an AIPN

Note: The term "3GPP system" used within this chapter refers to the 3GPP system as specified up to and including Rel-6.

It should be possible to evolve the 3GPP system to an AIPN without degradation in the capabilities [5] of the current 3GPP system whilst also maintaining the 3GPP system service principles [4]. More specifically, the following capabilities provided within the ~~22 series of~~ 3GPP specifications are felt to be suitable for an AIPN:

- Provision of IMS services [6]
  - Support for IP multimedia sessions
    - IP Multimedia Session control [4]
  - QoS for IP multimedia sessions
  - Support of multiple UEs with a single IMS subscription.
- Cost effective Control and Charging of IP Flows through FBC [7]
  - Identify IP flows for charging and policy control in a generic manner
  - Perform Real Time Charging
  - Support differentiated charging including zero rating of the bearer and event charging
  - Authorization of IP Flows
  - Awareness of user identity, subscription class, time-of-day, roaming status, QoS, Service input etc

6.2 New capabilities required for an AIPN

An AIPN will enhance the 3GPP system from the perspectives of providing enhanced functionality as well as improvements in system performance (e.g. communication delay, communication quality, connection set-up time).

6.2.1 Enhanced network performance

Together with the diversification of the services, requirements for network resource utilization will become diversified. It is necessary that network resources, especially the wireless resource, be used effectively and efficiently, including selection of the access system used based on the provided service.

The main traffic use case when defining~~, although~~ the connection and routing methods of the current PS domain has been user-to-server communication. However~~,~~, user-to-user communication is expected to increase more and more as services and service usage diversifies. Therefore, it is necessary that an AIPN provides the ability to efficiently handle a variety of different types of IP traffic and has optimized routing mechanisms, in particular for user-to-user traffic.

Recommended requirements:

- An AIPN shall provide the following features:
  - Ability to efficiently handle a variety of different types of IP traffic including user-to-user and user-to-multicast traffic models

- Optimized routing of IP traffic, in particular for user-to-user traffic.

- Efficient usage of radio resources (e.g. signalling optimization, compression), including selection of access system, based on the provided service.

6.2.1.1 IP-based routing and addressing

Due to future increases in the number of users and terminals accommodated by mobile networks it is necessary to ensure that addressing and routing schemes can accommodate a number of users and terminals significantly greater than the present number of mobile subscribers. Due to the limited amount of available MSISDN numbering capacity it would be desirable to be able to accommodate new users and terminals without the need to associate an MSISDN with terminals for which there are no need to receive calls addressed to E.164 numbers.

Moreover, adoption of 3GPP specific technology in existing 3GPP system results in cost increases for network operators (which are subsequently passed on to users) due to the need to deploy specialised network equipment. The use of specialised equipment also makes flexible service expansion difficult.

The use of IP technology is widespread which results in low costs for equipment based on IP technology. Moreover, the use of IP technology is standard throughout both the telecommunications and IT industries and it is necessary to enable the 3GPP system to be realised based wholly upon IP technology in the future. In particular, the use of IP technology for addressing and the routing technology within an AIPN is applicable.

Recommended requirements:

- An AIPN shall enable the accommodation of a vast number of users and terminals.

- Based upon industry trends IP technology shall be applied to the addressing and routing technology within an AIPN to enable accommodation of a vast number of users and terminals.

6.2.2 Support of a variety of different access systems (existing and future)

-Wireless coverage is different depending on the radio technology and the radio signals of each of the accesses used may not necessarily be available within a particular area. Also, in the future it may be possible for AIPN operators to realise cost reduction by efficiently introducing appropriate access systems within different geographical areas. Therefore, in order to facilitate efficient provision of services, an AIPN shall support accommodation of several access systems (existing and future). The 3GPP system currently provides access to the CS and PS domain via UTRAN and GERAN as well as access to PS services over I-WLAN. However,~~but~~ currently there is no detailed specification for accommodation of access systems other than those based on UTRAN, GERAN and WLAN. Therefore, it is necessary that the accommodation of access systems be expanded to include other different access systems within an AIPN.

Concerning the provision of IP based services an AIPN shall support provisioning of services over several access systems accommodated within an AIPN. However, there will be some differences for the provision of IP services over different access systems hence it shall be possible for an AIPN to coordinate service provision across a variety of different access systems.

Recommended requirements:

- An AIPN shall support accommodation of several access systems (existing and future).

  - An AIPN shall support service provision across different access systems.

  - An AIPN shall support adaptation of service provision across different access systems.

6.2.2.1 Access system selection

The introduction of multiple access systems within the same coverage area raises new AIPN operator and user requirements; the user may wish to influence the selection of the access system for use based on such aspects as supported QoS, mobility, pricing, coverage, etc. and the AIPN operator may wish to influence the access system selection by setting policies. Optionally, a user may even wish to use simultaneous multi-access as well.

Note that the selection of the access system needs to be easy for the end user, e.g., it could be based on some preferences and the actual process can be partly or completely hidden.

It is expected that users using multiple access systems will require an appropriate service continuity experience as they switch from one access system to another. This means that their sessions remain in operation, with minimal interruption. In addition, the services provided should be made access system aware (e.g., choose video quality based on the available bandwidth).

Recommended requirements:

- An AIPN shall enable use of ~~the~~ multiple access systems
- It should be possible to reach a user over multiple access systems simultaneously.
- It should be possible to provide access system-aware services.
- An AIPN shall provide support for access system selection based on combinations of AIPN operator policies, user preferences, service requirements of applications, ~~and~~ access system conditions, and/or other AIPN operator-defined criteria.

Note: The user preferences shall be respected as long as they do not negatively effect the operation of the system.

6.2.3 Enhanced Mobility

6.2.3.1 Heterogeneous Access Systems Mobility

An AIPN shall allow connectivity via a wide variety of access systems (both fixed and wireless). Some of these systems are specified by 3GPP where others are developed and specified by other organisations.

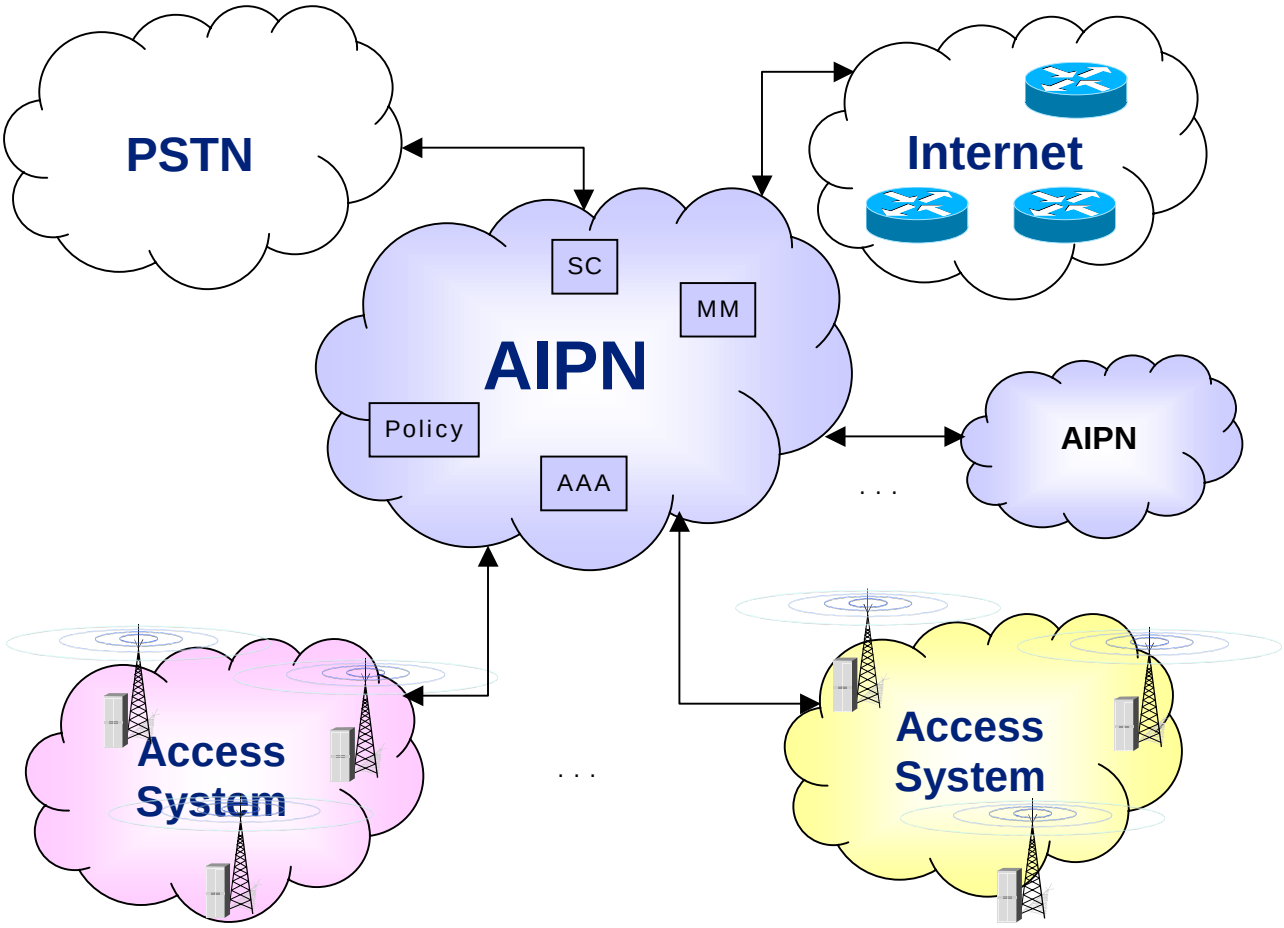


Figure 4: AIPN and Heterogeneous Access Systems

For the purpose of optimising the mobility among ~~the~~ diverse access systems, the AIPN shall provide open interfaces that allow the AIPN operator to direct the terminal towards the most suitable access system. The decision to move a terminal from one access system to another should be based on the information available in the AIPN e.g. load balancing, subscriber's profile as well as on the information provided by the terminal. Mobility within a given non-3GPP access system is not under the responsibility of the AIPN.

