TECHNICAL REPORT

# ISO/IEC TR 26927

First edition
2006-12-01

# Information technology — Telecommunications and information exchange between systems — Corporate Telecommunication Networks — Mobility for Enterprise Communications

*Technologies de l'information — Télécommunications et échange d'informations entre systèmes — Réseaux de télécommunication d'entreprise — Mobilité pour les communications d'entreprise*

Reference number
ISO/IEC TR 26927:2006(E)

© ISO/IEC 2006

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

**PDF disclaimer**

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



© ISO/IEC 2006

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland



Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

© ISO/IEC 2006 – All rights reserved

# Contents

Page


Foreword ..... v

Introduction ..... vi

1 Scope ..... 1

2 Normative references ..... 1

3 Terms and definitions ..... 2

4 Acronyms and abbreviations ..... 7

5 Overview ..... 9

6 Taxonomy of mobility ..... 11
6.1 Basic mobility types ..... 11
6.1.1 Terminal mobility (also known as device mobility) ..... 11
6.1.2 User mobility (also known as personal mobility) ..... 11
6.1.3 Session mobility ..... 11
6.1.4 Service mobility ..... 11
6.2 Mobility across different network infrastructures (network roaming) ..... 12
6.2.1 Mobility across access network technologies ..... 12
6.2.2 Mobility across administrative network domains ..... 12
6.3 Granularity of mobility ..... 12
6.3.1 Continuous mobility (mobile access) ..... 13
6.3.2 Discrete mobility (nomadic and portable access) ..... 13
6.3.3 Local and global mobility ..... 14

7 Overview on technical issues of mobility ..... 14
7.1 Mobility Management ..... 14
7.1.1 Protocols for IP-mobility management ..... 15
7.1.2 Terminal management ..... 16
7.1.3 User profile management ..... 17
7.1.4 Roaming services ..... 17
7.1.5 Presence services ..... 18
7.2 Service architecture issues ..... 18
7.2.1 IMS architecture ..... 18
7.2.2 Quality of Service (QoS) ..... 18
7.3 Security ..... 19
7.3.1 User and device identification ..... 19
7.3.2 Authentication ..... 20
7.3.3 Authorization ..... 20
7.3.4 Access by VPN ..... 20

8 Use cases of enterprise mobility ..... 22
8.1 Mobility starting from the home network ..... 22
8.1.1 Use case: Discrete mobility within the home domain ..... 24
8.1.2 Use case: Discrete mobility between home and visited domain ..... 24
8.1.3 Use case: Continuous mobility between two visited domains ..... 26
8.1.4 Use case: Continuous mobility between home domain and a visited network ..... 27
8.2 Mobility starting from a visited network ..... 28
8.2.1 Use case: Discrete mobility in a visited public network ..... 29
8.2.2 Use case: Discrete mobility in a visited enterprise network ..... 31
8.2.3 Use case: Discrete mobility in a residential network ..... 31
8.2.4 Use case: Continuous mobility within a visited public network ..... 32
8.2.5 Use case: Continuous mobility between different network technologies of a visited public network ..... 33


© ISO/IEC 2006 – All rights reserved



Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

**8.2.6 Use case: Continuous mobility between different visited public networks ..... 34**
**8.2.7 Use case: Continuous mobility between a visited public network and the home network ..... 35**

**9 Functional requirements on enterprise-grade mobility ..... 36**
**9.1 Enterprise user's perspective ..... 36**
**9.2 Enterprise network operator's and IT manager's perspective ..... 38**
**9.3 Perspective of 3rd party service providers ..... 42**
**9.4 Perspective of regulatory authorities and administrations ..... 43**

**Annex A** (informative) **Standardization and promotion activities on enterprise mobility issues ..... 44**

--`,,```,,,,````-`-`,,`,,`,`,,`---



© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

# Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, the joint technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 26927 was prepared by Ecma International (as ECMA TR/92) and was adopted, under a special "fast-track procedure", by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

# Introduction

This Technical Report identifies key mobility issues for IP-based enterprise communication. This includes the taxonomy of mobility aspects, use cases and connectivity scenarios of mobile enterprise users. Based on the scenarios requirements for mobility management, architecture and security are identified.

This Technical Report is based upon the practical experience of Ecma member companies and the results of their active and continuous participation in the work of ISO/IEC JTC1, ITU-T, ETSI, IETF and other international and national standardization bodies. It represents a pragmatic and widely based consensus.


© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

# Information technology — Telecommunications and information exchange between systems — Corporate Telecommunication Networks — Mobility for Enterprise Communications

## 1 Scope

This Technical Report identifies key mobility issues for access to IP-based enterprise information and communications services. It defines a taxonomy of mobility terms and then explores use cases and connectivity scenarios involving mobile enterprise users. From these, it derives requirements for mobility management, architecture and security.

Mobility for enterprise communication is about making desktop communication and information resources available at different locations and while on the move. This Technical Report encompasses both wired and wireless connectivity using enterprise and public all-IP networks for voice, data and converged services.

This Technical Report is intended as an aid to analysing gaps in standardization that prevent or hinder mobility in enterprise communications and information access. More general interworking issues of enterprise communications are covered by a companion Technical Report, ISO/IEC TR 26905.

## 2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC TR 26905:2006, *Information technology — Telecommunications and information exchange between systems — Enterprise Communication in Next Generation Corporate Networks (NGCN) involving Public Next Generation Networks (NGN)*

IETF RFC 2486, *The Network Access Identifier*

IETF RFC 3261, *SIP: Session Initiation Protocol*

IETF RFC 3344, *IP Mobility support for IPv4*

IETF RFC 3775, *IP Mobility support in IPv6*

ETSI EG 202 325, *Human Factors: User Profile Management*

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

## 3 Terms and definitions

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

**3.1**
**access network**
**AN**
collection of network entities and interfaces that provide underlying IP transport connectivity between a user's terminal and an enterprise or a public core network

**3.2**
**accounting**
process of collecting resource usage measurements and apportioning charges for services provided by a network operator or service provider

**3.3**
**active profile**
set of all active profile components related to a user

**3.4**
**administrative domain**
collection of physical or functional network entities under the control of a single administration

**3.5**
**Application Service Provider**
**ASP**
provides and manages applications on top of IP

**3.6**
**authentication**
proof that an identity is genuine, e.g. the user is as claimed

**3.7**
**authorization**
process or result of assigning certain execution rights or a role to an authenticated user or entity

**3.8**
**availability**
willingness and ability of a user to engage in a communications session

**3.9**
**base profile**
rules and settings that are always active in a profile

**3.10**
**billing**
function whereby charges generated by a network accounting function are transformed into bills

**3.11**
**core network**
portion of a communication system composed of networks, system equipment and infrastructures providing connections between access networks and between service providers and access networks

**3.12**
**Corporate Network**
**CN**
sets of equipment (Customer Premises Equipment and/ or Customer Premises Networks) that are located at geographically dispersed locations and are interconnected to provide services to a defined group of users


© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

**3.13**
**domain**
collection of physical or functional network entities belonging to a restricted geographical area, a topological IP-area or owned/operated by an enterprise, public carrier or service provider

**3.14**
**end-to-end security**
security (including privacy and information integrity) for the exchange of information between two or more end points that does not rely on secure channels or other security features in between these end points

**3.15**
**enterprise-grade service**
performance level for security, availability and service perception that is comparable to PBX-based services

**3.16**
**extranet**
closed IP-network of an enterprise used for data or converged communication services by external partners of the enterprise

**3.17**
**federated management**
management with access to the control functions of another network on the basis of a federation agreement between the network administrations

**3.18**
**firewall**
security means to shield an enterprise IP-network from unwanted traffic by blocking certain IP addresses and port numbers or certain application data content

**3.19**
**handover**
handoff
process of transferring an ongoing network connection from one point of attachment to another

**3.20**
**home domain**
home network administrative domain where the mobile user has a service agreement/subscription

NOTE For sake of more efficient mobility management, a visited network may provide a temporary home domain, but such concepts are currently still research topics.

**3.21**
**home network**
network where the mobile user has a service agreement and which maintains user-specific data including location, authentication, authorization and service profile information

**3.22**
**hosting network**
access network that provides point of network attachment to a mobile user

NOTE This can be the home network or a visited network

**3.23**
**hotspot**
location of a wireless point of attachment

NOTE Hotspots can be public or restricted to customers or employees of an enterprise.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

**3.24**
**identity**
a name by which the user of a network is known

**3.25**
**inactive profile**
profile that does not currently apply but that may apply to a user when the circumstances change

**3.26**
**internet**
public IP network

**3.27**
**intranet**
closed IP network of an enterprise used for data or converged communication services by members of the enterprise

**3.28**
**IP network**
public or user-specific network offering connectionless packet-mode services based on the Internet Protocol (IP) as the network layer protocol

NOTE The Internet is the prime example of a public IP network.

**3.29**
**IP-PBX**
PBX capable of IP-based telecommunications

**3.30**
**location**
information on the network point of attachment through which a user is currently accessing a network, including e.g. identification of the geographical, administrative and IP-topology domain

**3.31**
**mobile network**
network that provides continuous connectivity to mobile terminals by wireless access

**3.32**
**mobility management**
set of functions used in the core network and access networks to provide mobility

NOTE These functions include authentication, authorization, location updating, paging, download of user information and more.

**3.33**
**Network Access Provider**
**NAP**
business entity that provides network access infrastructure to one or more Network Service Providers (NSPs)

NOTE A NAP implements this infrastructure using one or more Access Service Networks (ASN).

**3.34**
**Network Service Provider**
**NSP**
business entity that provides IP connectivity and services to subscribers compliant with the service level agreement it establishes with subscribers

NOTE To provide these services, an NSP establishes contractual agreements with one or more NAPs. An NSP may also establish roaming agreements with other NSPs and contractual agreements with third-party application providers (e.g. ASP or ISPs) for providing services to subscribers.


© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

**3.35**
**Next Generation CN**
**NGCN**
self-contained corporate network designed to take advantage of emerging IP-based communications solutions and that can have its own applications and service provisioning

**3.36**
**Next Generation Network**
**NGN**
packet based public network able to provide telecommunication services, able to make use of multiple QoS enabled transport technologies and in which service related functions are independent of underlying transport related technologies

**3.37**
**personal user agent**
functional entity (probably implemented as a software object) with a one-to-one relationship to a specific user identifier

**3.38**
**portal**
web-based based interface that provides a single access point to dispersed information, e.g. corporate portals provide enterprise-wide information to employees

**3.39**
**presence**
set of data representing the status and availability of a user or a group of users for communication

**3.40**
**privacy**
feature that enables a user to control the disclosure of his identity, communication status or other communications related information, including media, to others

**3.41**
**profile**
total set of user related information, preferences, rules and settings which affects the way in which a user experiences terminals, devices and services

**3.42**
**profile provider**
entity (e.g. company such as a service provider, organization such as a special interest or affinity organization) that provides profiles and associated services

**3.43**
**Quality of Service**
**QoS**
measure of the quality level of services to users which determines how different traffic will be handled and prioritized in the network, according to the enterprise's business policy and specific requirements in a Service Level Agreement (SLA) between the enterprise and the network operator or a virtual network operator, e.g. an MVNO

**3.44**
**residential network**
private network that provides network access and interconnection on a restricted geographical area, e.g. a university campus or a private building

**3.45**
**roaming service**
service that enables users to access services according to their user profile while outside their home domain, i.e. by using an access point of a visited network

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

NOTE This requires the ability of the user to get access in the visited network, the existence of an interface between the home network and the visited network, as well as a roaming agreement between the respective network administrations.

**3.46**
**service mobility**
network ability that enables a user to obtain a particular (agreed) service irrespective of his PoA (network technology and administrative domain) and the terminal that is used

**3.47**
**service provider**
entity that offers services to users involving the use of network resources

**3.48**
**session mobility**
network ability that enables a user to maintain an active session while switching between terminals or changing to another subnet or access network

**3.49**
**single sign-on**
procedure by which a user gains access to all authorised communication services

NOTE Such services may comprise telephony features and/or enterprise applications that employ embedded communication functions.

**3.50**
**terminal mobility**
ability of a network or networks to provide network connectivity to a user even when the point of attachment (PoA) of his terminal changes within the network or between different networks

**3.51**
**transit network**
network that provides interconnection between a visited network and a home network on the basis of a service contract

**3.52**
**URI**
identifier for a communication resource which may represent a user, a device, a service or combinations thereof

**3.53**
**user**
person, organization or technical system that accesses a network in order to communicate using the services provided by that network

**3.54**
**user mobility**
ability of a network or networks to provide network connectivity to a user even when his PoA changes, regardless of whether or not this involves a change of terminal

**3.55**
**user profile**
set of information describing a user's service environment

**3.56**
**Virtual Private Network**
**VPN**
virtual network that can deliver ubiquitous and secure connectivity over a shared network infrastructure (e.g. public carrier networks) using the same access policies as an enterprise network


--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

**3.57**
**visited domain**
administrative domain that provides a PoA outside the home domain of the mobile user

**3.58**
**visited network**
network that provides a PoA outside the home network of a mobile user

## 4 Acronyms and abbreviations

| | |
|---|---|
| AAA | Authentication, Authorization and Accounting |
| AC | Access Controller (WLAN) |
| AN | Access Network |
| AP | Access Point (WLAN) |
| API | Application Program Interface |
| ASN | Access Service Networks |
| ASP | Application Service Provider |
| CIP | Cellular IP |
| CN | Corporate Network |
| CPE | Customer Premises Network |
| CRM | Customer Relation Management |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name Service |
| ERP | Enterprise Resource Planning |
| GPRS | General Packet Radio Service |
| GSM | Global System for Mobile communication |
| GW | Gateway |
| HIP | Host Identity Protocol |
| HLR | Home Location Registry |
| HSDPA | High Speed Downlink Packet Access |
| IdP | Identity Provider |
| ICT | Information Communication Technology |
| IM | Instant Messaging |
| IMS | IP Multimedia Subsystem |
| IP | Internet Protocol |

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

| | |
|---|---|
| ISDN | Integrated Services Digital Network |
| ISP | IP-Service Provider |
| IVR | Interactive Voice Response |
| LAN | Local Area Network |
| MIP | Mobile IP |
| MM | Mobility Management |
| MVNO | Mobile Virtual Network Operator |
| NA | Not Applicable |
| NAP | Network Access Provider |
| NAT | Network Address Translator |
| NSP | Network Service Provider |
| OAM | Operation, Administration and Maintenance |
| PAN | Personal Area Network |
| PBX | Private Branch Exchange |
| PIM | Personal Information Management |
| PKI | Public Key Infrastructure |
| PLMN | Public Land Mobile Network |
| PoA | Point of Attachment |
| PSTN | Public Switched Telephony Network |
| PWLAN | Public Wireless LAN |
| QoS | Quality of Service |
| RFC | Request For Comment |
| RPC | Remote Procedure Call |
| SLA | Service Level Agreement |
| SCTP | Stream Control Transmission Protocol |
| SIM | Subscriber Identity Module |
| SIP | Session Initiation Protocol |
| SMS | Short Message Service |
| SOHO | Small Office Home Office |
| SSL | Secure Socket Layer |
| TCP | Transmission Control Protocol |

-`,,```,,,,````-`-`,,`,,`,`,,`---



© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

| | |
|---|---|
| TDM | Time Division Multiplexing |
| VoWLAN | Voice over WLAN |
| UMTS | Universal Mobile Telecommunications System |
| URI | Uniform Resource Identifier |
| USIM | UMTS Subscriber Identity Module |
| UTRAN | UMTS Terrestrial Radio Access |
| VLAN | Virtual LAN |
| VoIP | Voice over IP |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| WLAN | Wireless LAN |
| WWAN | Wireless WAN (Wide Area Network) |
| xDSL | Denotes a class of Digital Subscriber Lines technologies, e.g. ADSL, VDSL |

## 5 Overview

Globalization of economy and the need for more responsive business processes (also referred to as the 'real-time enterprise') have created new demands on enterprise networks. Progress in digital technology is transforming corporate networks and will ultimately transform the way companies provide communications and information technology for the enterprise in order to improve business value. Examples are the migration from separate voice and data networks to a converged IP network, providing both information access and real time communication in a single network. Other important developments are the convergence of the enterprise's telecom services with its IT processes to enhance workflows, the increase of hosted ICT services provided by ISPs or public carriers for non-core enterprise tasks, the demand for access to ICT resources from everywhere, meaning mobility, and the fast growing variety in types and applications of communications technology.

In the highly responsive enterprise of the future (real-time enterprise) the office no longer represents the actual physical location where all of the employees are situated, but the environment they are working in – at the office, away from the desk in a conference room, at home or on the road – with a range of digital appliances that continues to diversify and proliferate. Next generation public networks (NGN) and next generation corporate networks (NGCNs) are extending their reach to provide mobile connectivity with wireless or wired technology, e.g. high-bandwidth wireless hotspots, digital cellular or xDSL access to address the needs of anytime, anywhere at any device communications. This includes besides the support of interpersonal communication (e.g. via voice/ video), person-to-machine (e.g. IVR) and machine-to-machine communications (e.g. automatic software updates).

Access control, along with security, will be necessary to provide corporate users with transparent services and communication. Supporting secure mobility across a range of transports, both wired and wireless, inside and outside of the office and the enterprise owned network, will become a key element of the enterprise communication future. Other critical components are the provisioning of real-time communication and information services anytime, anywhere at any device with an appropriate level of quality of service. In addition, to realize the full potential of mobile communications, communication services, including real-time services, should be presence-aware and fully integrated in the IT environment (workflow, business processes) of the enterprise.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Examples for mobility applications in enterprise communications area are:

- Public transport, logistics
  - Voice over WLAN and mobile data for personnel, e.g. at loading docks
  - Access to resources during travel
- Hospitals
  - Easy ad-hoc access to patient data (for authorized personnel only) – anywhere
  - Voice over WLAN for nurses and doctors
  - Information on where to find personnel within premises
- Large industrial plants, campus areas
  - Many “mobile“ people (many meetings, projects, various large buildings…)
  - Mobile access to data, e.g. for service personnel
  - Remote and distributed inventory management
- Enterprise grade Voice over WLAN on campus

Figure 1 depicts an example of an enterprise mobility environment.

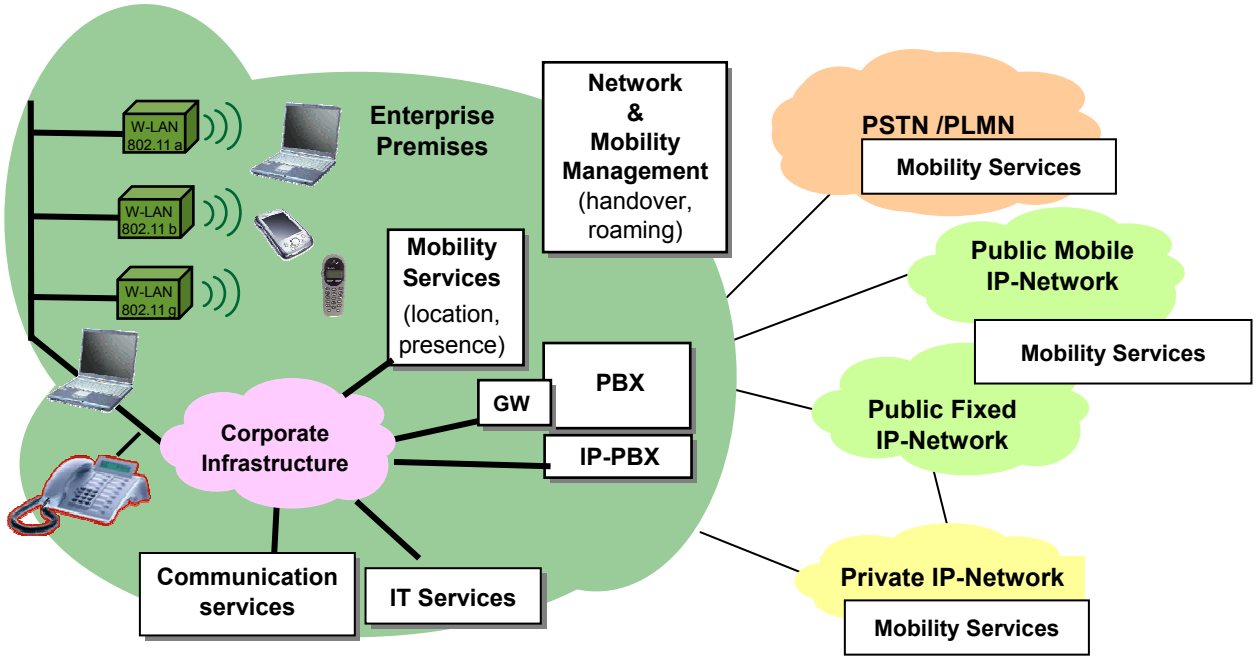


**Figure 1 — Enterprise mobility environment**

As shown in Figure 1 mobility for enterprise communication is supported besides the Corporate LAN/WAN by the emerging IP-based public mobile and fixed networks including the Internet. Of high importance for mobility is the provision of WLAN islands (hotspots) either on the enterprise campus or in public areas, which provides broadband data access and voice telephony (VoWLAN). Other promising technologies for enterprise mobility are WIMAX, WLAN in vehicles (moving networks) and self-organizing mobile networks, e.g. meshed networks.


© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

# 6 Taxonomy of mobility

Mobility comes in various forms and with various limitations. A large number of terms are frequently used to describe different types of mobility, often with different terms used for the same thing and the same term used for different things. This clause introduces the terms used in this Technical Report to describe types of mobility. It also groups these terms in the form of a taxonomy.

## 6.1 Basic mobility types

Generalized mobility as stated in the previous clause includes four mobility types: terminal, user, session and service mobility, which refer to different functionalities that the mobility management (MM) of networks can provide.

NOTE The functionality of these mobility types is complementary, but not independent, i.e. session and service mobility can not be used without terminal or user mobility.

### 6.1.1 Terminal mobility (also known as device mobility)

The purpose of terminal mobility is to provide network connectivity to the user even when the Point of Attachment (PoA) of his terminal changes within the network or between different networks. One of the major tasks is the maintenance of the IP-address of the mobile terminal. This requires the capability of the network to identify and locate the terminal. Terminal mobility may also entail a change of access technology, for example from a GSM to a WLAN access network.

### 6.1.2 User mobility (also known as personal mobility)

User mobility denotes the ability of a network or networks to provide network connectivity to a user even when his PoA changes, regardless of whether or not this involves a change of terminal. It also potentially allows the user to retain access to authorised services (in the case of a persistent single sign-on capability).

This requires a personal identifier, and the capability of the network(s) concerned to provide at different terminals those services listed in the user's profile. In addition, user mobility includes the possibility of accessing services from several terminals simultaneously.

An important requirement for user mobility is that the user register with the network(s) by supplying suitable credentials for identifying and authenticating themselves, e.g., user identity, account name, password, PIN, cryptographic information, biometric evidence, etc. This information can be entered by the user or, particularly where a cryptographic key is required, obtained from a smart card (e.g., SIM, USIM, etc.) or soft key store. The network has to provide appropriate means for authentication, authorization and accounting (AAA). Accounting does not usually depend on the type of device being used, but on the user who registers.

Users may also register in their corporate home network across public (either home or visited) or visited corporate networks infrastructures.

### 6.1.3 Session mobility

Session mobility enables the user to maintain an active session while switching between terminals or changing to another subnet or access network. The session handover is provided by the mobility management functions of the involved networks.

### 6.1.4 Service mobility

Service mobility is the ability for a user to obtain a particular (authorised) service irrespective of his PoA (including heterogeneous network technologies and different administrative domains) and the terminal that is used. Services can be of a transport or application nature. This ability is in general supported by a coordinated set of service components provided by the network infrastructure of the access provider, by the enterprise network, by a 3rd party and by the client application on the mobile terminal. This means that a standardized network-to-network interface is required to make a service transparently accessible from different networks. In

© ISO/IEC 2006 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

addition the presentation and execution of a service has to be adapted to the characteristics of the user's terminal, e.g. computing performance, memory size, display capabilities, etc., and potentially tailored to the user preferences contained in their profile.

Examples of the benefits that service mobility can bring include (in each case irrespective of terminal or point of network access):

- the ability to use the same dial plan for establishing outgoing communications;
- the ability to subscribe to services such as presence and location;
- the retention of user preferences, favourites, short-cuts, user privileges, etc.

## 6.2 Mobility across different network infrastructures (network roaming)

The basic mobility types may be further classified according their ability to cope with crossing heterogeneous network infrastructures, such as different access technologies, or different network domains or both.

### 6.2.1 Mobility across access network technologies

This classification of mobility refers to the support of terminal, user, session and service mobility independent of network technology.

- *Intra-technology mobility*:
  supports mobility within a network or across networks with the same access network technology.
- *Inter-technology mobility*:
  supports mobility across networks using different access network technologies. Examples are transitions from LAN to WLAN or MAN to UTRAN.

### 6.2.2 Mobility across administrative network domains

This kind of mobility denotes the support of terminal, user, session and service mobility independent of the administrative network domain.

- *Intra-domain mobility:*
  denotes the support of mobility within a single administrative network domain.
- *Inter-domain mobility:*
  enables mobility across different network domains, e.g. across public and enterprise network infrastructures. This includes as well IP-subnets of a single enterprise.

Connection continuity across networks is supported by mobility management processes which provide network roaming by network handover on different network layers. The level of support is determined by roaming policies. In case of inter domain mobility a service level agreement (SLA) between the involved network administrations is needed in addition. However, any roaming service must be supported by the network architecture to provide the appropriate signalling and media transport capabilities.

## 6.3 Granularity of mobility

The granularity of mobility depends strongly on the performance of the mobility management process to handover an ongoing communication session from one access network to another. A handover may be initiated either by the hosting network, the mobile device or by the network assisted by the mobile device. In cases where the location change of the terminal does not result in delay or loss of data that would be perceived by the user as degradation of quality of service, the handover and the mobility involved is called seamless.. The availability of handover is typically not service dependent but its provision depends on the access network capabilities.


© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The handover (HO) itself can be within one access technology (horizontal HO) or between different access technologies (vertical HO).

The following terms have been introduced for classifying the granularity of mobility:

- Continuous mobility
- Discrete mobility
- Local and global mobility

### 6.3.1 Continuous mobility (mobile access)

Continuous mobility or mobile access denotes the ability of a user or a terminal to maintain communication while roaming between network PoAs without interrupting the network connection and the associated sessions (in case of session-based connections). A service that provides continuous mobility is also known as a mobile service.

Continuous mobility is not necessarily seamless, in some situations, the hand-over may lead to a briefly suspended service session or it may require a change in the service level provided as a consequence of the capabilities of the new access point to which the user has become connected through the handover process.

### 6.3.2 Discrete mobility (nomadic and portable access)

Discrete mobility denotes the ability of a user or terminal to change location or terminal only with interruption or loss of any connection and associated sessions in progress.

This usually happens between wired network accesses, such as changing desktop terminals (hot desking) in the enterprise, moving a portable terminal between wired accesses or changing from a wireless to a wired access and vice versa.

Discrete mobility can be subdivided into two categories:

- *Nomadic access:*
  This is the ability of the user or terminal to change his network PoA with no support for connection or session continuity. Any ongoing session must be stopped (or is lost) and then must be started again (if required) at the new PoA. In other words, there is no mobility of session or network connectivity provided. It is assumed that normal usage pattern is that users shutdown their connection before moving to another access point, as a user moves from one network to another.

  NOTE There is a special case of nomadic access that may be available on some access networks, where the user may be able to re-establish the authentication of their original network connection, even though their sessions need to be closed.

- *Portable access*:
  This is similar to nomadic access but provides support of discrete session mobility. This means a user or terminal is able to change the network access point while maintaining the ongoing session by suspending the session at predefined synchronisation points (application specific) and resuming after changing to the new access point.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

### 6.3.3 Local and global mobility

The extent of mobility support further depends on the level of co-operation of mobility management functions across networks. Two basic types of can be distinguished:

- *Local mobility*:
  denotes the limitation of mobility to an arbitrary collection of administrative domains. No reassignment of IP addresses need to take place - just the path to the mobile terminal is updated within the network, so that packets can be routed correctly.

- *Global mobility*:
  in this case mobility management is effective across different networks. This means the home and *corresponding* nodes of the visited network have to be informed on location changes, and a reassignment of IP addresses may occur.

# 7 Overview on technical issues of mobility

The following issues are addressed:

- Mobility management, which addresses issues of mobility control and signalling

- Mobility architecture, which addresses system level issues e.g. network architectures

- Security, which covers protection of business information and privacy.

## 7.1 Mobility Management

Mobility management (MM) denotes a set of functions used in the Core Network to provide mobility within the home network and across visited networks. These functions include communication with the home network for purposes of authentication, authorization, location updating and download of user information.

The provisioning of seamless mobility services across different networks and/or systems is in some cases restricted by:

- different access technologies

- non portability of services

- incompatible MM functions and protocols

- missing open MM interfaces

- specific user preferences and rules in their profile

Two types of MM can be distinguished:

- *Global mobility management*:
  supports global mobility by addressing MM issues between networks of different operators, which may include location and AAA functionality.

- *Local mobility management:*
  supports local mobility by addressing MM issues within a arbitrary set of domains, Local MM can reduce the amount of latency involved in re-establishing the mobile terminal`s network connection after handover, and can reduce the amount of signalling between the mobile terminal and the home network.


© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Standardisation activities for MM are carried out in various standardisation organisations, e.g. IETF, 3GPP or ITU-T. In general they have the following objectives:

- Independence of MM from the underlying access technology
- Minimal involvement of the mobile terminal in MM
- Definition of a reference architecture and network functions required to support the basic mobility types
- Definition of required interfaces for these functions in the control layer
- Efficient routing to provide seamless handovers.

For more information on involved standardization bodies see Annex A.