The AIPN should provide common open interfaces to allow the AIPN to exercise the control on the inter-access system mobility of the terminal. Furthermore, an AIPN should also provide other open interfaces that allow the terminal to access the other AIPN services needed for the management of the subscribers in the AIPN, i.e. session control, AAA, policy control~~.~~ (see ~~picture~~ figure 4 above).

Recommended requirements:

- An AIPN should provide open interfaces to AIPN services such as ~~MM~~ mobility management in order to ease the terminal mobility across different access systems.

6.2.3.2 Heterogeneous mobility mechanisms

An AIPN shall support not only a heterogeneous set of access systems, but also the inter-working of heterogeneous mobility mechanisms in the AIPN as well. This is needed because the AIPN will have to provide an evolution from currently deployed core network technologies. As an example, both legacy 3GPP PS mobility and IP based mobility schemes may co-exist.

In principle, AIPN should aim to minimise the number of different mobility solutions. However, adoption of multiple mobility solutions may be necessary in the AIPN due to the following reasons:

- The access system, terminal technology, the services or roaming agreements provided may put varying requirements on the AIPN mobility solution.
- The mobility mechanisms must also satisfy security, QoS or other requirements, which may also vary.
- The AIPN may incorporate multiple administrative domains.

Heterogeneous mobility mechanisms allow local optimizations. ~~E.g.,~~For example, parts of the AIPN may provide improved mobility performance by a solution that is tailor-made for the particular network configuration.

Recommended requirements:

- An AIPN must work with mobility mechanisms used by the specific networks it connects, including legacy mobility mechanisms of the current 3GPP PS core network.

6.2.3.3 Frequent mobility

Since an AIPN shall allow for multiple access systems optimized to particular user requirements, it will need to support access systems with highly varying characteristics in terms of robustness, quality and throughput as well as complexity and geographical coverage.

While 2G and 3G access systems provided a RAN with mobility support that can cover a large geographical area, an AIPN may need to accommodate access systems with RANs that provide mobility support only in a very limited area. In the extreme case, the access system may consist of base stations that are directly connected to the AIPN, or even access systems without any mobility management procedures at all.

Consequently, while in 2G and 3G networks most of the terminal mobility was handled in the radio access network and the core network had to handle only infrequent mobility, an AIPN shall support new access systems where handovers between AIPN nodes are also very frequent.

As a result, handover support in the AIPN has to provide a seamless user experience. Note that the corresponding performance requirements for a seamless user experience will depend on the service provided. This seamless user experience must be maintained even with an increasing AIPN size and increasing number of terminals.

Recommended requirements:

- ~~-~~An AIPN must support procedures related to frequent terminal mobility between AIPN nodes.

- Whenever feasible, the AIPN mobility solution must support seamless user experience for all services provided by the AIPN.
- The mobility solution must scale with the number of terminals and size of the AIPN.
- An AIPN shall be able to support access systems with very limited or no mobility management procedures.

6.2.4 Optimised IP session control

In principle it is assumed that session control within AIPN shall be optimised for user-to-user communication, i.e. from one user's mobile terminal to another user's mobile terminal, and for other traffic models such as those of streaming services, and shall be extended beyond IMS functionalities that are already provided. Some new session control mechanisms are introduced within an AIPN e.g. session mobility, session adaptation to terminal capability and session control for user to multicast.

Additionally, it is necessary for an AIPN to ensure efficient use of wireless resources and effective usage of power resources within mobile terminals whilst maintaining the appropriate usability for a particular service.

Recommended requirements:

- ~~-~~The IP session control mechanisms of AIPN shall be enhanced from the functionalities of IMS to provide session mobility, session adaptation to terminal capability and session control for user to multicast.
- Users shall perceive continuous service whilst ensuring the efficient use of wireless resources and the effective usage of power resources within mobile terminals.

6.2.5 Enhanced support of IP traffic

An AIPN will provide a variety of new mechanisms to support IP traffic.

6.2.5.1 Support of increased IP traffic demand

As the number of users accessing multimedia and data services from 3G networks will continue to accelerate, huge amounts of IP traffic are expected to be generated in the AIPN. Therefore, an AIPN must be able to accommodate a large increase of IP traffic whilst being able to guarantee QoS for different services, i.e. ensure that quality conditions for a particular communication are fulfilled without deterioration between the communication end-points, and ~~ensuring~~ ensure that network resources are used efficiently. This will enable the additional cost to AIPN operators to be minimised.

Advanced QoS control mechanism and traffic engineering techniques are possible methods to achieve better IP traffic performance and increase the efficiency of the AIPN resource usage.

Recommended requirements:

- An AIPN shall be able to provide guaranteed QoS for services and use AIPN resources with high efficiency i.e. ensure that quality conditions for a particular communication are fulfilled without deterioration between the communication end-points.

  Possible methods to achieve this within an AIPN include:

  a) The ability to control routing of IP traffic dynamically according to the actual resource usage condition from an end to end point of view which includes the end user devices, network entities and application servers. This could be achieved by using intelligent QoS routing algorithms taking into consideration of resource usage conditions.

  b) The ability to be able to monitor the AIPN entities statistics in real time, e.g. current reserved resources, un-used resource in order to route IP traffic dynamically based on network conditions.

6.2.5.2 Ability to effectively handle a variety of different types of IP traffic

An AIPN is expected to handle different types of IP traffic:~~,~~ real-time (e.g. VoIP), non-real time (e.g. Web browsing)~~,~~ and mission critical (e.g. M-Commerce). However it is not easy to predict the traffic model in an AIPN. Sometimes it will need to handle a large amount of IP traffic which requires higher QoS class traffic and less traffic for lower QoS

class traffic and ~~verse visa~~vice versa. This may result in a worst case scenario in which most of the AIPN resources are used to handle higher QoS class IP traffic~~,~~ (e.g. guaranteed services)~~,~~ and so lower QoS class IP traffic~~,~~ (e.g. best effort traffic)~~,~~ suffers congestion and long delays.

It is believed that even under such situations, AIPN should still be able to provide satisfactory QoS to lower QoS class traffic e.g. best effort traffic. A possible method to achieve this could be to use dynamical load balancing mechanisms in the AIPN to control the load in the AIPN entities in terms of handling different type of traffic class according to the actual traffic model in real time.

Recommended requirements:

- AIPN shall be able to support different levels of QoS according the type of the IP traffic.
- Mechanisms should be available to the AIPN operator to enable AIPN congestion for the lower QoS class IP traffic to be avoided when a large amount of AIPN resource is used to handle higher QoS class traffic. A possible method to achieve this could be by using dynamic load balancing among the AIPN entities.

6.2.6 Enhanced Quality of Service

Though existing 3GPP systems guarantee end-to-end QoS for a session between 3GPP systems, a similar function is also needed for AIPNs. However, within an AIPN, this functionality shall be enhanced to ~~be~~ enable guarantee of end-to-end QoS across a variety of different access systems. Also, it is required that the continuation of QoS provision be possible whilst moving within an AIPN including when moving across access systems during handover.

The QoS ensuring methods have to consider cost aspects. Therefore, it is very important to support a variety of QoS ensuring methods, cost effective and adapted to the operator needs. Different operators have different cost structures, i.e. multiple QoS ensuring methods may need to be supported in the end-to-end path. This may be also valid in a single operator case due to different cost structures of the different network parts.

Recommended requirements:

- It shall be possible to guarantee end-to-end QoS for a session between AIPNs. This includes the case where more than one network administration is involved in the provision of the end-to-end service.
- It shall be possible to support different QoS ensuring methods within the same AIPN and between different AIPNs.
- Interworking between different QoS ensuring methods in the end-to-end path has to be supported.
- QoS considerations need to be taken into account in handover decisions:
  - It shall be possible for AIPN to guarantee end-to-end QoS without modification when the terminal or session moves from one access system to another, if the target access system supports the required QoS.
  - It shall be possible for AIPN to guarantee end-to-end QoS, with QoS modification, when the terminal or session moves from one access system to another, if the target access system has a QoS mechanism but can not be guaranteed to support the required QoS.
  - It should be possible for AIPN to provide mobility for a terminal or session between an access system that provides QoS and one that does not. However, in this case, seamless experience is not guaranteed, the terminal/application/user may need to be notified via some means and the network may need to adjust service setting for the session(s) accordingly to the change (e.g. charging adjustments, etc).