As enterprise networks are usually protected by special network entities such as NATs and firewalls which may interfere with global MM signalling, special care has to be taken to solve NAT/firewall traversal. More information on this issue can be found in the companion ISO/IEC TR 26905.

### 7.1.1 Protocols for IP-mobility management

The role of an IP-address is twofold: it is used by routers to forward IP-packets to its destination and at the same time it is also used by the current transport and application protocols as a part of session identification. When a mobile terminal roams to another PoA in a different network the IP-address of the mobile device must change and will abort the session at upper layers, thereof.

The IETF and 3GPP have specified a couple of protocols for managing mobility in IPv4 and IPv6 networks, e.g. SIP, MIP, CIP and mSCTP. The most relevant protocols for enterprise mobility are briefly introduced in the following:

Mobile IP (MIP)

Mobile IP is a open standard of the IETF that allows users to keep the same IP address, remain connected without having to re-establish secure IP sessions, and maintain session persistence while roaming between IP networks.

MIP is a network layer protocol which is independent of the underlying access network technologies. It could be well harmonized with IP-based core networks because it is a standardized extension to IP. MIP supports both IPv4 and IPv6.but interworking between MIPv4 and MIPv6 will be required to support seamless mobility. Besides, MIP supports location management and limited handover management.

The base MIP specification is not sufficient for providing the seamless handover management for real-time or loss-sensitive applications, and thus enhancements or extensions of MIP are required.

Relevant IETF specifications on MIP are currently:

- RFC 3344, “IP Mobility support for IPv4”,
- RFC 3775, “IP Mobility support in IPv6”.

MIP has some well-known limitations, e.g. for real-time applications due to packet delays caused by triangular routing and significant overhead caused by the IP-in-IP encapsulation of the protocol.

Cellular IP (CIP)

CIP is a network layer protocol defined in IETF drafts (and being used in products) which provides handover management and limited location management. It needs dedicated CIP nodes for routing and a CIP gateway for interworking, but it does not require route optimisation. The protocol could be used with location management provided by MIP and SIP.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Session Initiation Protocol (SIP, RFC 3261)

SIP, specified in IETF RFC 3261), is a peer-to-peer application layer protocol that is designed for supporting session control in IP-based multimedia sessions. It is also the base signalling protocol in next generation corporate networks (NGCN) and next generation fixed and mobile carrier networks (NGN, UMTS). A SIP mobility service does not require any network mobility support, as in MIP, since it works at the application level. SIP mobility is therefore independent of the terminal provide user and service mobility. SIP also could support continuous handoff for keeping TCP session alive on the move between subnetworks. However, the support of seamless handover management in the current specification needs further enhancements.

SIP transparently supports user mobility by name mapping and by proxying and redirecting requests to the user's current location. Based on the use of a unique personal identity (URI) and the ability of SIP-users to register their current location, end users can originate and receive calls and access subscribed services on any terminal in any location. In addition session mobility is supported. In this case DHCP is used to get a new IP address and the SIP user agent (UA) resumes the session by sending a Re-INVITE message.

SiP based mobility support can improve the performance of real-time applications and is the preferred choice for SIP-based sessions; however, TCP connections will break during hand-over. To resume such connections the terminal needs to get a new IP-address, which may cause significant delay. To improve the situation assistance of SIP by other protocols, e.g. MIP or CIP has been proposed.

MM protocols under development

For supporting mobility management the IETF has developed new promising protocols, such as the Host Identity Protocol (HIP) and MOBIKE, MOBIKE, although originally designed for another purpose, offers features of a MM protocol, e.g. allowing a mobile terminal with a VPN tunnel assigned to remain connected during movement between IP links.

Besides some vendors have developed proprietary local MM protocols, that allow seamless subnet roaming in WLANs without requiring MM code on the mobile device, but WLAN network nodes from the same vendor. The IETF has started some standardization activities in that area, e.g. CAPWAP.

### 7.1.2 Terminal management

Due to the variety and complexity of mobility services the management of the relationship between networks, services and terminals becomes more and more important. The need for intelligent control and coordination mechanisms has been recognized. Standardisation of architectures and mechanisms for terminal management are underway in the relevant bodies.

The former WAP Forum has published specifications on related functions like service provisioning and user profiles. A more general technical solution for the realization of device management was specified in the SyncML Forum. 3GPP intends to use the SyncML Forum specifications on Device Management (DM) as a basis for standardizing a full top-down solution for the management of 3GPP User Equipment (UEM). The foundation of the Open Mobile Alliance (OMA) opened the way to incorporate all these activities into one comprehensive, bearer-independent approach for the management of mobile devices. The main interests of OMA member companies contain the following goals:

- Device diagnostics with built-in/ downloaded software
- Download/ update of applications/ native software
- Provisioning including first time provisioning
- Virus detection and prevention
- Queries for configuration, device/ software properties
- Reconfiguration of the terminal and its applications
- Collection and analysis of events and statistics
- Remote control of the terminal user interface.


© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

### 7.1.3 User profile management

User profile management functions are based on data which is either "user subscription data" or "network data" (e.g., current network, point of attachment (PoA) location). The management function may have the ability to exchange profiles with other instances (e.g. presence), synchronize databases with distributed instances and even provide mechanisms to dynamically switch profiles as the user is moving into another context and wants to get his session seamlessly transferred. The storage and the update of these profile elements are handled by the user profile management functions (such as a user profile agent application). A user profile component shall be provided especially for authentication, authorization, service subscription information, subscriber mobility services, land charging. It may be stored in one database or distributed to several databases which are usually under control of the user's home network. Access to the user profile data or parts of it from hosting service provider or 3rd party networks standardized interfaces are desirable, within specific guidelines to protect user privacy and maintain user preferences.

User Profiles are very valuable in flexible communications. They allow the various services individual and corporate users interact with to provide customized capabilities with very little user interaction or self-provisioning. Proper handling of the profiles also provides the security and privacy users and employers desire. With the support of enhanced applications profiles are also capable of carrying customized policy information that can be applied during any interactive session or during handover to new networks or devices.

### 7.1.4 Roaming services

Roaming is a mean to provide end-to-end services by co-operation across a number of service provider/ network provider administrative domains. It is a complex service requiring various layers of interactions and processes, including network discovery, authentication, authorization and usage tracking, and billing. Co-operation is needed between applications and user clients together with session control and transport via network-to-network interfaces.

Roaming between WLANs and wireless wide-area networks (WWANs) include all or most of the aforementioned processes, whereas subnet roaming may include only authentication and authorization.

The first step of roaming is network discovery (by the end user), which usually requires a client resident location database, a network-sniffing client and a NIC. Once the network is discovered, the user authentication and authorization starts. At this point, the user is authenticated by either a hot-spot resident gateway or the roaming partner authentication server. Both of these servers validate the user by querying the user's home authentication server.

For terminal mobility, in many implementations network devices need a unique and secure identity that can be transparently tunnelled back to a unique and secure point of authentication and billing across different types of networks. In many cellular networks the subscriber's identity is in the subscriber identity module (SIM) card or embedded in laptops and personal digital assistants (PDAs) and it is authenticated at the home network of a mobile operator in the home location registry (HLR) of cellular networks. This method allows account information and provider-hosted user profile data to follow subscribers and for the provisioning of a single bill. Other solutions use a carrier-based gateway that identifies a mobile subscriber, assigns them a mobile IP-address, tracks the subscriber activities and usage records, and, along with interfaces to carriers' existing billing systems, help to create a single bill for the customer.

Once the user is authenticated, a policy server determines the appropriate type of access authorized to the user. When the user gains access to the network, a tracking system tracks the usage in a variety of ways, including minutes of use, megabits downloaded, average bandwidth, etc. The usage records collected by the roaming agent are then transmitted either to its own billing engine or to the wireless ISP. In this phase, roaming is closely associated with billing and settlement. Currently, in the cellular world, clearinghouses distribute roaming fees to operators when other cellular customers use their network. Clearinghouses are now entering into WLAN roaming settlement as well, and will be required in the future with the wide deployment of multi-provider service bundles.

Another segment of a roaming service pertains to maintaining connections and session persistence while moving from one network type to another. This is performed by a handover service based on either the use of Mobile IP (MIP), SIP or proprietary solutions, depending on the network environment and whether the connection is session-based or not. (See also 7.1.1)

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

### 7.1.5 Presence services

An important enabler for user and terminal mobility is presence service. It denotes services to monitor, recognize and broadcast status (online/ offline), availability, contactibility and geographic location of a user or a group of users to communicate.

Several standardized solutions for presence are available. The most relevant proposal is the SIP-based SIMPLE approach of the IETF, which has been adopted as presence service for the IMS service architecture deployed by 3GPP and by ETSI TISPAN for their NGN architecture.

In addition, user profiles may contain rules for defining when the user (or when the user's employer) may or may not indicate presence, the available scope of that presentation, and when presence changes imply different security and functional requirements.

## 7.2 Service architecture issues

Mobile workers who do enjoy ubiquitous high-speed connectivity are demanding devices and applications that can roam across heterogeneous networks. Accomplishing this requires many improvements to the existing network infrastructure, which will facilitate network roaming, not prevent it.

The core networks which are deployed in enterprises for mobility support are based to a large part on standardized protocols but use proprietary architectures. However, carrier networks which are involved in enterprise mobility (as access, transit or service provider networks) are built upon standardized frameworks. For next generation fixed and mobile carrier networks the IMS architecture of 3GPP, expanded by ETSI TISPAN, seems to represent the most relevant core network architecture.

The key issues for enterprise mobility are to define appropriate interworking functions to provide seamless and secure mobility service across heterogeneous network architectures. This includes pure transit services on the transport level and as well federated solutions on the service level.

In the following the basics of the IMS architecture are described.

### 7.2.1 IMS architecture

The IMS (IP Multimedia Subsystem) has been specified by 3GPP as service architecture for the 3G mobile network UMTS Release 5. As ETSI TISPAN has adopted IMS as well as a core network for next generation fixed line carrier network (NGN) it is considered as common service architecture for both fixed as well as mobile networks which should significantly ease the fixed/ mobile convergence of carrier services and the provision of business communication services. Key functionalities of the architecture are:

- Independence from network access technologies
- Physical & logical separation of application, session control and transport traffic.

ETSI TISPAN NGN is required to support the mobility of both users and terminal equipment. The required mobility support in TISPAN NGN release 1 is limited to the ability of a terminal to be moved to different access points (which may be owned by a different access network provider) and a user to utilise different terminal and access points to retrieve their communication and content services (even from another network operator). The level of service may be dependent on user preferences, terminal capability and the specific mobility scenario (intra or inter-access network, intra or inter-provider). TISPAN NGN Release 1 mobility supports nomadic access, but is not required to support handover between access networks. There is no requirement to prevent autonomous handover within an access network (local mobility).

### 7.2.2 Quality of Service (QoS)

Enterprise communication is considered as a productivity component in the business processes of an enterprise where users are typically more sensitive to the quality of the offered service than independent users.


© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Real-time services, e.g. interpersonal communications using voice or video, as well as mission critical enterprise applications (e.g. ERP or CRM) demand a certain level of network performance to provide enterprise-grade service quality. Critical transport parameters include latency, delay jitter and data rate, which can be controlled in managed packet-networks by various QoS mechanisms which operate on different network layers. Standardized solutions include the Intserv and Diffserv mechanisms of the IETF and IEEE.802.11e for WLANs.

End-to-end QoS across network boundaries requires the co-operation of QoS management functions and defined network-to-network interfaces. Within the network of a single operator, this can be more readily realized, but across networks of different operators this is currently hard to achieve due to the lack of open standards. Because the access network is in many cases the weakest part of the transport chain in terms of network performance, QoS management is most required for this network.

## 7.3 Security

The security of remote access is a continuing concern in mobility services, especially in cases where the PoA is a visited network. Examples are vulnerability of communications at public terminals which may be exposed to illicit caching of data or keystroke logging.

In general remote access has to address all the security requirements of an enterprise network. The key issues are:

- Confidentiality: no unauthorized information leakage or access
- Integrity: no unauthorized data modification
- Non Repudiation: performed actions can not be denied
- Availability: no Denial of Service/ accessibility of services or data
- Privacy: no unauthorized profiling, disclosure and modification.

In the following some mobility related security functions are briefly introduced.

### 7.3.1 User and device identification

A common mean for identification of user and terminals in the IT world are names. This concept is going to be adopted by ICT services in public and enterprise networks, because names can be remembered more easily than IP addresses. In addition, such aliases form a basis for user mobility, since a user may change IP address while keeping the same name.

SIP allows a client to bind a permanent SIP URL to a temporary SIP URL reflecting the current network location. Location servers are used by a SIP or proxy server to obtain information about a callee's possible location(s). A SIP URL address can designate an individual (possibly located at one of several terminals), the first available person from a group of individuals or a whole group.

The use of names (aliases) requires mechanisms for assigning names to IP addresses and for translating names into IP addresses. These mechanisms can be enabled by the Domain Name System, which provides a hierarchical administration of names facilitating a distributed database for mapping names to IP addresses.

User profile capabilities will increase the ability of the user to provide appropriate identifications, and will also increase the ability of services and networks to translate those names into addresses, both under greater user and enterprise control.

© ISO/IEC 2006 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

### 7.3.2 Authentication

Authentification of users and terminals is a key functionality of the MM to prevent misuse of the enterprise ICT resources by attackers or unauthorized persons or entities. The support of both user and terminal mobility requires to separately authenticate both terminals and users.

Single sign-on

In case of provisioning of services across network boundaries authentication of service access by a single sign-on is of high importance for user acceptance of mobility.

The Liberty Alliance Project (LAP) provides such a single-sign on solution for HTTP traffic. The basic is that ISPs do not perform user authentication themselves but relies on an Identity Provider (IdP). The LAP does not mandate any particular mechanism for user authentication, e.g. 3GPP AKA may be used. The IdP generates Security Assertion Markup Language (SAML)-based authentication assertions related to multiple authentication contexts and provides these to ISPs. Ultimately the ISP authorizes end-user access to ISP services.

Corporate user mobility demands that multiple choices are available to complete any desired communication. Part of that is the increasing capability of end user devices and their ability to communicate in personal area networks. In most cases not all of a user's devices will contain the same authentication capabilities, so corporate mobility requires that any supporting networks and services allow the flexible execution of authentication and identification processes, such as the identification of a user's SIM card on one device through a network connection on another device within their PAN.

A user profile active when a user is on enterprise business may also carry various authentication data and information on the relationship between the two enterprises, such as the existence of a sales or non-disclosure agreement, which may allow greater trust in the visited network.

### 7.3.3 Authorization

Access to enterprise ICT resources by an identified user and terminal must be granted by a server which is under full control of the enterprise administration. The degree of access may depend according the enterprise security policy on the user profile information, the security level of client software and hardware and the trust level of the network environment of the PoA.

### 7.3.4 Access by VPN

A common approach for securing remote access to enterprise ICT resources from a visited network or for provisioning of supplemental security for WLAN deployments is the use of Virtual Private Networks (VPN).

VPNs can either be offered as a hosted service, as a managed service or operated by the staff of an enterprise using CPE and a 3rd party transit network. Key areas of functionalities for VPN to be used with mobility services are:

- Strong authentification and encryption options
- Universal secured access (any time, any where, any device)
- VPN mobility (session continuity while moving from a W-LAN into a cellular mobile network and vice versa)
- Security around the remote endpoint (monitoring and interrogation of trust level/ security level of endpoints depending on environment and installed client software)
- Able to scope with firewalls, full featured routing DHCP, filtering and intrusion detection
- Policy-based management system to control access and security policies
- Enforcement security policies before VPN tunnel is finalized.


© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Besides the widely used IPsec-VPNs SSL-VPNs are becoming an important method for securing communications, especially for remote access.

In Table 1 and Table 2 strengths and weaknesses of both approaches are presented:

**Table 1 — Strengths/ Weaknesses of IPsec VPNs**

| Strengths | Weaknesses |
|---|---|
| • IPSec provides full use of network resources including legacy applications<br>• Unique client on user device enhances authentication<br>• Application agnostic including VoIP<br>• Supports voice & data traffic<br>• Ideal applications are<br>  o Campus-to-campus trunking<br>  o Connection of teleworkers/ branch offices | • Requires client software installation/ management<br>• Needs firewall reconfiguration/ compatibility |

**Table 2 — Strength/ Weaknesses of SSL VPNs**

| Strengths | Weaknesses |
|---|---|
| • 'Clientless' extranet solution allows freedom of remote access device<br>• Provides tight access control because session is specific to an application/ server<br>• Network agnostic<br>• Ideal applications:<br>  o Remote access via enterprise web portals<br>  o eBusiness applications (B2C/B2B) | • Limited to SSL capable applications – Typically limited to 'web' applications – primarily HTTP, POP, IMAP, FTP<br>• SSL handshake slows performance<br>• One session per application, i.e. multiple sessions if need for many apps<br>• Not suitable for voice traffic<br>• Written for TCP traffic only<br>• Certificate verification and key signing uses large amount of server processing resources |

Independent of the type of VPN, there are some general issues with use of VPNs to secure traffic:

- Insufficient security of the authentification process.
- Inefficient routing, because all traffic is always routed across the enterprise network irrespective of the route destination.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

# 8 Use cases of enterprise mobility

The level of mobility service and the kind of required network resources is strongly dependent from the user's application profile and the network infrastructure being involved in the connection. Below some examples of main user roles and their corresponding characteristics are introduced in Table 3:

NOTE An individual will always have more than one role, having at least working and idle time modes.

**Table 3 — Mobility profiles of typical enterprise users**

| | Campus Nomad | Teleworker | Road Warrior |
|---|---|---|---|
| **Application profile** | Workers with frequent on-campus or inter campus movements | Small/ Home office (SOHO) workers | Workers with frequent off-campus movements, e.g. in the area of field service, sales, transport/ logistics |
| **Point of network attachment** | on campus<br>e.g. enterprise premises, hospital, manufacturing, retail | off campus<br>e.g. home office, branch office | off campus<br>e.g. external enterprise premises, hotel, airport, Internet cafe |
| **Typ. mobility services** | mobile,<br>portable | nomadic | mobile,<br>nomadic |
| **Access networks** | Corporate LAN, WLAN/ WiFi | Public WAN (carrier, ISP), WiMAX, xDSL | Public WAN (carrier, ISP), public WWAN, private LAN. public WLAN/ WiFi (hotspot), WiMAX |
| **Terminals** | office PC (voice & data),<br>office laptop (voice & data),<br>PDA (voice & data),<br>office desktop phone (voice)<br>WLAN-phone (voice),<br>cell phone (voice),<br>smart phone (voice & data), | office PC (voice & data),<br>office laptop (voice & data),<br>desktop phone (voice) | non-office PC (voice & data),<br>office laptop (voice & data),<br>PDA (voice & data),<br>desktop phone (voice)<br>WLAN-phone (voice),<br>cell phone (voice),<br>smart phone (voice & data) |

A selection of use cases for enterprise mobility is introduced in the subsequent clauses. Here, only full IP-based scenarios with fixed configured networks are considered. Technologies such as adhoc networks, meshed networks and moving networks have been left out as their relevance for enterprise mobility is currently unclear. The associated technical issues are presented by a brief analysis of the involved mobility types and the technical challenges of the communication system.

## 8.1 Mobility starting from the home network

The following use cases cover scenarios where the user changes his PoA from a location in his home network, i.e. the intranet of an enterprise. Figure 2 shows the network interconnections which may needed to provide the mobility service.


© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

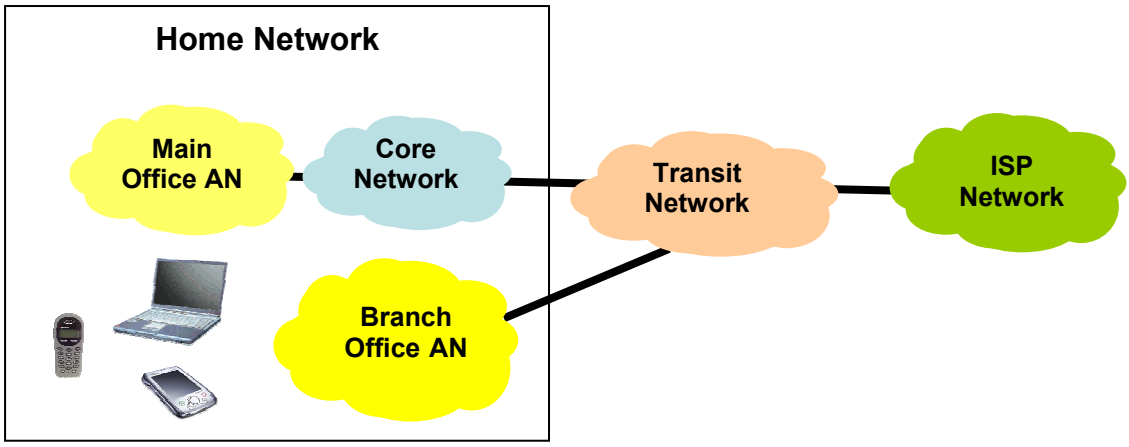


**Figure 2 — Network interconnections at on-campus scenarios**

A more detailed IP-network architecture of an enterprise campus is depicted in Figure 3 Besides the fixed line converged network infrastructure (IP-PBX, LAN, voice data terminals) a wireless infrastructure is provided by WLAN. The LAN and WLAN subnets are connected via LAN switches or routers. As depicted here the campus subnets may belong to diverse administrative domains. Although LAN and WLAN are physically different subnets they might appear to the user as a unique network by using Virtual LAN (VLAN) technology. Mobility support includes management (i.e. handover, roaming) and mobility services (i.e. location, presence) to provide mobility features to the network. In case of coverage of campus with a large number of access points (APs) access controllers (ACs) (not depicted here) may be used in addition to ease management and configuration.

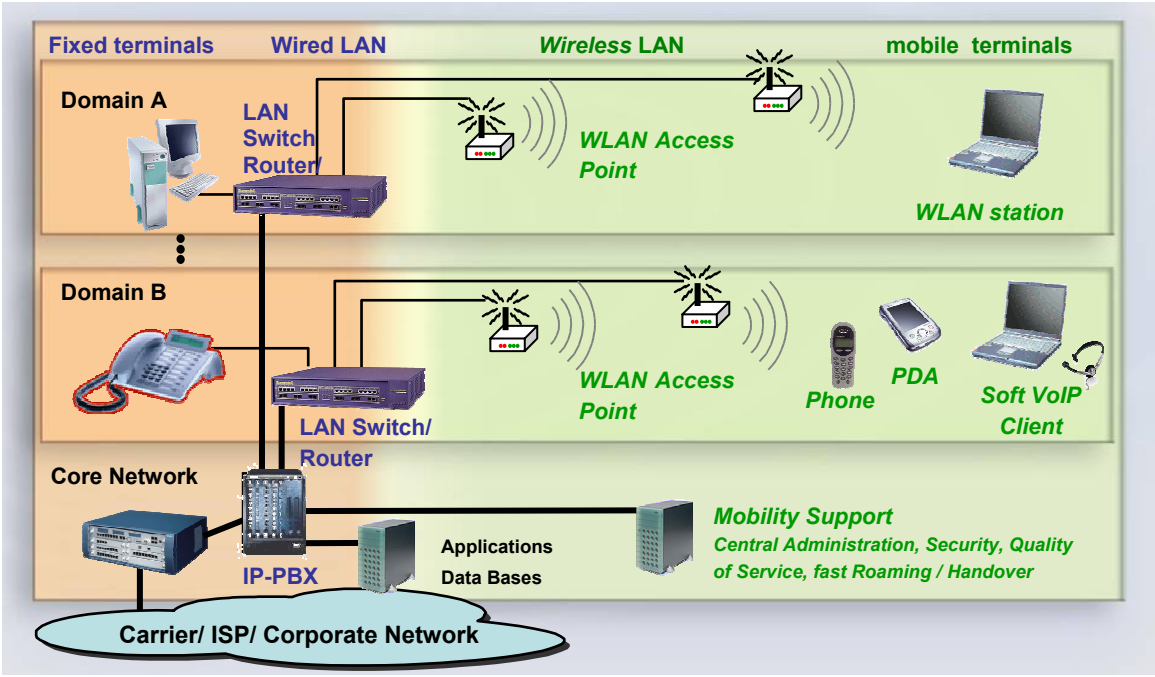


**Figure 3 — Overview to on-campus scenarios**

For the following use cases the home network of an employee is subdivided into a home domain, where the user has his service subscription, and a multitude of visited domains.

© ISO/IEC 2006 All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

### 8.1.1 Use case: Discrete mobility within the home domain

Scenario: An employee working at his office with his laptop using a LAN connection (voice & data connectivity) leaves his desk for an on-site business meeting. In the meeting room he reconnects his laptop via WLAN, which belongs to the same network domain, without having quit his previous communication session.

**Table 4 — Mobility issues of use case 8.1.1**

| Mobility Type | Network roaming | | Granularity |
|---|---|---|---|
| | Cross-technology | Cross-domain | |
| user, terminal, session | inter | intra | portable |

**Table 5 — Technical challenges of scenario 8.1.1**

| | Challenges |
|---|---|
| **Architecture** | • Provisioning of a location service<br>• Provisioning of a presence & availability service |
| **Management** | • Session handover from LAN to WLAN subnet |
| **Security** | • Authentication and authorization of terminal and user<br>• Encryption of WLAN connection (WPA2 or 802.11i) |

### 8.1.2 Use case: Discrete mobility between home and visited domain

Scenario 1: An employee disconnects his laptop from his office WLAN in building A (home domain A) without closing his session and moves to a meeting room in building B of the campus, where he reconnects his laptop to the WLAN (visited domain B).

**Table 6 — Mobility issues of use case 8.1.2 scenario 1**

| Mobility Type | Network roaming | | Granularity |
|---|---|---|---|
| | Cross-technology | Cross-domain | |
| user, terminal, session | intra | inter | portable |


© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

**Table 7 — Technical challenges of use case 8.1.2**

| | Challenges |
|---|---|
| **Architecture** | • Support of inter-domain roaming service<br>• Provisioning of a location service<br>• Provisioning of a presence & availability service |
| **Management** | • Roaming between domain A and B<br>• Management of terminal and user profiles<br>• Management of large WLAN AP networks |
| **Security** | • Authentication and authorization of terminal and user<br>• Encryption of WLAN connection (WPA2 or 802.11i) |

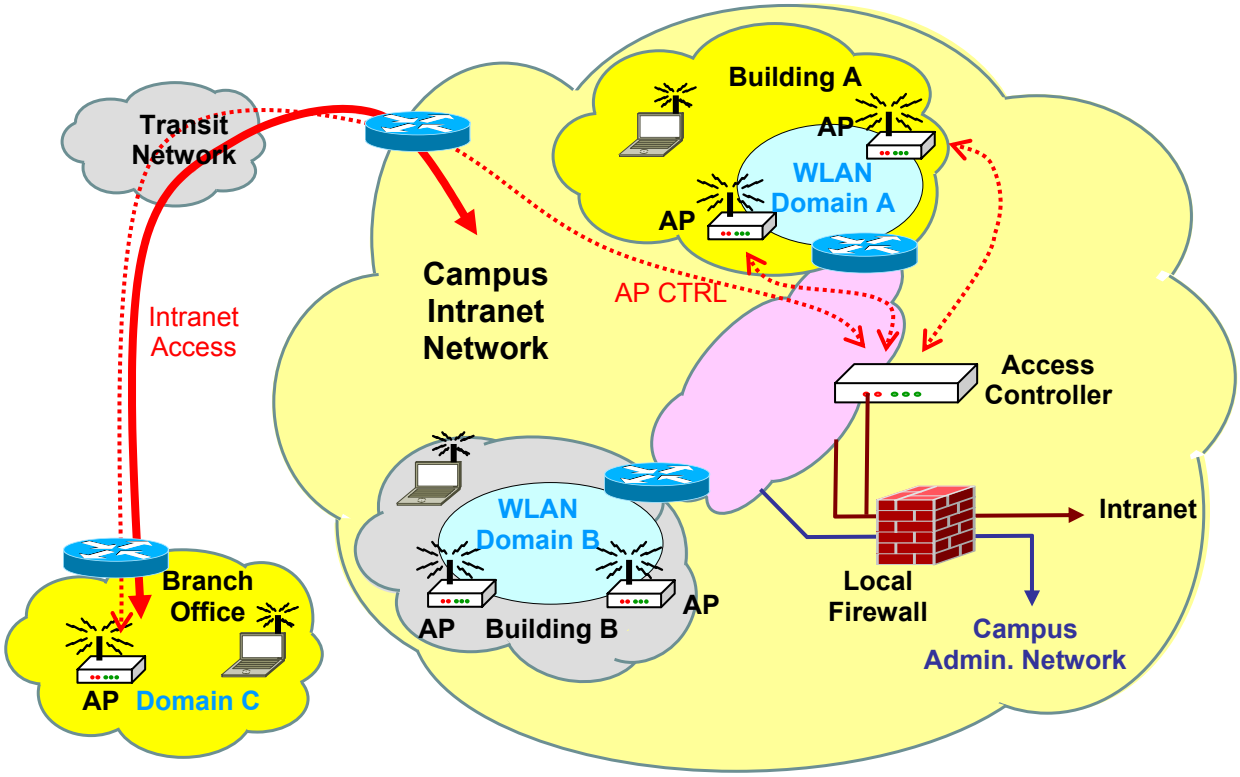


**Figure 4 — Interconnection scenarios 1 and 2 of use case 8.1.2 (The solid red line indicates data transport, the dotted red lines indicate mobility management signalling)**

Scenario 2: An enterprise user accesses the enterprise resources (voice & data) from a branch office using a wireless guest terminal (desktop phone or computer) which belongs to different domain (domain C) than the user's home domain (domain A).