6.2.7 Personal Network~~s~~, Personal Area Network (PAN), Ad-hoc Network and Moving Network Support

An AIPN will offer users the services through Personal Networks, PANs, Ad-hoc Networks and Moving Networks (see Annex E), which will encourage users to utilize the 3GPP services. Therefore, it is required that AIPN shall support Personal Networks, Personal Area Networks (PAN), Ad-hoc Networks and Moving Networks.

Recommended requirements:

Personal Networks:

- -AIPN shall support a wide variety of service capabilities with the different (U)SIMs from the same AIPN operator (e.g. twin (U)SIMs) associated with a single user.

- -AIPN shall provide a connection between the terminal devices of a Personal Network that is reliable and provides adequate protection to the user's data to give confidence that his data is adequately protected.

Personal Area Networks:

- -The AIPN shall support multiple simultaneous sessions originated from one or several devices using the same (U)SIM authority.

Ad-hoc Networks:

- -The AIPN shall accept consolidated and distributed traffic from a group of users arriving through various access routes.

- -The AIPN shall be able to re-route traffic to ~~ad~~Ad-hoc ~~network~~ Network devices via another gateway.

- -The AIPN shall support changes in the access route for the consolidated traffic from an Ad-~~Hoc~~ hoc Network. These changes may take place with no warning to the AIPN.

- -Elements of the consolidated traffic from an Ad-~~Hoc~~ hoc Network may originate from a PAN.

- -Accurate charging records shall be created and maintained for the originating terminal when the traffic is routed through a terminal belonging to another subscriber.

Requirements for devices (terminals):

- A ~~G~~gateway device (terminal) must be able to route and forward packets to other devices in the ~~ad~~Ad-hoc N~~n~~etwork
- Ad-hoc N~~n~~etwork UEs must be able to discover 'near by' gateway devices

Note: Some type of incentives will need to ~~must~~ be created for devices to act as gateways (e.g. a reward scheme whereby a gateway can "earn" something)

Moving Networks:

Use Case 1:

- The AIPN shall support a point of access to the access system that has full mobility throughout the geographic region that uses the 3GPP access system for backhaul.

Use Case 2

- The AIPN shall accept consolidated traffic from a 3GPP terminal mounted in a vehicle with a router.
- The AIPN shall support changes in the alternate access route as the wireless access router moves throughout the service region.
- Accurate charging records shall be created and maintained for the originating terminal when the traffic created is routed through a Wireless Access Router.

Use Case 3:

- The AIPN shall support a mobile router connected directly to the AIPN using an alternate access route, e.g. via satellite.
- The AIPN shall support 'handovers' of whole M~~m~~oving N~~n~~etworks; i.e. it must be able to continuously route traffic for AIPN nodes of a ~~moving network~~Moving Network to a mobile router travelling as part of the ~~moving network~~Moving Network
- Accurate charging records shall be created and maintained for the originating terminal when the traffic is routed through a Mobile Router.

Next modified section

7 Conclusions

This chapter describes the conclusions of this Technical Report.

7.1 Roadmap for work within Rel-7

7.1.1 New requirements for introduction to the 3GPP specifications in Rel-7

New requirements for the 3GPP system that should be specified to enable introduction of an AIPN have been identified in Chapter 6.2 of this Technical Report. It is therefore recommended that the content of this chapter be used as a basis for introducing AIPN service requirements in to the 3GPP Technical Specifications in Rel-7. Additionally, the content of other chapters may be considered within specification work for an AIPN as appropriate.

The introduction of new functionalities and the enhancement of existing functionalities are necessary to achieve multiple access system accommodation and the mobility across multiple different access systems which are the fundamental key aspects of an AIPN. For this reason it is recommended that these functionalities are captured by new service~~s~~ requirements for the 3GPP system with the highest priority.

7.1.2 Impact to specifications in Rel-7

~~-~~The following table lists the recommended requirements ~~in each of the subsections~~described within this Technical Report and indicates the relevant existing SA1 Technical Specifications. These requirements should be analysed and captured within SA1 Technical Specifications as appropriate.

Chapter	Recommended requirement	Relevant Existing SA1 Technical Specification
5.1.1.4	- An AIPN shall incorporate naming and addressing schemes that address a given user or session. - The AIPN shall support end-user mobility. - The AIPN shall support terminal mobility. - The AIPN shall support session mobility.	TS 22.101 TS 22.129 TS 22.228
~~5.1.1.6~~	~~- The AIPN should provide a means to enable access system selection based on a range of criteria e.g. user preferences, service requirements of applications, network conditions or other AIPN operator-defined criteria.~~	~~TS 22.011~~
5.1.1.15	- An AIPN should support Identity Federation and Single Sign On for the end user. This would allow automatic authentication of the user to a multitude of service providers once the user has been authenticated by the AIPN.	TS 22.101 (possibly) Note 4
5.2.1.4	- An AIPN mobility solution must support UTRAN and GERAN based systems as possible access systems besides supporting alternative existing accesses such as WLAN and other emerging new technologies. - An AIPN mobility solution must be able to co-exist with the current 3GPP PS core	TS 22.101 TS 22.129

	network in a cost-efficient way. - An AIPN mobility solution should support seamless terminal mobility across various access systems. - AIPN should support services handover between 3GPP CS services (e.g. CS telephony) and AIPN equivalent services (e.g. Voice over IP).	
6.2.1	- An AIPN shall provide the following features: - Ability to efficiently handle a variety of different types of IP traffic including user-to-user and user-to-multicast traffic models - Optimized routing of IP traffic, in particular for user-to-user traffic. - Efficient usage of radio resources (e.g. signalling optimization, compression), including selection of access system, based on the provided service.	TS 22.101 TS 22.105
6.2.1.1	- An AIPN shall enable the accommodation of a vast number of users and terminals. - Based upon industry trends IP technology shall be applied to the addressing and routing technology within an AIPN to enable accommodation of a vast number of users and terminals.	TS 22.101 TS 22.105
6.2.2	- An AIPN shall support accommodation of several access systems (existing and future). - An AIPN shall support service provision across different access systems. - An AIPN shall support adaptation of service provision across different access systems.	TS 22.101 TS 22.105 TS 22.011
6.2.2.1	- An AIPN shall enable use of the multiple access systems - It should be possible to reach a user over multiple access systems simultaneously. - It should be possible to provide access system-aware services. - An AIPN shall provide support for access system selection based on combinations of AIPN operator policies, user preferences, service requirements of applications ~~and~~ access system conditions, and/or other AIPN operator-defined criteria.	TS 22.101 TS 22.105 TS 22.011
6.2.3.1	- ~~-~~An AIPN should provide open interfaces to AIPN services such as ~~MM~~mobility management in order to ease the terminal mobility across different access systems.	TS 22.101 TS 22.129 TS 22.234
6.2.3.2	- An AIPN must work with mobility mechanisms used by the specific networks it connects, including legacy mobility mechanisms of the current 3GPP PS core network.	TS 22.101 TS 22.129 TS 22.234
6.2.3.3	- ~~-~~An AIPN must support procedures related to frequent terminal mobility between AIPN nodes. - Whenever feasible, the AIPN mobility solution must support seamless user experience for all services provided by the AIPN. - The mobility solution must scale with the number of terminals and size of the AIPN. - An AIPN shall be able to support access systems with very limited or no mobility management procedures.	TS 22.101 TS 22.129 TS 22.234