© ISO/IEC 2006 All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

**Table 8 — Mobility issues of use case 8.1.3 scenario 2**

| Mobility Type | Network roaming | | Granularity |
|---|---|---|---|
| | Cross-technology | Cross-domain | |
| user | NA | inter | nomadic |

**Table 9 — Technical challenges of scenario 8.1.3 scenario 2**

| | Challenges |
|---|---|
| **Architecture** | • Support of domain roaming service<br>• Provisioning of a location service<br>• Provisioning of a presence & availability service<br>• Provision of VPN connection from branch office to the core network<br>• NAT/ firewall traversal at the edge of branch office and core network<br>• Interfacing with transit network |
| **Management** | • Roaming between domain A and C<br>• Management of user profile |
| **Security** | • Provision of secure transit connection between enterprise locations (use of VPNs, others)<br>• Authentication and authorization of terminal and user |

### 8.1.3 Use case: Continuous mobility between two visited domains

Scenario: An employee is connected at a meeting via a smart phone to the WLAN in building B (domain B), and roams during a phone call into the WLAN domain of building D (domain D). Both domains belong to different administrations and are not the home domain of the user.

**Table 10 — Mobility issues of use case 8.1.3**

| Mobility Type | Network roaming | | Granularity |
|---|---|---|---|
| | Cross-technology | Cross-domain | |
| user, terminal, session | intra | inter | mobile |


© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

**Table 11 — Technical challenges of use case 8.1.3 scenario 1**

| | Challenges |
|---|---|
| **Architecture** | • Provisioning of secure connection (L2 VPN, voice VPN, no VPN)<br>• Provisioning of a location service<br>• Provisioning of a presence & availability service |
| **Management** | • Seamless handover between WLAN domain B and WLAN domain D |
| **Security** | • Authentication and authorization of terminal and user<br>• Encryption of WLAN connection (WPA or 802.1i) |

### 8.1.4 Use case: Continuous mobility between home domain and a visited network

Scenario: An employee has received a call on his dual-mode smart phone which connects him via the campus WLAN. During the call he left the coverage area of the enterprise WLAN and the connection is continued by public carrier mobile network.

**Table 12 — Mobility issues of use case 8.1.4**

| Mobility Type | Network roaming | | Granularity |
|---|---|---|---|
| | Cross-technology | Cross-domain | |
| user, terminal, session, service | inter | inter | mobile |

**Table 13 — Technical challenges of scenario 8.1.4**

| | Challenges |
|---|---|
| **Architecture** | • Interworking of presence and location services<br>• IP-Gateways (policy enforcement, NAT/ Firewall traversal)<br>• Means for secure transport (VPN, …)<br>• carrier/ enterprise network-to-network Interface |
| **Management** | • Accounting & billing<br>• Handover between WLAN and carrier network<br>• Seamless roaming between carrier<br>• Federated management of end to end security and QoS<br>• Interoperability between public network services and enterprise network services<br>• Presence & location service across network borders |
| **Security** | • Authentication & authorization of user and terminal<br>• Secure transport<br>• Adaptation of access rights according to the trust level of the network entities of the visited network |

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2006 All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

## 8.2 Mobility starting from a visited network

Off-campus mobility cover use cases where the PoA is located in a visited network, i.e. remote access to enterprise ICT resources by employees from outside the enterprise network.

Figure 5 shows a generic interconnection path. The required services of a session, e.g. PBX-features, security services, presence services, are in many cases provided by the home network but may be provided by a service provider or the visited network as well.

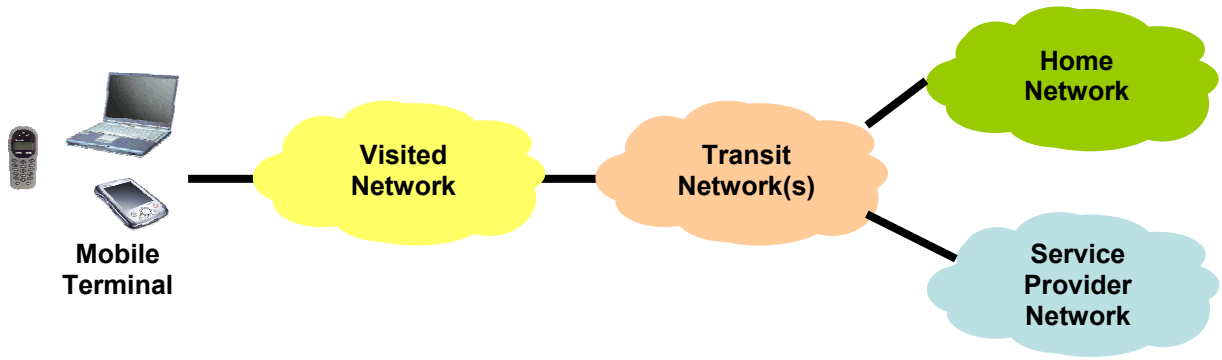


**Figure 5 — Network interconnections for off-campus mobility**

As shown in Figure 6 possible access scenarios include access by wireless and wireline devices from the following visited networks:

- WLAN Hotspots at e.g. airports, hotels, conference sites
- Hospitality LANs e.g. at hotels
- Public IP-based Wireless WANs e.g. UMTS
- Carrier based IP- networks, e.g. an NGN
- Residential LAN or WLANs owned by e.g. a SOHO or teleworker
- Public IP networks e.g. the Internet or ISP-networks
- Intranet of a different enterprise
- Moving networks such as WLAN access in a train or airplane.

Transit networks provide the transport from the access network to the user's home network, in most cases by VPNs. Such service may be offered by public carriers and ISPs.

For security reasons enterprise networks are shielded from outside networks by a firewall, NAT, or combination thereof to block unwanted traffic. In most cases enterprise networks use an isolated IP address space. For connection of enterprise networks (with a private IP address space) to external networks (with globally unique IP addresses) NAT and NAPT devices are used.


--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2006 – All rights reserved
Not for Resale

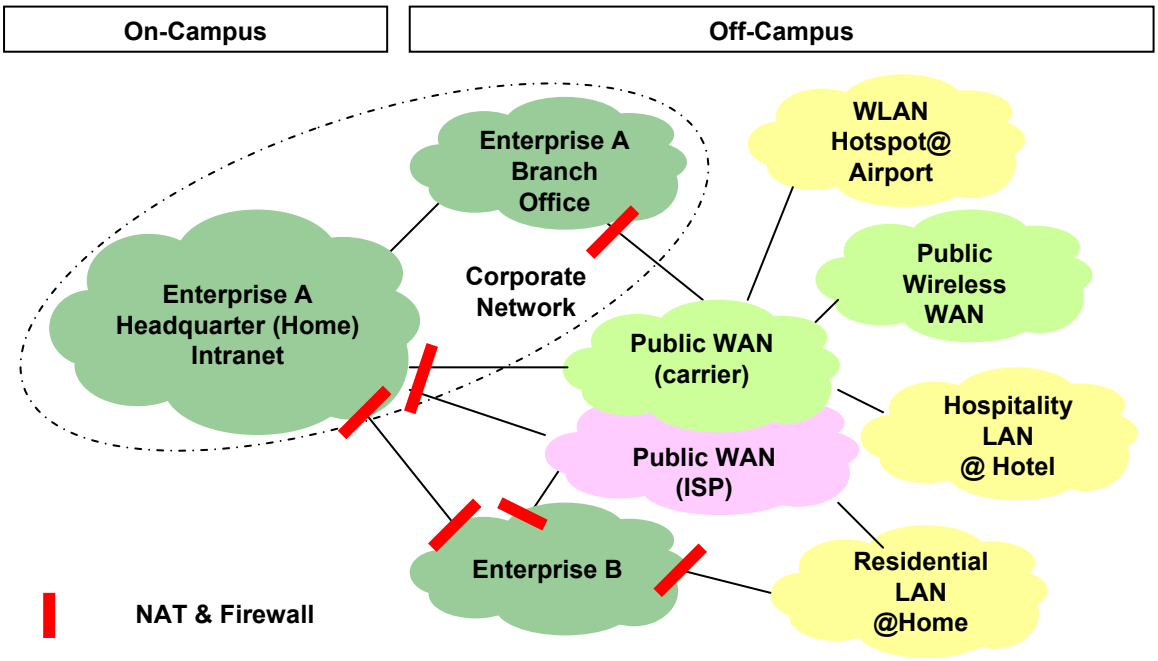


**Figure 6 — Overview of off-campus scenarios**

### 8.2.1 Use case: Discrete mobility in a visited public network

Scenario: A mobile worker accesses the enterprise intranet via a public WLAN connection being provided by a hotel. Figures 7 and 8 show suitable network scenarios with and without use of a managed VPN service provided by an ISP.

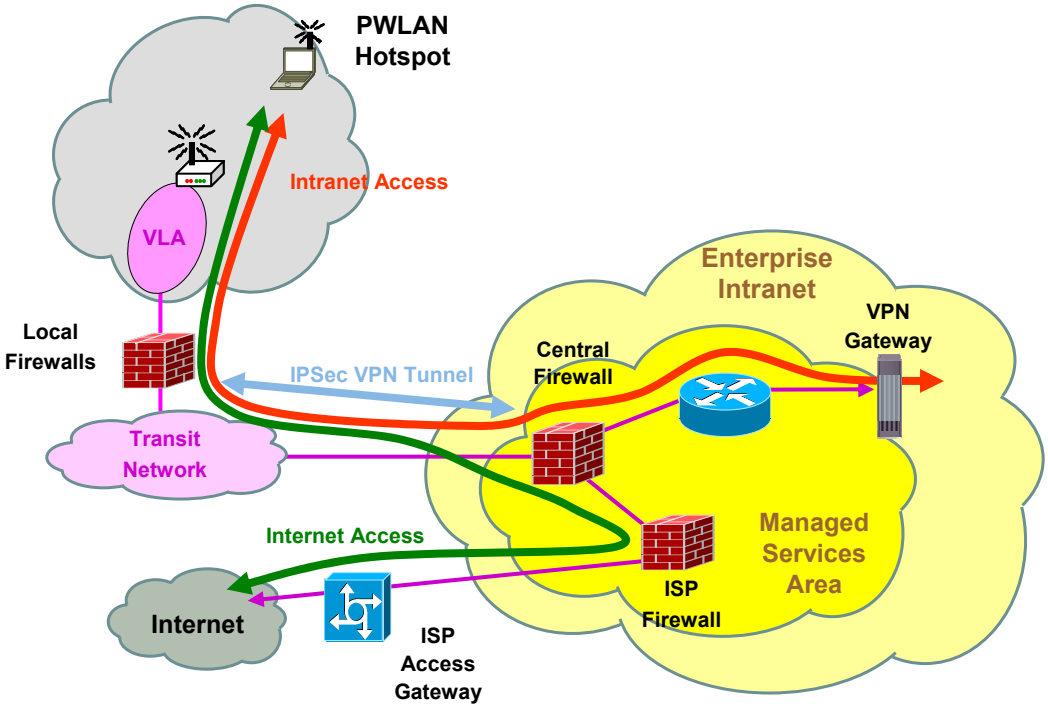


**Figure 7 — Intranet & Internet access from PWLAN with VPN using managed services from an ISP**

© ISO/IEC 2006 All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

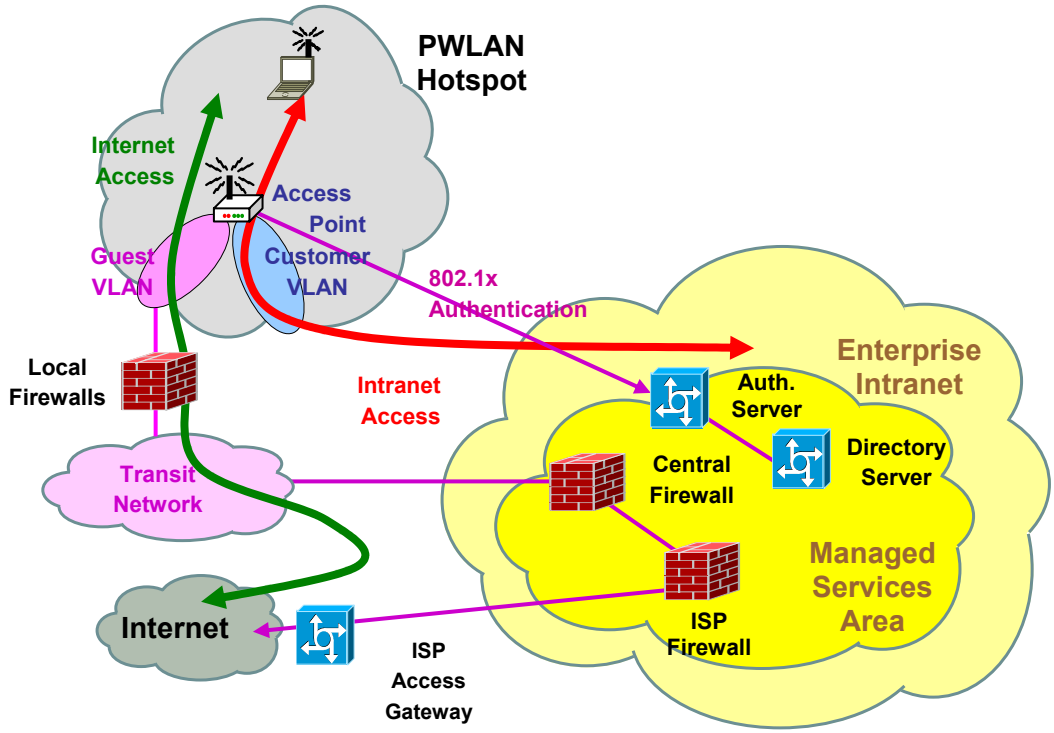


**Figure 8 — Intranet and Internet access from PWLAN without VPN using managed services from an ISP**

**Table 14 — Mobility issues of use case 8.2.1**

| Mobility Type | Network roaming | | Granularity |
|---|---|---|---|
| | Cross-technology | Cross-domain | |
| user, terminal, service | NA | inter | nomadic |

**Table 15 — Technical challenges of use case 8.2.1**

| | Challenges |
|---|---|
| **Architecture** | • Interfaces between WLAN and transit network<br>• Interfaces transit network and enterprise network<br>• Roaming interfaces<br>• Provisioning for end-to-end QoS<br>• IP-gateway control (NAT/firewall, interconnection policy) |
| **Management** | • Federation agreement between involved parties<br>• one number identity across networks<br>• Aggregation of presence and availability information |
| **Security** | • Secure connection by SSL-VPN tunnels, IPsec tunnels or VPN less solutions,<br>• Federated authentication and authorization between networks enabling single sign-on service<br>• End-to-end security |


Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2006 – All rights reserved
Not for Resale

### 8.2.2 Use case: Discrete mobility in a visited enterprise network

Scenario: For field service automation a manufacturer lets the field employees to schedule and dispatch workforces, and allows creating, reviewing and updating work orders at the customer site by using mobile devices.

**Table 16 — Mobility issues of use case 8.2.2**

| Mobility Type | Network roaming | | Granularity |
|---|---|---|---|
| | Cross-technology | Cross-domain | |
| user, terminal, service | NA | inter | nomadic |

**Table 17 — Technical challenges of use case 8.2.2**

| | Challenges |
|---|---|
| **Architecture** | • Gateways/interfaces from/to transit network<br>• Traversal of multiple NAT/ firewalls operated by different companies<br>• Interfaces transit network and enterprise network<br>• Roaming interfaces<br>• Provisioning for end-to-end QoS<br>• IP-gateway control (NAT/firewall, interconnection policy)<br>• Provision of location information |
| **Management** | • one number identity<br>• Aggregation of presence and availability information |
| **Security** | • Use of VPN tunnels, or VPN less solutions, e.g. RPC over HTTP<br>• Federated authentication and authorization between networks enabling single sign-on service<br>• End-to-end security<br>• Different trust levels between known visitors and the NGCN |

### 8.2.3 Use case: Discrete mobility in a residential network

Scenario: A teleworker access his enterprise resources (voice and data) from his private terminal at his home. He is connected via an xDSL access to the public IP-network. A possible network interconnection is shown in Figure 9.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

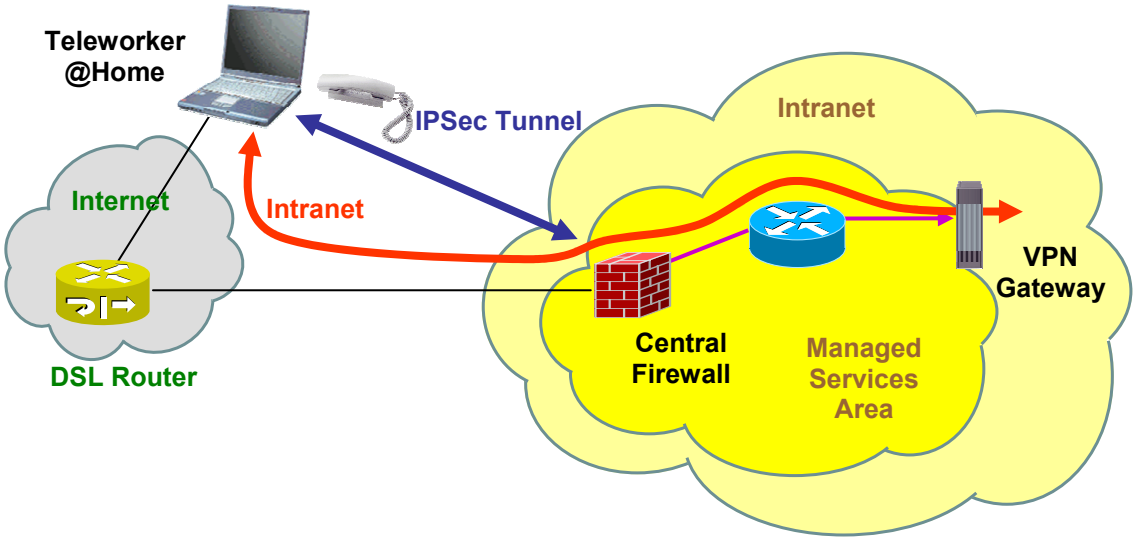


**Figure 9 — Access from a residential network via Internet access**

**Table 18 — Mobility issues of use case 8.2.3**

| Mobility Type | Network roaming | | Granularity |
|---|---|---|---|
| | Cross-technology | Cross-domain | |
| user, terminal, service | NA | inter | nomadic |

**Table 19 — Technical challenges of use case 8.2.3**

| | Challenges |
|---|---|
| **Architecture** | • Similar to use case 8.2.2 but NAT/firewall traversal is more relaxed<br>• Aggregation of presence and availability information<br>• Provision of location information |
| **Management** | • Authentication, authorization controlled by visited network<br>• one number identity |
| **Security** | • Secure transport by IPsec VPN tunnel<br>• End-to-end security |

### 8.2.4 Use case: Continuous mobility within a visited public network

Scenario: A user is travelling outside his premises network and is connected with his smart phone (voice & data) via the mobile network of a single mobile carrier.


Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2006 – All rights reserved
Not for Resale

**Table 20 — Mobility issues of use case 8.2.4**

| Mobility Type | Network roaming | | Granularity |
|---|---|---|---|
| | Cross-technology | Cross-domain | |
| user, terminal, session; service | intra | inter | mobile |

**Table 21 — Technical challenges of scenario 8.2.4**

| | Challenges |
|---|---|
| **Architecture** | • Service and management gateways |
| **Management** | • Local mobility management<br>• Provision of location and presence information to MM of home network<br>• end-to-end provisioning of services with quality and security constraints<br>• Collaboration of MMs of visited and home network |
| **Security** | • Provision of enterprise-grade security by VPN or other means |

### 8.2.5 Use case: Continuous mobility between different network technologies of a visited public network

Scenario: A user is connected to his enterprise with a dual-mode mobile phone via the WMAN of a public carrier. When entering the coverage area of the PWLAN network of the same carrier, the phone automatically hands over the session to the WLAN part of the phone.

**Table 22 — Mobility issues of use case 8.2.5**

| Mobility Type | Network roaming | | Granularity |
|---|---|---|---|
| | Cross-technology | Cross-domain | |
| user, terminal, session; service | inter | inter | mobile |

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

**Table 23 — Technical challenges of use case 8.2.5**

| | Challenges |
|---|---|
| **Architecture** | • Distribution of AAA tasks between enterprise and carrier networks<br>• Support of route optimizations for fast handovers<br>• Provision of location information to the home network |
| **Management** | • Local mobility management enabling fast handover between WWAN and WLAN<br>• Global mobility management for handling of enterprise network/ public network roaming<br>• Interworking of MM functions between visited network and home network<br>• Distribution of access control between visited network and home network<br>• Seamless handover from WMAN to WLAN<br>• End-to-end QoS<br>• Adaptation of user's access rights according to the trust level of his connection |
| **Security** | • Enterprise grade security level of WLAN connection<br>• End-to end security<br>• Determination of trust level of involved network nodes |

### 8.2.6 Use case: Continuous mobility between different visited public networks

Scenario: A user has a real-time communication session using enterprise resources. The PoA of his connection changes from public WWAN of carrier A to public WWAN of carrier B during his trip.

**Table 24 — Mobility issues of use case 8.2.6**

| Mobility Type | Network roaming | | Granularity |
|---|---|---|---|
| | Cross-technology | Cross-domain | |
| user, terminal, session; service | intra | inter | mobile |


© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

**Table 25 — Technical challenges of use case 8.2.6**

| | Challenges |
|---|---|
| **Architecture** | • Inter carrier & carrier-enterprise interworking (network-to-network interfaces)<br>• Provision of secure end-to-end services (QoS, security) |
| **Management** | • Local MM (roaming service) between carrier A, B and enterprise<br>• Global MM between carrier network and enterprise network<br>• Presence and location management<br>• Seamless handover and roaming |
| **Security** | • AAA<br>• Reachability by the enterprise dial plan<br>• Single sign-on |

### 8.2.7 Use case: Continuous mobility between a visited public network and the home network

Scenario: A user has an ongoing voice call received on his dual-mode mobile phone. When entering one of his enterprise domains the call is automatically handed over from the cellular network of the public carrier to the WLAN domain of the enterprise campus.

**Table 26 — Mobility issues of use case 8.2.7**

| Mobility Type | Network roaming | | Granularity |
|---|---|---|---|
| | Cross-technology | Cross-domain | |
| user, terminal, session, service | inter | inter | mobile |

**Table 27 — Technical challenges of use case 8.2.7**

| | Challenges |
|---|---|
| **Architecture** | Similar to use case 8.1.4 |
| **Management** | Similar to use case 8.1.4 |
| **Security** | Similar to use case 8.1.4 |

© ISO/IEC 2006 All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

# 9 Functional requirements on enterprise-grade mobility

As enterprise mobility has many stakeholders with different interests, the requirements are organized to reflect their particular perspectives. Stakeholders are:

- The mobile user.
- The operator(s) of the enterprise network domain(s), including the administration of communication, information resources and the mobility services.
- 3rd party service providers, providing hosted mobility services for the enterprise. Examples are public network operators (wireline and wireless) and Internet Service provider (ISPs).
- Regulation authorities, who set a legal framework for operating services in their area of responsibility.

The requirements are categorized according to the concerns of these parties. The numbering of the requirements consists of a 4-digit code which is organized as follows:

| TYPE (G/ A/ M/ S) | PERSPECTIVE (U/ O/ P/ R) | 2 digit number |
|---|---|---|

TYPE: **G**eneral, **A**rchitecture, **M**anagement, **S**ecurity

PERSPECTIVE: **U**ser, enterprise network **O**perator, service **P**rovider, **R**egulation authority

**Figure 10 — Code letters used for requirements**

For improved understanding of the requirements additional information and references to relevant use cases are given below.

## 9.1 Enterprise user's perspective

The users of enterprise mobility services are one of the most critical actors in the enterprise communication chain. If the user of such services don't find their acceptance the communication process is broken. Table 28 lists their requirements on a enterprise-grade mobility infrastructure:

**Table 28 — User requirements**

| User Requirements | | Notes | Use Case |
|---|---|---|---|
| AU01 | Availability of highly responsive services. | By providing presence and availability aware communications, (instant messaging, push-to-talk, etc. with short latency and set-up times. | All |
| AU02 | Use of a variety of terminals and access points with automatic configuration, including devices with shared resources on a personal area network, such as Bluetooth. | E.g. WLAN phones, laptops, PDA, cell phones, …. | 8.2.1, 8.2.4, 8.2.5, 8.2.6, 8.2.7 |
| AU03 | Enterprise-grade quality for voice and data services. | In terms such as security, reliability and perceived media quality. | All |

--`,,```,,,,````-`-`,,`,,`,`,,`---



Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale
© ISO/IEC 2006 – All rights reserved

**Table 28 — User requirements** (*continued*)

| | | | |
|---|---|---|---|
| AU04 | Support of rule based call routing, with rule sources including corporate and private user profiles. | Denotes specific routing based on calling party (individual or priority groups), time zone, presence status, availability or access situation (e.g. sitting in a car which implies voice only access/ availability, participating a meeting which implies restricted access/ availability via text messages such as IM, SMS, or e-mail.), etc. | All |
| AU06 | Enterprise-grade availability/ reliability of service access. | The change of networks must be transparent to the user. | All |
| AU07 | Assured end-to-end quality of service for real time and data services. | E.g. by DiffServ mechanisms. | All |
| AU08 | Enterprise-grade secure access to business information services for authorized users. | E.g. PIM, CRM, ERP services. | 8.2.1 to 8.2.7 |
| AU09 | Access to enterprise resources with non-specific enterprise terminals. | E.g. by terminals with non-enterprise client software. Means may include SSL VPNs, portal services, RPC over HTTP or security updates of client software. | 8.2.1, 8.2.4, 8.2.5, 8.2.6, 8.2.7 |
| AU10 | Subscription to a single presence entity to monitor and publish presence information from different sources for a single user, possibly limited to user selected modes (such as “working” or “playing”). | This must be supported by an aggregated presence service of the home network operator. | 8.2.1, 8.2.4, 8.2.5, 8.2.6, 8.2.7 |
| GU01 | Use with unified user experience across networks. | E.g. user authentication, dialling plan, permissions, user interface, security policy, quality of service, end-to-end speech quality, personal and enterprise directory, applications, application settings, e.g. favourites): the point of network access or the device should not impact the behaviour of a service or data communication. | All |
| GU02 | Use of the enterprise dial plan for establishing outgoing and incoming communications. | The remote terminal user should be addressed by the same number or identifier by which he is reachable in his enterprise office. | 8.2.1 to 8.2.7 |
| GU03 | Reception of incoming communications with the same filtering and forwarding rules applied. | The remote terminal should behave as if it were connected directly to the enterprise LAN. | 8.2.1 to 8.2.7 |
| GU04 | The retention of user preferences, favourites, short-cuts, privileges, etc.; independent of the PoA. | | All |

© ISO/IEC 2006 All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

**Table 28 — User requirements** (*continued*)

| | | | |
|---|---|---|---|
| MU01 | Support of seamless mobile access across networks for real-time and data services. | Regardless of whether the user is connected via a cellular or wireless access he is available under one single address/number. | All |
| MU02 | Access to features of enterprise services/ applications should be agnostic to the network technology and administration. | Restrictions may be applied to access to enterprise critical applications/services from a unsecured environment (e.g. Internet Café). | All |
| SU01 | Single log-on for authentification irrespective of PoA. | The user has to register only once to get access to the network resources and to the services for which the user is registered at the network (mobile, carrier, enterprise) and allowed to use. | 8.2.1 to 8.2.7 |
| SU02 | No unauthorized disclosure or manipulation of user data. | Including user preferences, profiles, presence & availability and location information. | All |
| SU03 | Support of role based identities. | A business user can identify himself to the network with different identities e.g. as an ordinary employee, as project manager etc. thus getting different access rights to ICT resources. | All |
| SU04 | Easy to use secure connection models. | E.g. for WLAN via portals using UAM or 802.11i. | All |

## 9.2 Enterprise network operator's and IT manager's perspective

The justification for evolving enterprise networks to provide mobility is to give a competitive advantage in terms of increased customer satisfaction by more responsive workflows. However, mobility for enterprise communication comes with new challenges for the security and stability of the enterprise ICT network. Table 29 lists the requirements from a enterprise network operator:

**Table 29 — Operator requirements**

| Operator Requirements | | Notes | Use Case |
|---|---|---|---|
| AO01 | Interoperability of mobility functions between the enterprise network and the visited networks via intervening transit networks. | This will require a federated management system with standardized interfaces to realize fault, configuration, accounting, performance and security management across networks and network boundaries. | 8.1.4, 8.2.1 to 8.2.7 |
| AO02 | Network must provide mediation functions between different networks technologies and terminal types. | This is related to the provision of inter-technology mobility for networks and the adaptation of application to the capabilities of the terminal. | All |


--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale
© ISO/IEC 2006 – All rights reserved

**Table 29 — Operator requirements** (*continued*)

| | | | |
|---|---|---|---|
| AO03 | Provision of seamless handover and roaming for real-time services. | Essential for enterprise-grade voice services. | All |
| AO04 | Seamless integration of communication processes into business processes/ workflow. | E.g. Customer Relation Management (CRM), Enterprise Resource Planning (ERP), personal Information Management (PIM). | All |
| AO05 | Network must provide full featured call control services across networks. | Enterprise applications should seamlessly interwork on-campus and off-campus networks. | All |
| AO06 | Network must provide means (signalling & management) for on-campus handling of emergency calls of mobile users. | This includes availability of location information. | 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.7 |
| AO07 | Provision of aggregated billing mechanisms for 3rd party mobility services. | | 8.1.4 to 8.2.7 |
| AO08 | Interface definitions and MM functions shall support discrete & continuous mobility across heterogeneous access networks, preserving enterprise-grade service quality. | | All |
| AO09 | The number of different authentication mechanisms for access networks should be kept to a minimum. | | All |
| AO10 | Single set of QoS classes (open standard) across heterogeneous networks/ domains. | | All |
| AO11 | Common (open standard based) data collection/ rating for billing charging. | | 8.1.4 to 8.2.7 |
| AO12 | Common (open standard based) service reporting. | | All |
| AO13 | Separation of information relating to mobile users (e.g. service feature, preferences) from service execution and network domain data. | This will enable simplified information management. User data will be resident in a profile server. | All |
| AO14 | Provision of centralized access control and configuration of WLAN access points. | For full coverage of an enterprise campus with seamless mobile service with large number of Aps. | 8.1.2 |
| AO15 | Centralized management and control of all user specific corporate data by the enterprise. | E.g. user profiles. | All |