6.2.4	- -The IP session control mechanisms of AIPN shall be enhanced from the functionalities of IMS to provide session mobility, session adaptation to terminal capability and session control for user to multicast. - _ –Users shall perceive continuous service whilst ensuring the efficient use of wireless resources and the effective usage of power resources within mobile terminals.	TS 22.101 TS 22.228
6.2.5.1	- An AIPN shall be able to provide guaranteed QoS for services and use AIPN resources with high efficiency i.e. ensure that quality conditions for a particular communication are fulfilled without deterioration between the communication end-points.	TS 22.105
6.2.5.2	- AIPN shall be able to support different levels of QoS according the type of the IP traffic. - Mechanisms should be available to the AIPN operator to enable AIPN congestion for the lower QoS class IP traffic to be avoided when a large amount of AIPN resource is used to handle higher QoS class traffic. A possible method to achieve this could be by using dynamic load balancing among the AIPN entities.	TS 22.105
6.2.6	- It shall be possible to guarantee end-to-end QoS for a session between AIPNs. This includes the case where more than one network administration is involved in the provision of the end-to-end service. - It shall be possible to support different QoS ensuring methods within the same AIPN and between different AIPNs. - Interworking between different QoS ensuring methods in the end-to-end path has to be supported. - QoS considerations need to be taken into account in handover decisions: - It shall be possible for AIPN to guarantee end-to-end QoS without modification when the terminal or session moves from one access system to another, if the target access system supports the required QoS. - It shall be possible for AIPN to guarantee end-to-end QoS, with QoS modification, when the terminal or session moves from one access system to another, if the target access system has a QoS mechanism but can not be guaranteed to support the required QoS. - It should be possible for AIPN to provide mobility for a terminal or session between an access system that provides QoS and one that does not. However, in this case, seamless experience is not guaranteed, the terminal/application/user may need to be notified via some means and the network may need to adjust service setting for the session(s) accordingly to the change (e.g. charging adjustments, etc). ~~- It shall be possible for systems for which it is feasible to guarantee end-to-end QoS continuously even when the terminal moves, and the access system connection changes during communication i.e. the same communication is maintained across changes in access system connection.~~	TS 22.105
6.2.7	Personal Networks: - -AIPN shall support a wide variety of service capabilities with the different USIMs from the same AIPN operator (e.g. twin USIMs) associated with a single user. - -AIPN shall provide a connection between the terminal devices of a Personal Network that is reliable and provides adequate protection to the user's data to give confidence that his data is adequately protected. Personal Area Networks: - -The AIPN shall support multiple simultaneous sessions originated from one or several devices using the same (U)SIM authority.	TS 22.011 Note 3

	Ad-hoc Networks: - -The AIPN shall accept consolidated and distributed traffic from a group of users arriving through various access routes. - -The AIPN shall be able to re-route traffic to Aad-hoc Nnetwork devices via another gateway. - -The AIPN shall support changes in the access route for the consolidated traffic from an Ad-hHoc Network. These changes may take place with no warning to the AIPN. - -Elements of the consolidated traffic from an Ad-Hhoc Network may originate from a PAN. - -Accurate charging records shall be created and maintained for the originating terminal when the traffic is routed through a terminal belonging to another subscriber. Requirements for devices (terminals): A Ggateway device (terminal) must be able to route and forward packets to other devices in the Aad-hoc Nnetwork Ad-hoc Nnetwork UEs must be able to discover 'near by' gateway devices ~~Some type of incentives must be created for devices to act as gateways (e.g. a reward scheme whereby a gateway can "earn" something)~~ Moving Networks: Use Case 1: - The AIPN shall support a point of access to the access system that has full mobility throughout the geographic region that uses the 3GPP access system for backhaul. Use Case 2 - The AIPN shall accept consolidated traffic from a 3GPP terminal mounted in a vehicle with a router. - The AIPN shall support changes in the alternate access route as the wireless access router moves throughout the service region. - Accurate charging records shall be created and maintained for the originating terminal when the traffic created is routed through a Wireless Access Router. Use Case 3: - The AIPN shall support a mobile router connected directly to the AIPN using an alternate access route, e.g. via satellite. - The AIPN shall support 'handovers' of whole mMoving Nnetworks; i.e. it must be able to continuously "route traffic" for AIPN nodes of a ~~moving network~~Moving Network to a mobile router travelling as part of the ~~moving network~~Moving Network - Accurate charging records shall be created and maintained for the originating terminal when the traffic is routed through a Mobile Router.	
Note 1:	The introduction of aspects relevant to Technical Specifications not under SA1 responsibility is to be determined by the appropriate 3GPP TSG WG.	
Note 2:	The content of the column entitled 'Relevant Technical Specification' is non-exhaustive, i.e. the introduction of requirements for an AIPN into Technical Specifications other than those stated may be considered if appropriate.	
Note 3:	~~—~~No SA1 Technical Specification appropriate to fully capture these requirements.	
Note 4:	The relevant existing SA1 Technical Specification for this functionality is for further study.	

7.2 Overall Conclusion

This Technical Report has analysed the vision and the key aspects of AIPN and identified new capabilities to be specified for the 3GPP system to enable evolution to an AIPN. It is concluded that the ~~features~~capabilities required for introduction of an AIPN into the 3GPP system require new specification work within 3GPP. The recommendation of this Technical Report is that the work be undertaken as a single Feature. A new Technical Specification may be produced to capture the service requirements for an AIPN. It is also recommended that new requirements identified within this Technical Report relevant to existing features of the 3GPP system, i.e. indicating that expansion of an existing capability (e.g. IMS), be added to existing specifications where appropriate.

Note 1: When undertaking specification work for an AIPN care should be taken to ensure that service requirements are not duplicated across multiple Technical Specifications. This could be achieved by e.g. adding the text for a new requirement to a single Technical Specification and referencing this requirement within other Technical Specifications as appropriate.

End of changes

TSG-SA WG1 #28 **S1-050502**

Beijing, P. R. China, 4 - 8 April 2005 **Agenda Item: 10.1**

CR-Form-v7

CHANGE REQUEST

⌘ **22.978** **CR** **005** ⌘ **rev** **-** ⌘ Current version: **7.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☒ Core Network ☒

Title:	⌘	Content-based Charging between Operators
Source:	⌘	SA1 (China Mobile)
Work item code:	⌘	AIPN
Date:	⌘	30/03/2005
Category:	⌘	**F**
Release:	⌘	Rel-7

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Content-based charging between operators should be considered in AIPN in addition to the traditional measurements such as volume and time. When subscriber roams from his home PLMN to another, he will use the services supplied by home network and visited network. So the charging between operators, which takes place when the user is enjoying the services supplied by visited PLMN, should be taken into account. In this case, the operators need more flexible charging functions, and content-based charging shall be considered, whereby some parameters, e.g. user identity, services ID, roaming status, QoS grades, may be concerned.
Summary of change:	⌘	It is suggested to add the requirement concerning content-based charging between operators.
Consequences if not approved:	⌘	Content-based charging between operators may not be supported.

Clauses affected:	⌘	4.3.1			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

******* FIRST MODIFICATION ******

4.3.1 Impacts to current charging models

Users are aware and understand the current charging models such as flow based charging and event based charging where a user pays for each time he/she uses a specific service, hence the possibility to provide these with an AIPN should be maintained. However, as the environment in which the 3GPP system is utilised adapts an AIPN should also provide the capabilities for and provide the necessary improvements in efficiency and cost reduction to enable new charging models to be introduced.

An AIPN should be flexible enough to support the different pricing models that are needed. Many Internet users expect that services such as email, news and search engines are free of charge and that they should pay only for the access via a flat rate pricing model. Other users will instead have to pay an additional amount according to the “calling party pays” principle. Therefore AIPN operators will need to use sophisticated pricing models, including event based charging. AIPNs should support those models. What pricing model to utilize at a given time is dependant on the circumstance of the AIPN operator e.g. based on different strategies such as Cost Leadership or Differentiation. An AIPN needs to support a cost effective charging system in order to be able to quickly launch new services but yet be as flexible such that an AIPN operator can use price models such as:

- Charge extra for guaranteeing a QoS
- Charge extra for “Calling Party Pays”
- Charge for the transport
- Charge for the event
- Additional charge (positive or negative) for the simultaneous use (combination) of services
- Adjust the price for different reasons e.g. to reward certain users, enable subscription bands (e.g. gold, silver, bronze)
- Charge for the content

Further the charging system for an AIPN shall contribute to minimizing the credit risks for the AIPN operator. The charging system in an AIPN shall in a cost efficient manner support various access systems with minimal impact on the terminal from a charging point of view. Further the AIPN shall from a control and charging point of view support different type of services e.g. RealTime and Bursty traffic such as PoC. Both real-time and none real-time schemes must be supported by an AIPN.

In a multi-access system environment the current charging and policy control architecture needs to be enhanced in order to allow for the business models defined in 4.3.2 e.g.

- The service provider having a relationship with the AIPN operator provides rating information and minimal QoS he assessed (as well as other content related polices) that apply for different access systems a service should have.
- For seamless handover between access systems in a multi-access system environment the subscription class/credit availability may allow service continuity or may not allow it. Hence based on subscription class different redirection points are applied e.g. for top up or to initiate a subscription such that credit are given for a service in a new access system.

There is a need to support flexible charging models between operators so that it is possible to charge roaming subscribers according to the different charging models identified above.

******* END OF MODIFICATION ******

TSG-SA WG1 #28 **S1-050503**

Beijing, China, 4th to 8th April 2005 **Agenda Item: 10.1**

CR-Form-v7.1

CHANGE REQUEST

⌘ **22.978** **CR** **006** ⌘**rev** **-** ⌘ Current version: **7.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Modification of AIPN session adaptation
Source:	⌘	SA1 (China Mobile, Panasonic)
Work item code:	⌘	AIPN
Date:	⌘	06/04/2005
Category:	⌘	**C**
Release:	⌘	Rel-7

Use one of the following categories:
- ***F*** *(correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(addition of feature),*
- ***C*** *(functional modification of feature)*
- ***D*** *(editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	Important functions of session control in AIPN are missing.
Summary of change:	⌘	Requirement for the AIPN to adapt sessions not only according to terminal capabilities, but also according to user preferences, subscriber priorities, network conditions or other operator-defined criteria is introduced. Furthermore session adaptation should be under the control of the operator.
Consequences if not approved:	⌘	Poorly defined functionality of session control. Sessions will not adapt according to user preferences, subscriber priorities, network conditions or other operator-defined criteria.

Clauses affected:	⌘	5.1.1.5, 6.2.4, 7.1.2

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
		X	Test specifications	
		X	O&M Specifications	

Other comments:	⌘	

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

******* FIRST MODIFICATION ******

5.1.1.5 Enhanced session management:

- Service adaptation to terminal capabilities, user preferences, subscriber priorities, network conditions or other operator-defined criteria. Service adaption shall be under the control of the operator.

  The services provided to users should be, as much as possible, independent of the terminal used and the condition of the network. The network should be able to adapt the service (e.g. information rendering) to the capabilities of the terminal being used and the condition of the network with minimum or no user interaction.

- Session mobility: seamless mobility of sessions between terminals.

  It should be possible to move sessions from one terminal (or a set of terminals) to another according to the preferences of the user e.g. automatically with minimum user involvement or based upon a specific user request/pre-determined user preference settings.

  Care needs to be taken to ensure there is no burden on the user to interact in a complex way.

******* SECOND MODIFICATION ******

6.2.4 Optimised IP session control

In principle it is assumed that session control within AIPN shall be optimised for user-to-user communication, i.e. from one user's mobile terminal to another user's mobile terminal, and for other traffic models such as those of streaming services, and shall be extended beyond IMS functionalities that are already provided. Some new session control mechanisms are introduced within an AIPN e.g. session mobility, session adaptation to terminal capability, user preferences, subscriber priorities, network conditions or other operator-defined criteria~~, and session control for user to multicast.~~. Session adaption shall be under the control of the operator. The AIPN shall support session control for multicast sessions (e.g. user-to-multicast) and the solution shall scale with the number of participants.

Additionally, it is necessary for an AIPN to ensure efficient use of wireless resources and effective usage of power resources within mobile terminals whilst maintaining the appropriate usability for a particular service.

Recommended requirements:

- The IP session control mechanisms of AIPN shall be enhanced from the functionalities of IMS to provide session mobility, session adaptation to terminal capability, user preferences, subscriber priorities, network conditions or other operator-defined criteria~~ and session control for user to multicast~~. Session adaption shall be under the control of the operator. The AIPN shall support session control for multicast sessions (e.g. user-to-multicast) and the solution shall scale with the number of participants.

- Users shall perceive continuous service whilst ensuring the efficient use of wireless resources and the effective usage of power resources within mobile terminals.

******* THIRD MODIFICATION ******

7.1.2 Impact to specifications in Rel-7

The following table lists the requirements in each of the subsections and indicates the relevant existing SA1 Technical Specifications. These requirements should be analysed and captured within SA1 Technical Specifications as appropriate.

Chapter	Recommended requirement	Relevant Existing SA1 Technical Specification
5.1.1.4	- An AIPN shall incorporate naming and addressing schemes that address a given	TS 22.101

	user or session. - The AIPN shall support end-user mobility. - The AIPN shall support terminal mobility. - The AIPN shall support session mobility.	TS 22.129 TS 22.228
5.1.1.6	- The AIPN should provide a means to enable access system selection based on a range of criteria e.g. user preferences, service requirements of applications, network conditions or other AIPN operator-defined criteria.	TS 22.011
5.1.1.15	- An AIPN should support Identity Federation and Single Sign On for the end user. This would allow automatic authentication of the user to a multitude of service providers once the user has been authenticated by the AIPN.	TS 22.101 (possibly)
5.2.1.4	- An AIPN mobility solution must support UTRAN and GERAN based systems as possible access systems besides supporting alternative existing accesses such as WLAN and other emerging new technologies. - An AIPN mobility solution must be able to co-exist with the current 3GPP PS core network in a cost-efficient way. - An AIPN mobility solution should support seamless terminal mobility across various access systems.	TS 22.101 TS 22.129
6.2.1	- An AIPN shall provide the following features: - Ability to efficiently handle a variety of different types of IP traffic including user-to-user and user-to-multicast traffic models - Optimized routing of IP traffic, in particular for user-to-user traffic. - Efficient usage of radio resources (e.g. signalling optimization, compression), including selection of access system, based on the provided service.	TS 22.101 TS 22.105
6.2.1.1	- An AIPN shall enable the accommodation of a vast number of users and terminals. - Based upon industry trends IP technology shall be applied to the addressing and routing technology within an AIPN to enable accommodation of a vast number of users and terminals.	TS 22.101 TS 22.105
6.2.2	- An AIPN shall support accommodation of several access systems (existing and future). - An AIPN shall support service provision across different access systems. - An AIPN shall support adaptation of service provision across different access systems.	TS 22.101 TS 22.105 TS 22.011
6.2.2.1	- An AIPN shall enable use of the multiple access systems - It should be possible to reach over multiple access systems simultaneously. - It should be possible to provide access system-aware services. - An AIPN shall provide support for access system selection based on combinations of AIPN operator policies, user preferences and access system conditions.	TS 22.101 TS 22.105 TS 22.011
6.2.3.1	- An AIPN should provide open interfaces to AIPN services such as MM in order to ease the terminal mobility across different access systems.	TS 22.101 TS 22.129 TS 22.234
6.2.3.2	- An AIPN must work with mobility mechanisms used by the specific networks it connects, including legacy mobility mechanisms of the current 3GPP PS core	TS 22.101

	network.	TS 22.129 TS 22.234
6.2.3.3	- An AIPN must support procedures related to frequent terminal mobility between AIPN nodes. - Whenever feasible, the AIPN mobility solution must support seamless user experience for all services provided by the AIPN. - The mobility solution must scale with the number of terminals and size of the AIPN. - An AIPN shall be able to support access systems with very limited or no mobility management procedures.	TS 22.101 TS 22.129 TS 22.234
6.2.4	- The IP session control mechanisms of AIPN shall be enhanced from the functionalities of IMS to provide session mobility, session adaptation to terminal capability, user preferences, subscriber priorities, network conditions or other operator-defined criteria ~~and session control for user to multicast~~. Session adaption shall be under the control of the operator. The AIPN shall support session control for multicast sessions (e.g. user-to-multicast) and the solution shall scale with the number of participants. - Users shall perceive continuous service whilst ensuring the efficient use of wireless resources and the effective usage of power resources within mobile terminals.	TS 22.101 TS 22.228
6.2.5.1	- An AIPN shall be able to provide guaranteed QoS for services and use AIPN resources with high efficiency i.e. ensure that quality conditions for a particular communication are fulfilled without deterioration between the communication end-points.	TS 22.105
6.2.5.2	- AIPN shall be able to support different levels of QoS according the type of the IP traffic. - Mechanisms should be available to the AIPN operator to enable AIPN congestion for the lower QoS class IP traffic to be avoided when a large amount of AIPN resource is used to handle higher QoS class traffic. A possible method to achieve this could be by using dynamic load balancing among the AIPN entities.	TS 22.105
6.2.6	- It shall be possible to guarantee end-to-end QoS for a session between AIPNs. This includes the case where more than one network administration is involved in the provision of the end-to-end service. - It shall be possible to support different QoS ensuring methods within the same AIPN and between different AIPNs. - Interworking between different QoS ensuring methods in the end-to-end path has to be supported. - It shall be possible for systems for which it is feasible to guarantee end-to-end QoS continuously even when the terminal moves, and the access system connection changes during communication i.e. the same communication is maintained across changes in access system connection.	TS 22.105
6.2.7	Personal Networks: - AIPN shall support a wide variety of service capabilities with the different USIMs from the same AIPN operator (e.g. twin USIMs) associated with a single user. - AIPN shall provide a connection between the terminal devices of a Personal Network that is reliable and provides adequate protection to the users data to give confidence that his data is adequately protected. Personal Area Networks: - The AIPN shall support multiple simultaneous sessions originated from one or	TS 22.011 Note3

	several devices using the same SIM authority. Ad-hoc Networks: - The AIPN shall accept consolidated and distributed traffic from a group of users arriving through various access routes. - The AIPN shall be able to re-route traffic to ad-hoc network devices via another gateway. - The AIPN shall support changes in the access route for the consolidated traffic from an Ad-Hoc Network. These changes may take place with no warning to the AIPN. - Elements of the consolidated traffic from an Ad-Hoc Network may originate from a PAN. - Accurate charging records shall be created and maintained for the originating terminal when the traffic routed through a terminal belonging to another subscriber. Requirements for devices (terminals): Gateway device (terminal) must be able to route and forward packets to other devices in the ad-hoc network Ad-hoc network UEs must be able to discover 'near by' gateway devices Some type of incentives must be created for devices to act as gateways (e.g. a reward scheme whereby a gateway can "earn" something) Moving Networks: Use Case 1: - The AIPN shall support a point of access to the access system that has full mobility throughout the geographic region that uses the 3GPP access system for backhaul. Use Case 2 - The AIPN shall accept consolidated traffic from a 3GPP terminal mounted in a vehicle with a router. - The AIPN shall support changes in the alternate access route as the wireless access router moves throughout the service region. - Accurate charging records shall be created and maintained for the originating terminal when the traffic created is routed through a Wireless Access Router. Use Case 3: - The AIPN shall support a mobile router connected directly to the AIPN using an alternate access route, e.g. via satellite. - The AIPN shall support 'handovers' of whole moving network; i.e. it must be able to continuously “route traffic” for AIPN nodes of a moving network to a mobile router travelling as part of the moving network - Accurate charging records shall be created and maintained for the originating terminal when the traffic routed through a Mobile Router.	
Note 1:	The introduction of aspects relevant to Technical Specifications not under SA1 responsibility is to be determined by the appropriate 3GPP TSG WG.	
Note 2:	The content of the column entitled 'Relevant Technical Specification' is non-exhaustive, i.e. the introduction of requirements for an AIPN into Technical Specifications other than those stated may be considered if appropriate.	
Note 3:	No SA1 Technical Specification appropriate to fully capture these requirements.	

******* END OF MODIFICATION ******

CR-Form-v7.1

CHANGE REQUEST

⌘ **22.978** **CR** **007** ⌘ **rev** **-** ⌘ Current version: **7.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	**Multiple Public Addresses for Single User**
Source:	⌘	SA1 (AIPN SWG)
Work item code:	⌘	AIPFS
Date:	⌘	08/04/2005
Category:	⌘	**C**
Release:	⌘	Rel-7

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*
Rel-7 *(Release 7)*

Reason for change:	⌘	To clarify the use of multiple public identities by individuals
Summary of change:	⌘	To explain the requirement for the AIPN to manage multiple public addresses associated with a single user
Consequences if not approved:	⌘	Poorly defined functionality

Clauses affected:	⌘	4.2.1.3, 5.1.1.5

Other specs affected: ⌘	Y	N	
		X	Other core specifications
		X	Test specifications
		X	O&M Specifications

⌘

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

First Proposed Change:

4.2.1.3 Social behaviour and the need to understand one's environment

Futurologists have identified some basic human behaviour patterns that have become increasingly important in modern societies. Two of them have been named "cocooning" and "clanning". "Cocooning" describes a behaviour in which an individual tries to isolate itself for a while from the surrounding society. It essentially expresses the wish for privacy with respect to permanent over-stimulation. "Clanning" describes the opposite phenomenon. It is the need of an individual to become integrated into a "clan", a group of similar minded people. This is mainly observed with young people and is a well known finding in group dynamics.

A third social factor that becomes strongly apparent is the need for the individual to better understand their environment. While an ever growing data stream permanently pours over the individual it becomes increasingly difficult to filter out the relevant information content. This results in disorientation, the difficulty of self-organisation and the feeling of uneasiness about one's environment. Also, the capability to quickly filter out important information from that which is unimportant is a competitive advantage of the individual.

A fourth social factor is that individuals spend their days and nights in many different roles (e.g. family person (me@personal.net), worker (me@company.com), sports club official (official@sportsclub.com)). Depending on their roles, time of day, and location, they may wish to be reachable via these different publicly known user IDs on certain specific systems or devices. By arrangement with the AIPN operator for terminating calls to the Public ID, the recipient of calls directed towards a Public Identity may change on a temporary basis (e.g. a sports club official is temporarily unavailable and wishes calls to that Public Identity to be answered by an alternate individual).

Deductions

- An AIPN will need to provide means that respect and ensure a user's need for privacy.
- The basic human wish to become integrated within social groups could be a good basis for services in an AIPN. Good examples are chat-rooms and the like.
- An All-IP system that offers services which allow an individual to gain a better orientation within their environment (geographic, social, business) will provide significant added value to its users.
- An AIPN system should offer the users the ability to be reachable by several different publicly known IDs in a flexible manner.

Second Proposed Change

5.1.1.5 Enhanced session management:

- Service adaptation to terminal capabilities.

  The services provided to users should be, as much as possible, independent of the terminal used. The network should be able to adapt the service (e.g. information rendering) to the capabilities of the terminal being used with minimum or no user interaction.

- Session mobility: seamless mobility of sessions between terminals.

  It should be possible to move sessions from one terminal (or a set of terminals) to another according to the preferences of the user e.g. automatically with minimum user involvement or based upon a specific user request/pre-determined user preference settings.

- An end-user shall be able to select how calls and services directed towards her through each of her public IDs will be treated. For example, for a given public ID, she may set which of her terminal device(s) is used and with what priority, through which access system(s), and whether calls are automatically answered by the network at certain times of day.

  Care needs to be taken to ensure there is no burden on the user to interact in a complex way.

End of changes

CR-Form-v7

CHANGE REQUEST

⌘ **22.978** **CR** **008** ⌘**rev** **-** ⌘ Current version: **7.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Enabling integrated services in AIPN
Source:	⌘	SA1 (China Mobile, Telecom Italia)
Work item code:	⌘	AIPFS
Date:	⌘	30/03/2005
Category:	⌘	**F**
Release:	⌘	Rel-7

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	In 4.2.1.1, it is stated that AIPN operator should offer diversified and flexible services to satisfy the varied needs of users. It is envisaged that integrated service will be popular. For example, when you call your friend, you may also want to share some music or video with him. Currently, several enhanced services are well defined in 5.1.1.7, such as support for advanced application services and ubiquitous services. However, there is no requirement definition for intergrated services. But in traditional service architectures, it is difficult for operators to integrate different services easily and rapidly, so it is benefitial to add this requirement.
Summary of change:	⌘	Add the requirement of integrated services in section 5.1.1.7
Consequences if not approved:	⌘	Integrated services may not be support by AIPN.

Clauses affected:	⌘	3.1, 5.1.1.7

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

******* FIRST CHANGE ******

3.1 Definitions

…

AIPN operator: An operator of an AIPN. It is assumed that the AIPN operator will also be a network/PLMN operator as defined within [1].

Integrated Service: A -service, which is perceived by user as a single service, composed by a combination of different independent services.

IP service: a service using an IP bearer provided by an IP service provider. For IP services data traffic is routed according to the IP addresses of the sender and receiver.

…

******* SECOND CHANGE ******

5.1.1.7 Enhanced services

- Support for advanced application services
- Support for integrated services, e.g. a service including a mixture of services among SMS/MMS/Instant Message, or a service- including voice call/video call/voice mail.
- Provision of seamless services (e.g. transparent to access systems, adaptable to terminal capabilities, etc)

  Users should be able to move transparently and seamlessly between access systems and to move communication sessions between terminals.

  An AIPN will be able to adapt services as much as possible to the capabilities of the user's terminal, allowing the user to access services independently of which terminal they are using.

…

******* END OF CHANGE ******

CR-Form-v7

CHANGE REQUEST

⌘ **22.978** **CR** **009** ⌘ **rev** **-** ⌘ Current version: **7.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [X] Core Network [X]

Title:	⌘	Introduce Group Communication Services to AIPN
Source:	⌘	SA1 (China Mobile, Panasonic)
Work item code:	⌘	AIPFS
Date:	⌘	07/04/2005
Category:	⌘	**B**
Release:	⌘	Rel-7

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The prospect of group communication services is cheerful. However, when the size of the group increases, there are few efficient mechanisms to handle the situation in current specifications. As described in AIPN TR 22.978 clauses 4.2.1.3, the basic human wish to become integrated within social groups could be a good basis for services in an AIPN. That indicates in some cases, human wish to communicate each other in a large-scale group. For example, conference call of a company or association is required in some cases, and various meetings are held all over the world. Unfortunately, there is only one key aspect 'Optimised IP Session Control' could be mapped to this motivation. More affected aspects shall be defined. Furthermore, in order to provide high bit-rate services to a huge size group, multicast is a possible functionality to provide these types of services. It is reasonable to include multicast support in some key aspects, e.g. advanced mobility management and enhanced quality of service.
Summary of change:	⌘	It is proposed to add the requirement of group communication services and make some related modifications to enhance the text describing the support of multicast. In particular with regard to QoS control.
Consequences if not approved:	⌘	Communications in a group, especially in a large size group, may not be supported. Addditionally, QoS control for multicast services will not be considered within TR 22.978.

Clauses affected:	⌘	3.1, 5.1.1.7, 5.1.1.12, 6.2.6, 7.1.2, Annex A

		Y	N			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

******* FIRST CHANGE ******

3.1 Definitions

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

Ad-hoc Network: An *Ad-hoc Network* is a dynamically organized network of mobile terminals that are able to communicate with each other via some means (e.g. using IEEE 802.15 or WLAN in ad-hoc mode). An Ad-hoc Network may contain terminals that are capable of connection to a variety of access systems. In the context of AIPN, it is assumed that every terminal in the Ad-hoc Network is under the control of a separate user, each able to independently access the AIPN. The Ad-hoc Network routes their consolidated traffic towards the AIPN, to an Access system through one or more terminals in the Ad-hoc Network. The Ad-hoc network may change the terminal carrying the consolidated traffic change dynamically according to rules set up by the users. The Ad-hoc network may move throughout the geographic coverage area. (See Annex E)

All-IP Network (AIPN): A collection of entities that provide a set of capabilities for the provision of IP services to users based on IP technology where various access systems can be connected. The AIPN provides a set of common capabilities (including mobility, security, service provisioning, charging and QoS) which enable the provision of services to users and connectivity to other external networks. An AIPN requires one or more connected access systems to allow users to access the AIPN.

Access system: An entity or collection of entities that provides the user the capability to connect to the AIPN.

AIPN operator: An operator of an AIPN. It is assumed that the AIPN operator will also be a network/PLMN operator as defined within [1].

IP service: a service using an IP bearer provided by an IP service provider. For IP services data traffic is routed according to the IP addresses of the sender and receiver(s).

IP service provider: a service provider that provides IP services. This may or may not be a network operator e.g. the operator of an IMS would be an IP service provider according to this definition.

IP service subscriber: a subscriber to an IP service provider that uses IP services.

Moving Network: A *Moving Network* is a group of user devices (terminals) that move together, for example, as part of vehicular network. The user devices (terminals) are interconnected in a way that their consolidated traffic towards the AIPN is routed through a well-defined system (gateway). The elements of the consolidated traffic may originate from PAN and Ad-hoc Networks within a Moving Network. (See Annex E)

Personal Network: A Personal Network, in the context of AIPN, consists of more than one device (terminal or server provided by the AIPN operator) under the control of one user providing access to the AIPN. These devices are interconnected by the AIPN such that the user perceives a continuous secure connection regardless of their relative locations. The user controls the PN using facilities provided by the AIPN. (See Annex E)

Personal Area Network: A Personal Area Network (PAN), in the context of AIPN consists of more than one device (terminal) controlled by, and physically close to, the same user (person). All the devices within a PAN use the same USIM. These devices are connected together using internal PAN means. The user obtains services from the AIPN using his multiple devices which all access the users USIM through the PAN to gain access to the AIPN. The user controls the PAN directly. (See Annex E)

Seamless: A user experience that is unaffected by changes in the mechanisms used to provide services to a user.

Note: The determination of whether something satisfies the requirement for being seamless or not is dependent on the user's (e.g., human end-user, protocol, application, etc.) perception of the service being received and not necessarily the technology used to provide the service.

Seamless Service: services provided across access systems and terminal capabilities. Provisioning of this service is continued between and within access systems and between terminals with minimal degradation in the service as seen by the user.

Seamless session: A session that is maintained during a change in access system, with no perceivable interruption from a user perspective, while adapting to the capabilities of each access system.

End-user mobility: The ability for the subscriber to communicate using the device or devices of his/her choice

Terminal mobility: The ability for the same UE to communicate whilst changing its point of attachment to the network. This includes both handovers within the same access system, and handover from one access system to another.

Session mobility: The ability for a communication session to be moved from one device to another under the control of the user.

For further definitions see [1].

******* SECOND CHANGE ******

5.1.1.7 Enhanced services

- Support for advanced application services

- Support for group communication services, e.g. voice group call, instant group messaging, and multicast delivery. In some cases, a group may include a large number of participants.

- Provision of seamless services (e.g. transparent to access systems, adaptable to terminal capabilities, etc)

  Users should be able to move transparently and seamlessly between access systems and to move communication sessions between terminals.

  An AIPN will be able to adapt services as much as possible to the capabilities of the user's terminal, allowing the user to access services independently of which terminal they are using.

Note: this may not be feasible in all cases (e.g. some services will require "minimum terminal capabilities" to be able to be accessed, with these "minimum capabilities" being service dependent), but an AIPN will be designed to enable this property in as many cases as possible.

…

******* THIRD CHANGE ******

5.1.1.12 Quality of Service

- AIPN operators should be able to guarantee QoS within their networks.

- The QoS mechanisms used by an AIPN should be able to guarantee end to end QoS for a ~~traffic flow~~ unicast and multicast traffic when all network segments (including access, core network and inter-connecting networks) are able to provide the requested QoS.

Note: Business agreements for QoS guarantees between the parties (e.g. operators, national- and international carriers, corporate customers) are today regularly based on static agreements. These types of agreements may need to be re-considered in order to reflect the advanced means to guarantee QoS between AIPNs.

******* FOURTH CHANGE ******

6.2.6 Enhanced Quality of Service

Though existing 3GPP systems guarantee end-to-end QoS for a session between 3GPP systems, a similar function is also needed for AIPNs. However, within an AIPN, this functionality shall be enhanced to be enable guarantee of end-to-end QoS across a variety of different access systems. Also, it is required that the continuation of QoS provision be possible whilst moving within an AIPN including when moving across access systems during handover. It is also required to provide QoS control for multicast (e.g. user-to-multicast) traffic.

The QoS ensuring methods have to consider cost aspects. Therefore, it is very important to support a variety of QoS ensuring methods, cost effective and adapted to the operator needs. Different operators have different cost structures, i.e. multiple QoS ensuring methods may need to be supported in the end-to-end path. This may be also valid in a single operator case due to different cost structures of the different network parts.

Recommended requirements:

- It shall be possible to guarantee end-to-end QoS for a user-to-user or multicast (e.g. user-to-multicast) session between AIPNs. This includes the case where more than one network administration is involved in the provision of the end-to-end service.

- It shall be possible to support different QoS ensuring methods within the same AIPN and between different AIPNs.

- Interworking between different QoS ensuring methods in the end-to-end path has to be supported. QoS considerations need to be taken into account in handover decisions:

  - It shall be possible for AIPN to guarantee end-to-end QoS without modification when the terminal or session moves from one access system to another, if the target access system supports the required QoS.

  - It shall be possible for AIPN to guarantee end-to-end QoS, with QoS modification, when the terminal or session moves from one access system to another, if the target access system has a QoS mechanism but can not be guaranteed to support the required QoS.

  - It should be possible for AIPN to provide mobility for a terminal or session between an access system that provides QoS and one that does not. However, in this case, seamless experience is not guaranteed, the terminal/application/user may need to be notified via some means and the network may need to adjust service setting for the session(s) accordingly to the change (e.g. charging adjustments, etc).

- It shall be possible for an AIPN to guarantee QoS of a multicast session without modification to QoS of other terminals when one of the terminals moves from one access system to another (e.g. for multimedia streaming with adaptation to the conditions of each recipient).

  - It shall be possible for an AIPN to guarantee QoS of a multicast session without modification to QoS of other terminals when one of the terminals moves from one access system to another, when the target access system for this terminal does not support the required QoS.

  - It shall be possible for an AIPN to guarantee QoS of a multicast session with QoS modification to one of the terminals, when this terminal moves from one access system to another, if the target access system has a QoS mechanism but can not be guaranteed to support the required QoS. The QoS of the other terminals of the multicast session are unaffected by the modification of QoS of the terminal moving from one access system to another.

- It shall be possible for an AIPN to control guarantee of QoS of a multicast session with QoS modification to all of the terminals, when one of the terminals moves from one access system to another, if the target access system for this terminal has a QoS mechanism but can not be guaranteed to support the required QoS (e.g. for a gaming application where the conditions are to be equal for each of the players).

******* FIFTH CHANGE ******

7.1.2 Impact to specifications in Rel-7

The following table lists the requirements in each of the subsections and indicates the relevant existing SA1 Technical Specifications. These requirements should be analysed and captured within SA1 Technical Specifications as appropriate.

Clause	Recommended requirement	Relevant Existing SA1 Technical Specification
5.1.1.4	- An AIPN shall incorporate naming and addressing schemes that address a given user or session. - The AIPN shall support end-user mobility. - The AIPN shall support terminal mobility.	TS 22.101 TS 22.129 TS 22.228

Clause	Recommended requirement	Relevant Existing SA1 Technical Specification
	- The AIPN shall support session mobility.	
5.1.1.6	- The AIPN should provide a means to enable access system selection based on a range of criteria e.g. user preferences, service requirements of applications, network conditions or other AIPN operator-defined criteria.	TS 22.011
5.1.1.15	- An AIPN should support Identity Federation and Single Sign On for the end user. This would allow automatic authentication of the user to a multitude of service providers once the user has been authenticated by the AIPN.	TS 22.101 (possibly)
5.2.1.4	- An AIPN mobility solution must support UTRAN and GERAN based systems as possible access systems besides supporting alternative existing accesses such as WLAN and other emerging new technologies. - An AIPN mobility solution must be able to co-exist with the current 3GPP PS core network in a cost-efficient way. - An AIPN mobility solution should support seamless terminal mobility across various access systems.	TS 22.101 TS 22.129
6.2.1	- An AIPN shall provide the following features: - Ability to efficiently handle a variety of different types of IP traffic including user-to-user and user-to-multicast traffic models - Optimized routing of IP traffic, in particular for user-to-user traffic. - Efficient usage of radio resources (e.g. signalling optimization, compression), including selection of access system, based on the provided service.	TS 22.101 TS 22.105
6.2.1.1	- An AIPN shall enable the accommodation of a vast number of users and terminals. - Based upon industry trends IP technology shall be applied to the addressing and routing technology within an AIPN to enable accommodation of a vast number of users and terminals.	TS 22.101 TS 22.105
6.2.2	- An AIPN shall support accommodation of several access systems (existing and future). - An AIPN shall support service provision across different access systems. - An AIPN shall support adaptation of service provision across different access systems.	TS 22.101 TS 22.105 TS 22.011
6.2.2.1	- An AIPN shall enable use of the multiple access systems - It should be possible to reach over multiple access systems simultaneously. - It should be possible to provide access system-aware services. - An AIPN shall provide support for access system selection based on combinations of AIPN operator policies, user preferences and access system conditions.	TS 22.101 TS 22.105 TS 22.011
6.2.3.1	- An AIPN should provide open interfaces to AIPN services such as MM in order to ease the terminal mobility across different access systems.	TS 22.101 TS 22.129 TS 22.234
6.2.3.2	- An AIPN must work with mobility mechanisms used by the specific networks it connects, including legacy mobility mechanisms of the current 3GPP PS core network.	TS 22.101 TS 22.129

Clause	Recommended requirement	Relevant Existing SA1 Technical Specification
		TS 22.234
6.2.3.3	- An AIPN must support procedures related to frequent terminal mobility between AIPN nodes. - Whenever feasible, the AIPN mobility solution must support seamless user experience for all services provided by the AIPN. - The mobility solution must scale with the number of terminals and size of the AIPN. - An AIPN shall be able to support access systems with very limited or no mobility management procedures.	TS 22.101 TS 22.129 TS 22.234
6.2.4	- The IP session control mechanisms of AIPN shall be enhanced from the functionalities of IMS to provide session mobility, session adaptation to terminal capability and session control for user to multicast. - Users shall perceive continuous service whilst ensuring the efficient use of wireless resources and the effective usage of power resources within mobile terminals.	TS 22.101 TS 22.228
6.2.5.1	- An AIPN shall be able to provide guaranteed QoS for services and use AIPN resources with high efficiency i.e. ensure that quality conditions for a particular communication are fulfilled without deterioration between the communication end-points.	TS 22.105
6.2.5.2	- AIPN shall be able to support different levels of QoS according the type of the IP traffic. - Mechanisms should be available to the AIPN operator to enable AIPN congestion for the lower QoS class IP traffic to be avoided when a large amount of AIPN resource is used to handle higher QoS class traffic. A possible method to achieve this could be by using dynamic load balancing among the AIPN entities.	TS 22.105
6.2.6	- It shall be possible to guarantee end-to-end QoS for a user-to-user or multicast (e.g. user-to-multicast) session between AIPNs. This includes the case where more than one network administration is involved in the provision of the end-to-end service. - It shall be possible to support different QoS ensuring methods within the same AIPN and between different AIPNs. - Interworking between different QoS ensuring methods in the end-to-end path has to be supported. - It shall be possible for systems for which it is feasible to guarantee end-to-end QoS continuously even when the terminal moves, and the access system connection changes during communication i.e. the same communication is maintained across changes in access system connection. - It shall be possible for an AIPN to guarantee QoS of a multicast session without modification to QoS of other terminals when one of the terminals moves from one access system to another (e.g. for multimedia streaming with adaptation to the conditions of each recipient). - It shall be possible for an AIPN to guarantee QoS of a multicast session without modification to QoS of other terminals when one of the terminals moves from one access system to another, when the target access system for this terminal does not support the required QoS. - It shall be possible for an AIPN to guarantee QoS of a multicast session	TS 22.105

Clause	Recommended requirement	Relevant Existing SA1 Technical Specification
	with QoS modification to one of the terminals, when this terminal moves from one access system to another, if the target access system has a QoS mechanism but can not be guaranteed to support the required QoS. The QoS of the other terminals of the multicast session are unaffected by the modification of QoS of the terminal moving from one access system to another. - It shall be possible for an AIPN to control guarantee of QoS of a multicast session with QoS modification to all of the terminals, when one of the terminals moves from one access system to another, if the target access system for this terminal has a QoS mechanism but can not be guaranteed to support the required QoS (e.g. for a gaming application where the conditions are to be equal for each of the players).	
6.2.7	Personal Networks: - AIPN shall support a wide variety of service capabilities with the different USIMs from the same AIPN operator (e.g. twin USIMs) associated with a single user. - AIPN shall provide a connection between the terminal devices of a Personal Network that is reliable and provides adequate protection to the users data to give confidence that his data is adequately protected. Personal Area Networks: - The AIPN shall support multiple simultaneous sessions originated from one or several devices using the same SIM authority. Ad-hoc Networks: - The AIPN shall accept consolidated and distributed traffic from a group of users arriving through various access routes. - The AIPN shall be able to re-route traffic to ad-hoc network devices via another gateway. - The AIPN shall support changes in the access route for the consolidated traffic from an Ad-Hoc Network. These changes may take place with no warning to the AIPN. - Elements of the consolidated traffic from an Ad-Hoc Network may originate from a PAN. - Accurate charging records shall be created and maintained for the originating terminal when the traffic routed through a terminal belonging to another subscriber. Requirements for devices (terminals): Gateway device (terminal) must be able to route and forward packets to other devices in the ad-hoc network Ad-hoc network UEs must be able to discover 'near by' gateway devices Some type of incentives must be created for devices to act as gateways (e.g. a reward scheme whereby a gateway can "earn" something) Moving Networks: Use Case 1: - The AIPN shall support a point of access to the access system that has full mobility throughout the geographic region that uses the 3GPP access system for backhaul. Use Case 2 - The AIPN shall accept consolidated traffic from a 3GPP terminal mounted in a vehicle with a router. - The AIPN shall support changes in the alternate access route as the wireless access router moves throughout the service region. - Accurate charging records shall be created and maintained for the originating terminal when the traffic created is routed through a Wireless Access Router.	TS 22.011 Note3

Clause	Recommended requirement	Relevant Existing SA1 Technical Specification
	Use Case 3: - The AIPN shall support a mobile router connected directly to the AIPN using an alternate access route, e.g. via satellite. - The AIPN shall support 'handovers' of whole moving network; i.e. it must be able to continuously “route traffic” for AIPN nodes of a moving network to a mobile router travelling as part of the moving network - Accurate charging records shall be created and maintained for the originating terminal when the traffic routed through a Mobile Router.	

Note 1: The introduction of aspects relevant to Technical Specifications not under SA1 responsibility is to be determined by the appropriate 3GPP TSG WG.
Note 2: The content of the column entitled 'Relevant Technical Specification' is non-exhaustive, i.e. the introduction of requirements for an AIPN into Technical Specifications other than those stated may be considered if appropriate.
Note 3: No SA1 Technical Specification appropriate to fully capture these requirements.

******* SIXTH CHANGE ******

Annex A (Informative): Mapping of AIPN Motivations to Key Aspects of an AIPN

This annex contains a matrix mapping the AIPN Motivations and Drivers (Chapter 4) to the Key Aspects of an AIPN (Chapter 5).

			Key Aspects of an AIPN														
			Common IP-based network	Support of access different	Convergence towards IP	Advanced mobility	Session management	Access system selection	Enhanced services	Enhanced network performance	Network extensibility/comp	Network management	Security and privacy	Quality of Service	Terminal and User identification	Flexible future development	Identity federation
Motivations and Drivers	User related and Social Drivers	Consumer trend demanding diversification of mobile services	X	X	X	X	X	X	X	X				X	X		X
		Human need to be able to interact with his personal environment							X						X	X	
		Social behaviour and the need to understand one's environment				X	X	X	X	X			X	X			
		The social trend of increasing differences in income within societies							X					X			
		The need to satisfy user experience of ‘early-adopters’				X			X	X							
	Drivers from a Business	Mobile industry anticipating PS traffic to surpass CS	X		X					X							
		Desire of AIPN operators to encompass various access systems that are not specified by 3GPP	X	X	X	X		X	X							X	X
		Marriage of IT- and telecom world	X		X						X						X
		Need for increased system efficiency leading to substantial cost reduction	X	X	X					X		X				X	

		Trend of the industry to align along the structure: access / transport / control / services									X					X	
		Fixed/Mobile network convergence		X							X						
	Drivers from a Technology Perspective	Evolution of next generation radio access systems (3GPP specified)	X	X		X		X	X	X							
		Progress of broadband wireless IP-based networks (non-3GPP specified)	X	X		X		X	X	X							
		Progress in ad-hoc networking for user defined services.								X	X		X				
		Dawning of new, radio based services							X	X	X				X		
		Reconfigurable Radio		X		X		X		X							
		Web services							X								X
		Multi-access		X		X		X	X								
		Progress of advanced Traffic Engineering Technologies								X				X			

Note1: This matrix maps the sub-clauses of chapters 4.2 and 5.1.1 of this Technical Report. In some cases the sub-clause headings have been abbreviated to improve readability.

******* END OF CHANGE ******