© ISO/IEC 2006 All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

**Table 29 — Operator requirements** (*continued*)

| | | | |
|---|---|---|---|
| AO16 | Co-operation with visited to allow ICT service provision under control of the enterprise. | This requires federation of control functions, e.g. MM of involved networks. | 8.1.4 to 8.2.7 |
| GO01 | Provision of Enterprise-grade service quality across networks. | Same user experience and security for off-campus mobility as used from desktop access in the office<br><br>This includes:<br>• Authentification<br>• Dial plan<br>• Quality of voice and video communication<br>• Response times of applications (set up, latency)<br>• Protection to data theft, privacy and DoS attacks | All |
| M001 | Enterprise WLANs should support of seamless multi-subnet roaming. | Desired features are:<br>• use of standard WLAN devices without MM clients<br>• support of multimodal services<br>• independent of Layer 2 and 3 technology<br>• low latency for handover & roaming | 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.7 |
| MO02 | Aggregated presence management provision of users with a single site to subscribe to presence services dispersed over different networks. | Allows a user to subscribe to a single presence entity to monitor presence information from different sources for a single user. | 8.1.4, 8.2.1 to 8.2.7 |
| MO03 | Provisioning of standardized signalling to support mobility across heterogeneous networks and domains including enterprise and public networks. | | All |
| MO04 | Standardized methods for identifying users at access network level. | To guarantee interoperability of the roaming service across multiple administrative domains. An example is the NAI mechanism according. RFC 2486. | All |


Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2006 – All rights reserved
Not for Resale

**Table 29 — Operator requirements** (*continued*)

| | | | |
|---|---|---|---|
| MO05 | Mobility management for on-campus communication and remote access from visited networks including the support of a variety of mobility-enabled devices. | Remote support for a variety of access devices having multiple operating systems, client software and with varying computing and presentation capabilities. | All |
| MO06 | The visited network should provide location information on the current PoA to the home network. | For some business processes the location of the travelling work force is essential. | All |
| SO01 | The location information of users should be concealed from non-trusted entities (location privacy). | To avoid eavesdropping of a user's behaviour location related information, e.g. link and transport layer identifiers in protocols, and geographical data should keep private from third party which are not intentionally involved in the communication. | 8.1.4 to 8.2.7 |
| SO02 | Mobility security must be embedded into the enterprise security model. | | |
| SO03 | Support of single log-on across networks/ domains. | | All |
| SO04 | Support of trust levels for network & terminals according their supported security level. | | All |
| SO05 | Access to mission critical enterprise resources should depend on the user profile, the trust level of the involved network entities and the location of the PoA. | | 8.1.4, 8.2.1, 8.2.4 to 8.2.7 |
| SO06 | Possibility of means to upgrade security level by remote configuration of remote terminal. | Needed if access to mission critical ICT resources is not denied due to the insufficient trust level of client software of the terminal. | 8.1.4, 8.2.1, 8.2.4 to 8.2.7 |
| SO07 | Provision of multiple identities for a single user. | A single employee may take different business roles and therefore requires different profiles. | All |
| SO08 | Adaptation of access rights to mission critical resources according to the trust level of involved network entities and terminal. | Requires monitoring and interrogation of trust level (security level of endpoints depending on environment and client software). | 8.1.4 to 8.2.7 |
| SO09 | Automatic transfer of authentification when crossing network boundaries. | | All |

© ISO/IEC 2006 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

## 9.3 Perspective of 3rd party service providers

3rd party service providers get increasingly involved in enterprise communication by offering hosted and managed services to enterprises. Examples are IP CENTREX, transit services like VPNs to enterprise employees to access their home network from a visited network such as WLAN hotspots or wireless multimedia access by 3rd generation mobile networks. 3rd party services must fit into the enterprise network environment but also meet the business expectations of the service provider. Table 30 below lists their requirements:

**Table 30 — Service provider requirements**

| Service Provider Requirements | | Notes | Use Case |
|---|---|---|---|
| AP01 | Provision of means by the transit network operator to allow direct access to hosted ICT services by authorized users. | This should avoid delays due to routing of payloads via the home network of the user. | 8.1.4 to 8.2.7 |
| AP02 | Support of mobile, portable and nomadic access across networks for real-time and data with feature transparency. | | 8.1.4 to 8.2.7 |
| AP03 | Support of real-time services based on SIP. | NGNCN services will rely on SIP. | 8.1.4 to 8.2.7 |
| AP04 | One numbering service according enterprise dial plan. | Incl. ENUM service for interoperability between enterprise and public operator. | 8.1.4 to 8.2.7 |
| AP05 | Support of location service. | Information needed for presence/ availability services and is as well essential for business application as CRM. | 8.1.4, 8.2.1, 8.2.3 to 8.2.7 |
| AP06 | Support of presence service. | Presence-based communication is a key issue for future business communication. | 8.1.4, 8.2.1, 8.2.3 to 8.2.7 |
| AP07 | Provision of standard-based interfaces or profiles between network entities. | To enable co-operation on AAA, e2e security, e2e QoS, handover & roaming of multivendor/ operator WLAN networks. | 8.1.4, to 8.2.7 |
| AP08 | Provision of means for NAT/ firewall traversal. | This is essential for end-to-end signalling, e.g. global MM and the provision of end-to-end services in general. | 8.1.4 to 8.2.7 |
| MP01 | Management and performance monitoring with open standards. | | 8.1.4 to 8.2.7 |
| MP02 | Provisioning of an open mechanism (signalling & management) for charging/ billing. | | 8.1.4 to 8.2.7 |


Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale
© ISO/IEC 2006 – All rights reserved

**Table 30 — Service provider requirements** (*continued*)

| | | | |
|---|---|---|---|
| MP03 | Seamless roaming & handover to support enterprise-grade voice communication. | E.g. VoWLAN, requires improved fast handover and roaming mechanisms from standardization. | 8.1.4 to 8.2.7 |
| MP04 | Support of a standardized data format and network-2-network interface for accounting. | | 8.1.4 to 8.2.7 |
| MP05 | Provision of local MM for roaming between subnets of visited network. | To relief traffic to enterprise network | 8.1.4, 8.2.4 to 8.2.7 |
| MP06 | Standardized solution for federation of mobility management functions across administrative network boundaries. | To enable e2e services (QoS, security, applications). | 8.1.4 to 8.2.7 |
| SP01 | Provision of privacy of provider specific OAM information. | E.g. QoS reports. | 8.1.4 to 8.2.7 |
| SP02 | Support of multiple client credential types for user authentification. | | 8.1.4 to 8.2.7 |
| SP03 | Support of Single-sign-on across administrative network domains. | Single-authentification/ registration. | 8.1.4 to 8.2.7 |
| SP04 | Trust model for interworking between visited and home network. | For authorization of remote access to sensitive enterprise applications/ services, the home network needs a trust model to decide on security level of a connection. | 8.1.4, 8.2.1, 8.2.2, 8.2.4 to 8.2.7 |
| SP05 | Secure tunnels for authentification of connections without VPN tunnels. | E.g. 802.1x for WLAN. | 8.1.4 to 8.2.7 |
| SP06 | Enterprise-grade encryption of the air-interface. | E.g. 802.11i. | 8.1.4 to 8.2.7 |

## 9.4 Perspective of regulatory authorities and administrations

Potential issues for regulatory authorities and administrations are: emergency services, (including emergency telecommunication and disaster relief), lawful interception and privacy (to be considered in the context of presentation of business user's or terminal's identity, name, address and location information).

Several regulatory authorities, e.g. in the USA and in Europe, have started consultations on a regulatory framework for the provision of public VoIP-services.

However, at the time of preparation of this Technical Report it is not clear, whether or to what extent enterprise networks and in particular their internal communications traffic will be affected by those regulations that already apply to public network operators (e.g. on lawful interception, data retention). Beyond that, it is a still an open issue how to define the boundaries of an enterprise network, which, especially in the case of remote access, could share the network infrastructure of a universal services provider to which regulations apply. The challenge is how to handle such virtual enterprise networks.

NOTE In a circuit switched environment the T-reference point acted as demarcation between private and public network infrastructures and thus the boundary for regulation.

It is expected that enterprise networks, including virtual enterprise networks, will not be subject to more regulation than circuit switched enterprise networks.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

# Annex A
(informative)

# Standardization and promotion activities on enterprise mobility issues

The success and penetration of mobility in communication is tightly coupled to the availability of standards, e.g. transport protocols, signalling protocols and APIs. The following standardization organizations (SDO) and fora and consortia are among those active on standards and promotion of mobility issues which are considered as relevant for enterprise networks:

**Table A.1 — Standardization and promotion activities on enterprise mobility**

| | |
|---|---|
| 3GPP<br><br>3rd Generation Partnership Project | Is a collaboration agreement that brings together a number of telecommunications standards bodies such as ARIB, CCSA, ETSI, ATIS, TTA, and TTC. The original scope of 3GPP was to produce globally applicable Technical Specifications and Technical Reports for a 3rd Generation Mobile System based on evolved GSM core networks and the radio access technologies that they support (i.e., Universal Terrestrial Radio Access (UTRA) both Frequency Division Duplex (FDD) and Time Division Duplex (TDD) modes). The scope was subsequently amended to include the maintenance and development of the Global System for Mobile communication (GSM) Technical Specifications and Technical Reports including evolved radio access technologies (e.g. General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE)).<br><br>http://www.3gpp.org |
| 3GPP2<br><br>3rd Generation Partnership Project 2 | Is a collaborative third generation (3G) telecommunications specifications-setting project comprising North American and Asian interests developing global specifications for ANSI/TIA/EIA-41 Cellular Radiotelecommunication Intersystem Operations network evolution to 3G and global specifications for the radio transmission technologies (RTTs) supported by ANSI/TIA/EIA-41.<br><br>http://www.3gpp2.org |
| ATIS<br><br>(Alliance for Telecommunications Industry Solutions) | Is a U.S.-based organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach.<br><br>http://www.atis.org |
| ATIS – WTSC<br><br>Wireless Technologies & Systems Committee, formerly T1P1 | Develops and recommends standards and technical reports related to wireless and/or mobile services and systems, including service descriptions and wireless technologies. WTSC develops and recommends positions on related subjects under consideration in other North American, regional and international standards bodies.<br><br>http://www.atis.org/0160/index.asp |


--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2006 – All rights reserved
Not for Resale

**Table A.1 — Standardization and promotion activities on enterprise mobility** (*continued*)

| | |
|---|---|
| Ecma International | Is an industry association founded in 1961, dedicated to the standardization of information and communication systems.<br><br>http://www.ecma-international.org/ |
| Ecma TC32<br><br>Communications, networks and systems interconnection | Maintains an overall view and strategy for standardization in the field of private/ corporate telecommunications, and to prepare Ecma Standards and Technical Reports required in this field. TC32 is the home of this Technical Report.<br><br>http://www.ecma-international.org/memento/TC32.htm |
| ETSI<br><br>European Telecommunications Standards Institute | Is an independent, non-profit organization, whose mission is to produce telecommunications standards.<br><br>http://www.etsi.org/ |
| ETSI TC AT<br><br>Access Terminals | Is the "home" for terminal matters within ETSI, established on the basis of the global market sector of telecommunications terminals and residential networks and gateways.<br><br>http://portal.etsi.org/portal_common/home.asp?tbkey1=AT |
| ETSI TC BRAN<br><br>Broadband Radio Access Networks | Prepares standards for equipment providing broadband (25 Mbit/s or more) wireless access to wire-based networks in both private and public environments, operating in either licensed and license exempt spectrum. These systems address both business and residential applications.<br><br>http://portal.etsi.org/portal_common/home.asp?tbkey1=BRAN |
| ETSI TC HF<br><br>Human factors | Is the technical body within ETSI responsible for Human Factors issues in all areas of Information and Communications Technology (ICT). It produces standards, guidelines and reports that set the criteria necessary to build optimum usability into the emerging digital networked economy (DNE).<br><br>http://portal.etsi.org/portal_common/home.asp?tbkey1=HF |
| ETSI TC TISPAN<br><br>Telecoms & Internet converged Services & Protocols for Advanced Networks | Is responsible for all aspects of standardisation for present and future converged networks including the NGN (Next Generation Network) and including, service aspects, architectural aspects, protocol aspects, QoS studies, security related studies, mobility aspects within fixed networks, using existing and emerging technologies.<br><br>http://portal.etsi.org/portal_common/home.asp?tbkey1=TISPAN |

--`,,```,,,,````-`-,,`,,`,`,,`---

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

**Table A.1 — Standardization and promotion activities on enterprise mobility** (*continued*)

| | |
|---|---|
| FMCA<br><br>Fixed-Mobile Convergence Alliance | Is a global alliance of telecom operators whose objective is to accelerate the development of Fixed-Mobile Convergence products and services. With a rapidly growing membership base of leading Operators from around the world, and representing a customer base of approximately 500 million customers who stand to benefit from the development of Convergence services, the FMCA is playing a critical role in driving the availability of Convergence handsets and adoption of Convergence technologies.<br><br>http://www.thefmca.com/ |
| GSMA<br><br>GSM Association | Is the global trade association that exists to promote, protect and enhance the interests of GSM mobile operators throughout the world. The GSMA aims to accelerate the implementation of collectively identified, commercially prioritised operator requirements and to take leadership in representing the global GSM mobile operator community with one voice on a wide variety of issues nationally, regionally and globally.<br><br>http://www.gsmworld.com |
| IEEE 802 | Develops Local Area Network and Metropolitan Area Network standards and provides a complete set of standards for carrying IP. Standards define only the Physical and Link Layer of a network and the corresponding management procedures and services.<br><br>http://grouper.ieee.org/groups/802/ |
| IEEE 802.1 | Higher Layer LAN Protocols Working Group<br><br>802.1X Authentication.<br><br>http://grouper.ieee.org/groups/802/1/ |
| IEEE 802.3 | Ethernet Working Group.<br><br>http://grouper.ieee.org/groups/802/3/ |
| IEEE 802.11 | Wireless LAN Working Groups<br>802.11a 54Mbit/s using the 5.4 GHz band<br>802.11b 11Mbit/s using the 2.4 GHz band<br>802.11e Quality of Service<br>802.11g 54Mbit/s using the 2.4 GHz band<br>802.11i Security WPA2 and AES<br>802.11k Radio Measurement<br>802.11n Emerging standard for providing 100 Mbit/s<br>802.11r Fast roaming<br>802.11u Interworking with external networks.<br><br>http://grouper.ieee.org/groups/802/11/ |
| IEEE 802.16 | Broadband Wireless Access Working Group<br>802.16a portable service<br>802.16e mobile service<br><br>http://grouper.ieee.org/groups/802/16/ |


© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

**Table A.1 — Standardization and promotion activities on enterprise mobility** (*continued*)

| | |
|---|---|
| IEEE 802.20 | Mobile Broadband Wireless Access (MBWA) Working Group.<br><br>http://grouper.ieee.org/groups/802/20/ |
| IEEE 802.21 | Media Independent Handoff Working Group.<br><br>http://grouper.ieee.org/groups/802/21/ |
| IETF<br><br>Internet Engineering Task Force | Is an open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. Main focus of the IETF are the Internet protocols.<br><br>www.ietf.org |
| IETF CAPWAP Working Group<br><br>Control and Provisioning of Wireless Access Points | Goal is to facilitate control, management and provisioning of WLAN Termination Points (WTPs) specifying the services, functions and resources relating to 802.11 WLAN Termination Points in order to allow for interoperable implementations of WTPs and Access Controllers.<br><br>http://www.ietf.org/html.charters/capwap-charter.html |
| IETF GEOPRIV Working Group<br><br>Geographic Location/ Privacy | Primary task is to assess the authorization, integrity and privacy requirements that must be met in order to transfer geographic location information, or authorize the release or representation of such information through an agent.<br><br>http://www.ietf.org/html.charters/geopriv-charter.html |
| IETF HIP Working Group<br><br>Host Identity Protocol | Provides a method of separating the end-point identifier and locator roles of IP addresses. It introduces a new Host Identity (HI) name space, based on public keys. The public keys are typically, but not necessarily, self generated.<br><br>http://www.ietf.org/html.charters/hip-charter.html |
| IETF MANET Working Group<br><br>Mobile Ad-hoc Networks | Standardizes IP routing protocol functionality suitable for wireless routing application within both static and dynamic topologies with increased dynamics due to node motion or other factors.<br><br>http://www.ietf.org/html.charters/manet-charter.html |
| IETF MIP4 Working Group<br><br>Mobility for IPv4 | Works on IP mobility support for IPv4 nodes (hosts and routers), which allows a node to continue using its "permanent" home address as it moves around the internet. The Mobile IP protocols support transparency above the IP layer, including maintenance of active TCP connections and UDP port bindings.<br><br>http://www.ietf.org/html.charters/mip4-charter.html |

© ISO/IEC 2006 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

**Table A.1 — Standardization and promotion activities on enterprise mobility** (*continued*)

| | |
|---|---|
| IETF MIP6 Working Group<br><br>Mobility for IPv6 | Specifies routing support to permit an IPv6 host to continue using its "permanent" home address as it moves around the Internet. Mobile IPv6 supports transparency above the IP layer, including maintenance of active TCP connections and UDP port bindings.<br><br>http://www.ietf.org/html.charters/mip6-charter.html |
| IETF MIPSHOP Working Group<br><br>MIPv6 Signalling and Handoff Optimization | Specifies routing support to permit IP hosts using IPv6 to move between IP subnetworks while maintaining session continuity. Mobile IPv6 supports transparency above the IP layer, including maintenance of active TCP connections and UDP port bindings.<br><br>http://www.ietf.org/html.charters/mipshop-charter.html |
| IETF MOBIKE Working Group<br><br>IKEv2 Mobility and Multihoming | Works on extensions to the IKEv2 protocol required to enable its use in the context where there are multiple IP addresses per host (multihoming, SCTP) or where the IP addresses changes in the control of the IPsec host (mobility and roaming). The main scenario is making it possible for a VPN user to move from one address to another without re-establishing all security associations, or to use multiple interfaces simultaneously, such as where WLAN and GPRS are used simultaneously.<br><br>http://www.ietf.org/html.charters/mobike-charter.html |
| IETF NEMO Working Group<br><br>Network Mobility | Is concerned with managing the mobility of an entire network, which changes, as a unit, its point of attachment to the Internet and thus its reachability in the topology.<br><br>http://www.ietf.org/html.charters/nemo-charter.html |
| IETF SIMPLE Working Group<br><br>SIP for Instant Messaging and Presence Leveraging Extensions | Focuses on the application of the Session Initiation Protocol (SIP, RFC 3261) to the suite of services collectively known as instant messaging and presence (IMP).<br><br>http://www.ietf.org/html.charters/simple-charter.html |
| IETF SIP Working Group<br><br>Session Initiation Protocol | Is chartered to continue the development of the Session Initiation Protocol (SIP).<br><br>http://www.ietf.org/html.charters/sip-charter.html |
| IETF SIPPING Working Group<br><br>Session Initiation Proposal Investigation | Is chartered to document the use of SIP for several applications related to telephony and multimedia, and to develop requirements for any extensions to SIP needed for those applications.<br><br>http://www.ietf.org/html.charters/sipping-charter.html |
| IPDR.org | Is an open consortium of leading service providers, equipment vendors, system integrators, and billing and mediation vendors collaborating to facilitate the exchange of usage and control data between network and hosting elements and operations and business support systems by deployment of IPDR standards.<br><br>http://www.ipdr.org/about/index.html |

--`,,```,,,,````-`-`,,`,,`,`,,`---



Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2006 – All rights reserved
Not for Resale

**Table A.1 — Standardization and promotion activities on enterprise mobility** (*continued*)

| | |
|---|---|
| IRAP<br><br>International Roaming Access Protocols | To encourage improved customer experience, a group of key technology companies are working together to promote the adoption of International Roaming Access Protocols (IRAP). The IRAP technology package includes best-known methods, technical documentation and blueprints, and business connections that support establishing safer, simpler, seamless connectivity at PWLAN hotspots.<br><br>http://www.goirap.org/ |
| IRTF<br><br>Internet Research Task Force | To promote research of importance to the evolution of the future Internet by creating focused, long-term and small Research Groups working on topics related to Internet protocols, applications, architecture and technology.<br><br>http://www.irtf.org/ |
| IRTF MOPOPTS Working Group<br><br>IP Mobility Optimizations | Works on Mobile IP Route optimizations and improvements of handover performance and security.<br><br>http://www.irtf.org/charter?gtype=rg&group=mobopts |
| ITU-T<br><br>International Telecommunication Union - Telecommunication Standardization Sector | Mission is to ensure an efficient and on-time production of high quality standards (Recommendations) covering all fields of telecommunications.<br><br>http://www.itu.int/ITU-T/ |
| ITU-T SG11<br><br>Signalling requirements and protocols | Is or studies relating to signalling requirements and protocols for Internet protocol (IP) related functions, some mobility related functions, multimedia functions for networks including convergence toward NGN, and enhancements to existing Recommendations on access and internetwork signalling protocols of BICC, ATM, N-ISDN and PSTN.<br><br>http://www.itu.int/ITU-T/studygroups/com11/index.asp |
| ITU-T SG13<br><br>Next Generation Networks | Is responsible for the architecture, evolution and convergence of next generation networks including frameworks and functional architectures, signalling requirements for NGN, NGN project management coordination across study groups and release planning, implementation scenarios and deployment models, network and service capabilities, interoperability, impact of IPv6, NGN mobility and network convergence and public data network aspects.<br><br>http://www.itu.int/ITU-T/studygroups/com13/index.asp |

© ISO/IEC 2006 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

**Table A.1 — Standardization and promotion activities on enterprise mobility** (*continued*)

| | |
|---|---|
| ITU-T SG16<br><br>Multimedia terminals, systems and applications | Is responsible for studies relating to multimedia service capabilities, and application capabilities (including those supported for NGN). This encompasses multimedia terminals, systems (e.g., network signal processing equipment, multipoint conference units, gateways, gatekeepers, modems, and facsimile), protocols and signal processing (media coding).<br><br>http://www.itu.int/ITU-T/studygroups/com16/area.html |
| ITU-T SG 19<br><br>Mobile telecommunication networks | Is responsible for network aspects of mobile telecommunications networks, including International Mobile Telecommunications 2000 (IMT-2000) and beyond, wireless Internet, convergence of mobile and fixed networks, mobility management, mobile multimedia functions, internetworking, interoperability and enhancements to existing ITU-T Recommendations on IMT-2000.<br><br>http://www.itu.int/ITU-T/studygroups/com19/area.html |
| ITU-T FGNGN<br><br>Focus Group on Next Generation Networks | Is addressing the emerging needs for global standards for Next Generation Networks.<br><br>http://www.itu.int/ITU-T/ngn/fgngn/index.html |
| Jericho Forum | Aims to drive and influence development of security solutions, based on open standards, that will meet future business needs for secure interoperation of information systems to support collaboration and commerce over open networks, within and between organisations, based on a security architecture and design approach which the Forum calls de-perimeterisation.<br><br>http://www.opengroup.org/jericho/ |
| LAP<br><br>Liberty Alliance Project | Is an industry consortium with the mission to establish an open standard for federated network identity through open technical specifications.<br><br>http://www.projectliberty.org/ |
| MEA<br><br>Mobile Enterprise Alliance | Is a global advocacy group promoting the business benefits of workforce mobility to enterprise end users and decision makers.<br><br>http://www.mobileenterprise.org |
| OASIS<br><br>Organization for the Advancement of Structured Information Standards | Is a not-for-profit, global consortium that drives the development, convergence and adoption of e-business standards. Members themselves set the OASIS technical agenda, using a lightweight, open process expressly designed to promote industry consensus and unite disparate efforts. OASIS produces worldwide standards for security, Web Services, XML conformance, business transactions, electronic publishing, topic maps and interoperability within and between marketplaces.<br><br>http://www.oasis-open.org |


--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale
© ISO/IEC 2006 – All rights reserved

**Table A.1 — Standardization and promotion activities on enterprise mobility** (*continued*)

| | |
|---|---|
| OMA<br><br>Open Mobile Alliance | Is an industry alliance of mobile operators, wireless vendors, IT vendors and service/content-providers committed to create open mobile software and services based on global standards. Consequently one of OMA's working groups is focused on enabling Web Services in mobile environments.<br><br>http://www.openmobilealliance.org/ |
| OSGi™ Alliance – MEG<br><br>Mobile Expert Group | Is chartered to define the requirements and specifications to tailor and extend the OSGi Service Platform for mobile devices that are data-capable, and also capable of connecting to wireless networks. Examples of such devices include, but are not limited to, digital mobile phones, smartphones, Personal Digital Assistants (PDAs), etc. Development of the specifications and APIs entails the creation of supporting documentation, reference implementations and compatibility test suites. Technical areas addressed by the MEG will include the requirements, functional specifications, data formats, and communication protocols for the mobile Service Platform as well as defining new requirements for the base service platform.<br><br>http://www.osgi.org/about/charter_meg.asp |
| PARLAY Group | Is a multi-vendor consortium formed to develop open, technology-independent application programming interfaces (APIs) that enable the development of applications that operate across multiple, networking-platform environments. Parlay integrates telecom network services with IT applications via a secure, measured, and billable interface.<br><br>http://www.parlay.org |
| SCCAN Forum<br><br>Seamless Converged Communication Across Networks Forum | Will promote seamless mobility on a global basis through the development of open specifications for interoperation between dual-network handsets, Wi-Fi infrastructure, IP-PBXs across WLAN and cellular networks. Technical work in the SCCAN Forum will be complementary to -- and will leverage the existing work of -- related organizations such as WiFi Alliance and IEEE. The Forum will also drive interoperability certification related to its specifications.<br><br>http://www.sccan.org/ |
| SIP Forum | Is an industry organization with members from the leading SIP technology companies. Its mission is to advance the adoption of products and services based on SIP.<br><br>http://www.sipforum.org/ |
| TCG<br><br>Trusted Computing Group | Develops and promotes open specifications. Computing industry vendors use these specifications in products that protect and strengthen the computing platform against software-based attacks. In contrast, traditional security approaches have taken a "moat" approach and are software-based, making them vulnerable to malicious attacks, virtual or physical theft, and loss.<br><br>http://www.trustedcomputinggroup.org |

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2006 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

**Table A.1 — Standardization and promotion activities on enterprise mobility** (*continued*)

| | |
|---|---|
| UMA<br><br>Unlicensed Mobile Access | Is a set of open specifications, which a number of leading companies within the wireless industry have jointly developed. UMA technology provides access to GSM and GPRS mobile services over unlicensed spectrum technologies, including Bluetooth and 802.11. By deploying UMA technology, service providers can enable subscribers to roam and handover between cellular networks and public and private unlicensed wireless networks using dual-mode mobile handsets. With UMA, subscribers receive a consistent user experience for their mobile voice and data services as they transition between networks.<br><br>www.umatechnology.org |
| VoipSA<br><br>Voice over IP Security Alliance | Mission is to promote the current state of VoIP security research, VoIP security education and awareness, and free VoIP testing methodologies and tools.<br><br>http://www.voipsa.com/ |
| W3C<br><br>World Wide Web Consortium | Is a membership organization developing interoperable web technologies (specifications, guidelines, software and tools).<br><br>http://www.w3.org |
| W3C – MWI<br><br>Mobile Web Initiative | Is focussing on developing "best practices" and a trustmark for Web sites (working name: "mobileOK"), work on device information needed for content adaptation, and marketing and outreach activities. The work is organized in two working groups: The mission of the Mobile Web Best Practice (MWBP) Working Group is to develop a set of technical best practices and associated materials in support of development of Web sites that provide an appropriate user experience on mobile devices. The mission of the MWI Device Description Working Group (DDWG) is to enable the development of globally accessible, sustainable data and services that provide device descriptions in support of Web-enabled applications having an appropriate user experience on mobile devices.<br><br>http://www.w3.org/2005/MWI/ |
| WFA<br><br>Wi-Fi Alliance | Is a global, non-profit industry association of more than 200 member companies devoted to promoting the growth of wireless Local Area Networks (WLANs). With the aim of enhancing the user experience for mobile wireless devices, the Wi-Fi Alliance's testing and certification programs ensure the interoperability of WLAN products based on the IEEE 802.11 specification.<br><br>http://www.wi-fi.org |
| WiMAX Forum | Is working to facilitate the deployment of broadband wireless networks based on the IEEE 802.16 standard by helping to ensure the compatibility and inter-operability of broadband wireless access equipment. The organization is a nonprofit association formed in June of 2001 by equipment and component suppliers to promote the adoption of IEEE 802.16 compliant equipment by operators of broadband wireless access systems.<br><br>http://www.wimaxforum.org |


Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2006 – All rights reserved
Not for Resale

**Table A.1 — Standardization and promotion activities on enterprise mobility** (*continued*)

| | |
|---|---|
| WIMA<br><br>WI-Mesh Alliance | Is a group of companies with a common view towards rapidly achieving a complete and robust WLAN Mesh standard.<br>The Wi-Mesh proposal provides the specification for a scalable, adaptive and secure WLAN mesh standard. It offers the flexibility required to satisfy all residential, office, campus, public safety and military usage models. The proposal focuses on multiple dimensions: the MAC sublayer, the routing, the security and high layer interworking.<br><br>http://www.wi-mesh.org |
| ZigBee Alliance | Is an association of companies working together to enable reliable, cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard.<br><br>www.zigbee.org |

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

**ICS 35.110**

Price based on 53 pages

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale