TECHNICAL REPORT

ISO/IEC TR 26927

Second edition
2011-09-01

Information technology — Telecommunications and information exchange between systems — Corporate telecommunication networks — Mobility for enterprise communications

Technologies de l'information — Téléinformatique — Réseaux de télécommunication d'entreprise — Mobilité pour les communications d'entreprise

Reference number
ISO/IEC TR 26927:2011(E)

COPYRIGHT PROTECTED DOCUMENT

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

Contents

Page

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, 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), it may decide to publish a Technical Report. A Technical Report is entirely informative in nature and shall be subject to review every five years in the same manner as an International Standard.

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.

This second edition cancels and replaces the first edition (ISO/IEC TR 26927:2006), which has been technically revised, taking into account more recent information and identifying requirements and standardization gaps.

Introduction

This Technical Report identifies key mobility issues for IP-based enterprise communications. It defines terms for different types of mobility, describes basic functionality in support of mobility, and lists common deployment scenarios. For each scenario, it identifies functional requirements and standardization gaps related to the management of mobility, identity, terminals and reachability.

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.

Information technology — Telecommunications and information exchange between systems — Corporate telecommunication networks — Mobility for enterprise communications

1 Scope

Mobility for enterprise communications is the ability for persons and objects (e.g. vehicles, sensors and other machines) belonging to the enterprise to use communication and information services regardless of changes in their physical location. This includes also the ability to be reached by other persons or objects for communications.

This Technical Report encompasses the mobility of enterprise users connecting to enterprise and public IP networks using wired and wireless terminals for voice, data and converged services. It defines terms for different types of mobility, describes basic functionality in support of mobility, and lists common deployment scenarios. For each scenario, it identifies functional requirements and standardization gaps with the main focus on the management of mobility, identity, terminals and reachability. However, it does not provide technical solutions but lays the foundations for triggering standardization projects in areas where gaps have been identified.

More general aspects of enterprise communications based on Next Generation Corporate Networks (NGCN) and interconnection with Next Generation Networks (NGN) are covered by the companion series of Technical Reports on NGCN [1], [2], [3] and [4].

2 Normative references

No normative references are cited.

3 Terms and definitions

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

3.1
access network
network entity that provides 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
authentication
proof that an identity is genuine, e.g. the user is as claimed

3.4
authorization
process or result of assigning certain execution rights or a role to an authenticated user or entity

3.5
availability
property of being accessible and usable upon demand by an authorized entity

3.6
core network
portion of a communication system composed of networks, system equipment and infrastructures providing services and connections between access networks, service provider networks and other networks

3.7
corporate network
telecommunication network serving a corporation

NOTE 1 A corporation is a single organization, an extended enterprise, or an industry application group as defined by the International Chamber of Commerce (ICC).

NOTE 2 Sets of equipment [Customer Premises Equipment (CPE) and/or Customer Premises Networks (CPN)] are typically located at geographically dispersed locations and are interconnected to provide networking services to a defined group of users. A corporate network can employ connection-oriented and connectionless technology.

3.8
domain
collection of physical or functional network entities belonging to a restricted geographical area, a topological IP area or owned/administered by an enterprise, a public carrier or a service provider

3.9
enterprise network
corporate network comprising session layer capabilities and optionally application layer capabilities hosted on one or more infrastructures

NOTE Infrastructures can include the enterprise's own infrastructure (dedicated NGCN), the infrastructure of one or more hosting NGNs, the infrastructure of one or more hosting NGCNs or any combination of these.

3.10
end-to-end security
security (including privacy and information integrity) for the exchange of information between two or more end points that relies on protocols and mechanisms that are implemented exclusively on those endpoints

3.11
enterprise-grade service
performance level for security, availability and service perception that is comparable to PBX-based services

3.12
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

3.13
fixed-line network
WAN or MAN provided by a fixed-line operator (e.g. enterprise) which provides in general wired access, which may be extended locally by wireless access networks (DECT, WLAN, etc.)

3.14
foreign domain
administrative domain of a visited network

3.15
handover
handoff
process of transferring an ongoing network association of a mobile terminal/user from one point of attachment to another in case of crossing a cell or network boundary

3.16
home domain
domain that administers the account of a mobile user/terminal

3.17
home network
network that is in a mobility architecture the central source for mobility services to the mobile user/terminal and which interacts with the visited network

3.18
hotspot
wireless access point to the public internet based on WLAN technology

3.19
identity
name by which the user of a network is known

3.20
internet
public IP network

3.21
intranet
closed IP network of an enterprise used for data or converged communication services by members of the enterprise

3.22
IP network
public or private network offering connectionless packet-mode services based on the Internet Protocol (IP) as the network layer protocol

3.23
IP-PBX
PBX capable of IP-based communications between users

3.24
location
information identifying the network point of attachment (PoA) through which a user/terminal is currently accessing a network or the user's terminal's geographical position

3.25
mobile network
wireless WAN or MAN that provides continuous connectivity to mobile terminals

3.26
mobile terminal
device which is able to access the enterprise network from different locations

3.27
mobile user
user who accesses ICT resources of the enterprise from different locations

3.28
multihoming
〈property of a device〉 able to use more than one IP address at any given point of time

3.29
moving network
LAN or WLAN that is installed in a moving vehicle, e.g. train, and connected to a mobile network

3.30
Next Generation Network
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

3.31
Next Generation Corporate Network
self-contained corporate network designed to take advantage of emerging IP-based communications solutions and that can have its own applications and service provisioning

NOTE A Next Generation Corporate Network can be an entire enterprise network if none of that network is based on public network infrastructure.

3.32
portal
web-based interface that provides a single access point to dispersed information

EXAMPLE Corporate portals provide enterprise-wide information to employees.

3.33
presence
set of data representing the status and availability of a person/object or a group of persons/objects for communication

3.34
privacy
right of individuals to control or influence what information related to them may be collected and stored and by whom that information may be disclosed

3.35
private cloud
server farm for a closed user group

3.36
profile
total set of user- or terminal-related information, preferences, rules and settings

EXAMPLE Access rights.

3.37
quality of service
level of performance for the transport of data

3.38
roaming
service that enables users/terminals to use access networks and mobility services of a network operator which is different from the operator of the user's home domain

3.39
session
temporary interactive information interchange between two or more nodes in a network architecture

3.40
single sign-on
access control mechanism where a user logs on once and gains access to a number of applications and services without being prompted to log in again at each of them

3.41
terminal
device enabling users to access services via an access network

3.42
transit network
network that provides interconnection between networks

3.43
user
person, organization or technical object that accesses a network in order to communicate using the services provided by that network

3.44
Virtual Private Cloud
private cloud provided by a third party service provider

3.45
Virtual Private Network
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

3.46
visited network
network that interacts with the home network to provide mobility services to the mobile enterprise user/terminal at PoAs in a foreign network

4 Abbreviations

AAA	Authentication, Authorization and Accounting
AN	Access Network
AP	Access Point (WLAN)
API	Application Program Interface
ASA	Access Service Authorizer
ASP	Access Service Provider
CN	Correspondent Node
CoA	Care of Address
CPE	Customer Premises Network
CRM	Customer Relation Management
DECT	Digital Enhanced Cordless Telecommunications
DHCP	Dynamic Host Configuration Protocol
DM	Device Management
DSL	Digital Subscriber Line
ERP	Enterprise Resource Planning
FA	Foreign Agent
GSM	Global System for Mobile communication

HA	Home Agent
HIP	Host Identity Protocol
HO	HandOver
IAM	Identity and Access Management
ICA	Independent Computing Architecture
ICT	Information Communication Technology
IM	Instant Messaging
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISP	IP-Service Provider
IVR	Interactive Voice Response
LAN	Local Area Network
LTE	Long Term Evolution
MAC Address	Media Access Control Address
MIP	Mobile IP
MN	Mobile Node
MM	Mobility Management
MSA	Mobility Service Authorizer
MSP	Mobility Service Provider
NAT	Network Address Translator
NGCN	Next Generation Corporate Network
NGN	Next Generation Network
NIC	Network Interface Card
OAM	Operation, Administration and Maintenance
OSI	Open Systems Interconnection reference model
PAN	Personal Area Network
PBX	Private Branch Exchange
PKI	Public Key Infrastructure
PoA	Point of Attachment
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RDP	Remote Display Protocol
RFC	Request For Comment
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMB	Small Medium Business
SOA	Service Oriented Architecture
SOHO	Small Office Home Office
SSL	Secure Socket Layer protocol
SSO	Single Sign-On

TCP	Transmission Control Protocol
UMTS	Universal Mobile Telecommunications System of 3GPP
VDI	Virtual Desktop Infrastructure
VM	Virtual Machine
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WIMAX	Worldwide Interoperability for Microwave Access (IEEE 802.16)
WLAN	Wireless LAN
WMAN	Wireless Metropolitan Area Network

5 Background

Globalization of the economy and the need for more responsive business processes (also referred to as the 'Real Time Enterprise') have created new demands on enterprise networks and data centers. Progress in digital technology is transforming corporate networks and will ultimately transform the way companies provide and use communications and information technology (ICT) 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:

- integration of the enterprise's communication services with its business processes to enhance workflows;
- increase of hosted ICT services offered by ISPs or public carriers for non-core enterprise tasks;
- demand for access to ICT resources from everywhere, meaning mobility;
- fast growing variety in types and applications of ICT.

For the support of mobility, the architecture of the enterprise ICT infrastructure must support access by the mobile workforce. The architecture therefore has to provide interfaces to the basic functions of the data center, e.g. ERP and work flows, for a diversity of mobile/ portable terminals. In addition interfaces are needed to enable the provision of services, for exchange of data and communications in a managed and secure way.

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, at an industrial plant, 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 [1]) are extending their reach to provide mobility with wireless or wired technology, e.g. high-bandwidth wireless hotspots, digital cellular or DSL 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), machine-to-person (e.g. broadcast or alarms) and machine-to-machine communications (e.g. automatic software updates of terminals).

Examples for mobility applications in enterprise communications are:

- Public transport, logistics:
  - voice over WLAN and mobile data for personnel, e.g. at loading docks;
  - access to enterprise resources during travel.

- Hospitals:
- communications services and database access to patients;
  - patient personal communications;
  - monitoring patients;
  - data-interchange with ambulance;
  - 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:
  - machine-to-machine communication;
  - many “mobile“ people (many meetings, projects, various large buildings…);
  - mobile access to data, e.g. for service personnel;
  - remote and distributed inventory management.

Figure 1 depicts an example of an enterprise network environment for mobility using enterprise (solid lines) and public network (dotted lines) connections.

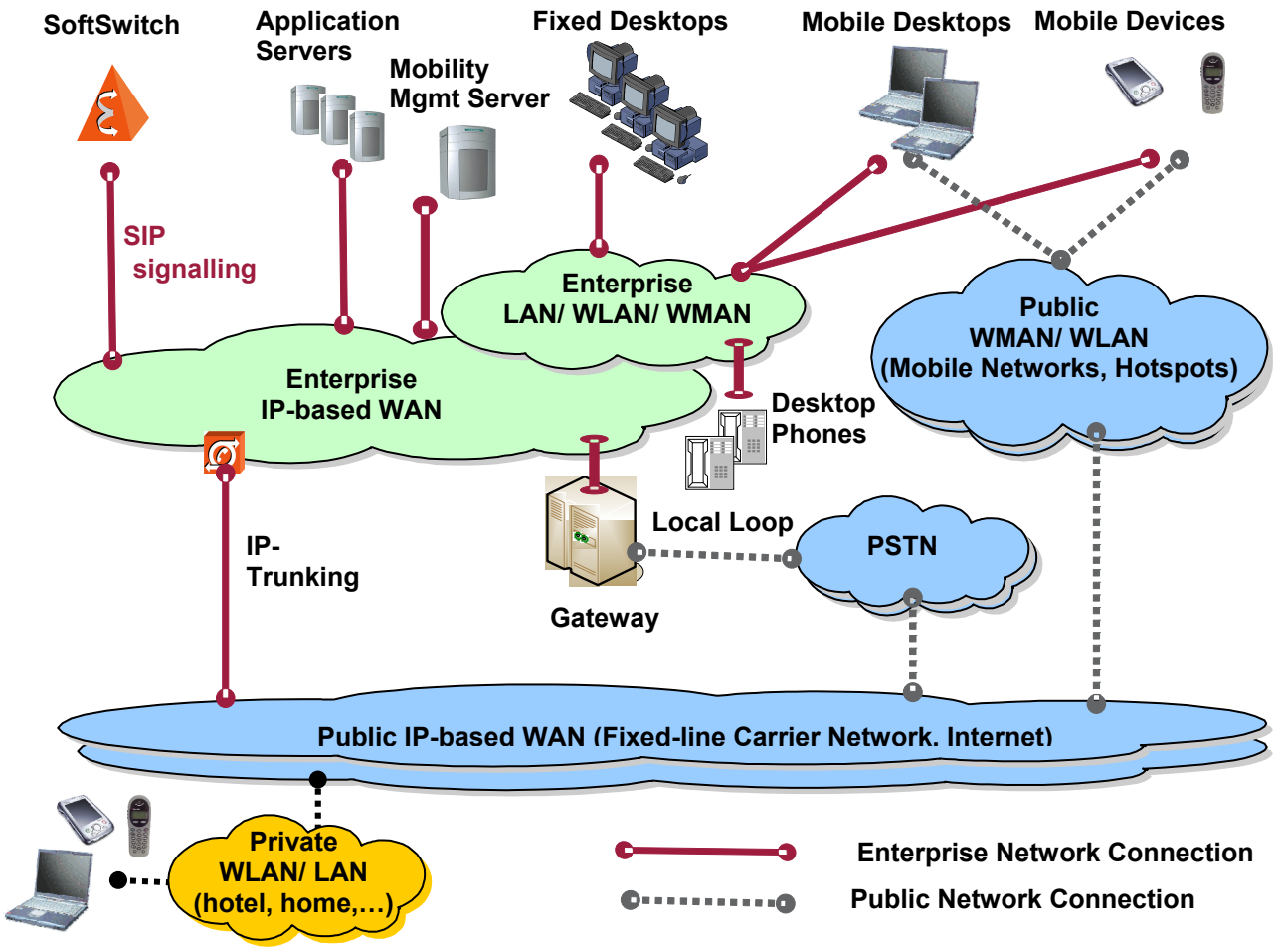

Figure 1 — Enterprise network environment for mobility

As shown in Figure 1, mobility for enterprise communication is supported not only by the corporate LAN/WAN but also by the emerging IP-based public mobile and fixed networks, including the Internet. Of high importance for mobility are WLAN islands (hotspots) that provide broadband data access and voice telephony (VoWLAN), either on the enterprise campus or in public areas, Other promising technologies for enterprise mobility are WIMAX, moving networks, self-organizing mobile networks (e.g. adhoc and meshed networks) and personal networks [5]. However, these technologies are out of scope of this report.

As ICT has become an integral part of business processes the provision of mobility may introduce serious risks to business continuity, due to the opening of the ICT network infrastructure to foreign network domains. In addition, the emergence of new mobile platforms (e.g. smart phones, netbooks) and the rapid growth of mobile applications have triggered the infiltration of personal devices into the workplace. Therefore enterprise ICT departments are challenged to exploit changed mobility technology and user behaviour for the benefit of business processes without threatening the security of enterprise data and infrastructure

For economic reasons the enterprise information and communication infrastructure has to rely on the same technologies and standards as used for the public infrastructure, however the selection of components and their standardization should take into account the special needs of enterprises. Clause 8 ‘Requirements and Standardization Gaps’ elaborates this in more detail.

6 Mobility types and terms

Mobility provided by an enterprise information and communication system comes in various forms and with various limitations. A large number of terms have been introduced to describe different types of mobility, often with different terms used for the same thing or with the same term used for different things. This Clause describes mobility types and their extensions as they are used in this Technical Report.

6.1 Mobility types

The key elements for providing mobility in an information and communication system are:

- terminal connectivity;
- user access;
- persistence of communication sessions;
- service availability.

The corresponding mobility types are introduced below. Their provision depends on the capabilities of the involved access and core networks and also on the hardware and software of the terminal.

NOTE Depending on the deployment, two or more mobility types may be used in combination. Clause 8 evaluates this for a set of deployment scenarios.

6.1.1 Terminal mobility

Terminal mobility denotes the ability of a terminal to have transparent network connectivity (OSI layers 1 - 4) even after it has moved between different network Points of Attachment (PoA).

In the case of an enterprise network, terminal mobility is typically provided to certified devices (e.g. laptops, PDAs, smart-phones, SIP-phones) which are in most cases identified by a unique hardware identifier, e.g. by the MAC address of the network interface card. In public mobile networks the terminal is usually identified by the IMEI of the terminal.

NOTE Terminal mobility is also known as device mobility.

6.1.2 User mobility

User mobility denotes the ability of a user to access information and services with a single identity even after moving between different PoAs, either as a result of his/her terminal moving or as a result of change of terminal In addition, user mobility can include the possibility of accessing services from several terminals simultaneously.

An important requirement for user mobility is that the user registers with his home network (and in some cases with the visited network, too) by supplying suitable means for identification and authentication, 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 token (e.g., smart card, SIM, USIM, USB-stick etc.) or soft key store. The involved networks have to provide appropriate means for identity and access management.

NOTE User mobility is also known as personal mobility.

6.1.3 Session mobility

Session mobility denotes the ability of a network or networks and the involved terminals to maintain active communication sessions, regardless of whether the terminal has moved to a different network PoA or the user has switched to another terminal. Session mobility comes always in conjunction with terminal and/or user mobility

6.1.4 Service mobility

Service mobility is the capability of the network(s) concerned to provide to the user/ terminal transparent support for subscribed and personalized services regardless of whether the terminal has moved to a different network PoA or the user has switched to another terminal Such services are usually contracted by SLAs or roaming agreements between the operators of the involved network access domains and the enterprise ICT administration.

Examples are:

- ability to use the same dial plan for establishing outgoing communications as in the enterprise network;
- support of using call control services provided by the enterprise PBX;
- ability to receive caller identification information from enterprise directories.

Similar to session mobility, service mobility comes in conjunction with terminal and/or user mobility.

6.2 Mobility across different network infrastructures

Each of the mobility types described in 6.1 can be extended by attributes describing their ability to operate across different access technologies, or different administrative network domains or both.

6.2.1 Mobility across access network technologies

To extend the description of terminal mobility the following terms are used. All other mobility types are not affected, as they are agnostic to the access network technology.

- *Intra-technology mobility*:
  supports terminal mobility within or across networks using the same access network technology.

NOTE Intra-technology mobility is also known as horizontal mobility.

- *Inter-technology mobility:*
  supports terminal mobility within or across networks using different access network technologies. Examples are transitions from LAN to WLAN, WMAN to WLAN. or DECT to GSM.

NOTE Inter-technology mobility is also known as vertical mobility.

6.2.2 Mobility across administrative network domains

The following attributes extend terminal, user, session and service mobility according to their ability to operate across different administrative domains.

- *Intra-domain mobility:*
  denotes the support of a mobility type inside a single administrative domain.

NOTE Intra-domain mobility is also known as micro-mobility.

- *Inter-domain mobility:*
  denotes the support of a mobility type across networks of different administrative domains, e.g. across administrative subnetworks of an enterprise network or across public and enterprise network domains. In some cases inter-domain mobility is provided on the basis of a roaming contract between the provider of the home domain of the terminal/ user and the provider of the foreign domain.

NOTE Inter-domain mobility is also known as macro-mobility.

6.3 Mobility modes

A further extension to describe the capabilities of mobility types is the distinction between the way mobility can be provided by the network or how the terminal/user makes use of it.

The following terms have been introduced:

- Nomadic mode;
- Portable mode;
- Mobile mode.

6.3.1 Nomadic mode

Nomadic mode refers to the provision/ use of mobility types just at distinct PoAs. Terminal, user and service mobility, require connection set up and terminal/ user registration each time the PoA and/or the terminal has changed. There is no support for session mobility. A typical example for nomadic use is mobility provided by a wired network, e.g. LAN.

6.3.2 Portable mode

Portable mode refers to the provision/ use of mobility similar to nomadic mode but with support of session mobility. This enables a terminal/ user to suspend all active sessions and resume them at a new PoA or on a different terminal.

6.3.3 Mobile mode

Mobile mode denotes the ability of the involved networks to provide continuous service to a mobile terminal/ user with virtually no interruption while moving. This requires the involved network(s) to be capable of identifying and tracking the terminal. In cases where delays or loss of data are not perceived by the involved parties as degradation of quality of service, the mobility involved is called seamless. Mobile mode is typically provided by wireless cellular networks, e.g. WMANs.

7 Basic functionalities to enable mobility

Mobility in enterprise communications is addressed not only by enterprise networks but also by carrier networks and by 3rd party service providers. Due to different business models architectures are usually different. While carriers are betting on IMS technology [27] in their core networks, enterprises are installing solutions which are seamlessly integrated in their ICT infrastructure. However with emergence of the use of IP in public and enterprise networks a large set of standardized IP based technology forms the common denominator for these solutions. This facilitates significantly the interworking of public and enterprise networks, which is a must for the provision of ubiquitous enterprise mobility, as e single network can only offer restricted coverage. The goal for enterprise solutions is the offering of centrally managed system with global access.

The central element for the provision of mobility types as described in Clause 6 is mobility management. It addresses among others handover of network connections and the continuity of IP sessions when the terminal/user is changing access. In addition to mobility management, an enterprise-grade mobility solution has to provide additional management functions to fit into the ITC infrastructure of the enterprise. These are:

- **Device management and policy enforcement,** which addresses security and reliability of the user terminal to maintain compliance with enterprise policies.

- **Identity and access management** which addresses the security constraints beyond connection/transport security including protection and proper use of business information and services. In addition it forms the basis for charging.

- **Location management**, which addresses the ability of the system to determine the location of the PoA of a mobile terminal/ user either in terms of geographical data or as a network address in the access network.

- **Reachability management,** which provides information to other users how to reach a mobile user for communication and supports access to reachability information of other users. This functionality is also known as presence service.

Other management functions, which are not covered in this report, are:

- **Service management**, which addresses monitoring, reporting and troubleshooting of connection, performance (QoS), SLA compliance and terminal issues.

- **Expense management**, which measures and logs the costs of mobility service utilization.

In the delivery of mobility services, including the above mentioned management functions, several operational entities may lead to complex arrangements. All these entities must trust each other and communicate. In most cases this is implemented by service level agreements (SLA), e.g. roaming agreements. The most relevant entity roles to be taken into account in this report are the following:

- **Access Service Authorizer (ASA):** a (virtual) network operator that authenticates a mobile terminal/user and establishes authorization to receive services at PoAs of his domain.. Authentication and authorization are managed by AAA servers [6] of the domain and data bases which contain user profiles on access rights and policies.

- **Access Service Provider (ASP**): a (virtual) network operator that provides data connection to the mobile terminal/user. Before establishing a connection access authorization by the respective ASA is needed.

- **Mobility Service Authorizer (MSA):** a (virtual) service provider that authorizes the use of mobility services. The authorization process is managed by AAA servers of the domain and data bases with terminal/user profile and policies.

- **Mobility Service Provider (MSP**): a (virtual) service provider that provides mobility services, for supporting mobility management, i.e. provision of Home Agents in case of the MIP protocol (see 7.2.1.2). Access to such services needs explicit authorization by the respective MSA.

Depending on the deployment of mobility a single entity can perform multiple roles, which impacts the requirements on mobility supporting protocols significantly. In Clause 8 this is analysed for some scenarios.

The following clauses give a brief overview of the technical issues and standardization efforts

7.1 Mobility management

Mobility management (MM) denotes a set of functions to provide connectivity and access independent of location. These functions provide

- handover of connection for various types of applications (reliable/unreliable, real-time/ near real-time/ non real-time);
- continuity of IP sessions in the mobile and portable mode including the communication between the terminal, visited network and the home network for purposes of authentication, authorization, location updating and download of user information;
- IP address assignment and update.

MM takes place in different layers of the OSI network model and may be assisted by non-network sources, providing e.g. location or profile information. The provision of MM across different networks and/or systems may be restricted by:

- access technology;
- network policies;
- missing support of MM functions and protocols;
- iIncompatible 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*:
  addresses MM issues between networks of different operators, which includes location and AAA functionality. Global MM of a enterprise terminal/user is usually a function of the enterprise network, being responsible for its administration, This is referred here as the home network However, for cost reasons the enterprise may outsource this function and parts of it to a 3rd party service provider.
- *Local mobility management:*
  addresses MM issues within a restricted area of a network topology, Local MM can reduce the amount of latency involved in re-establishing the mobile terminal`s network connection during handover, and can reduce the amount of signalling between the mobile terminal and the home network. However this may come with limiting the extent of roaming. The provision of local MM is usually associated with visited access networks.

In the following clauses, the focus is on mobility management functions needed for IP connectivity. Layer 1 and layer 2 support for MM within access networks (e.g. embedded in various standards of the IEEE 802 series and of 3GPP specifications for WLAN and WMAN) are out of scope of this document.

7.1.1 Handover of media connections and sessions

Mobile deployment of terminal and session mobility requires handover (HO). This describes a function used by mobility management that transfers the association of a mobile terminal between networks. In general handover is applied when a user moves through the coverage area of different access networks and crosses administrative domain and/or technology boundaries. . The control of the handover is done by network entities (network executed HO) or by the mobile terminal itself (mobile executed HO). Also hybrid solutions are used,

where the terminal aids HO decisions of the network (mobile assisted HO) and vice versa (network assisted HO). HOs require components in the mobility architecture for discovery of the new network, either by scanning or some information service, e.g. by device management, and the provision of a network selection mechanism, Triggering of HO always follows user requests or policies, which can either be located in the network or are part of the user profile data on the terminal. The required performance of a HO is strongly dependent on the application/ service it is used for. HO of non-real-time data sessions should be lossless but need not be very fast. Whereas HO of VoIP sessions must be fast but may tolerate some data losses. In the ideal case HO of real- time sessions should be seamless, which means impairments caused by the HO process, like buffering/processing delays or packet dropping, are not perceived by the involved parties as a degradation of QoS. According to ITU-T recommendation G.1010 [26] this means for conversational services one way delay time <150 ms and packet loss rate < 3% for voice and <1% for video.

According to the capability of the terminal handover of network connectivity (OSI layer 1 -4) two main handover processes are distinguished:

- Hard handover: refers to a process, where the connection to the current PoA is released and torn down before the new connection can be established. Terminals with just one network interface can only operate in this mode.

- Soft handover refers to a process, where the connection to the previous PoA is retained until the connection to the new PoA is established. This implies that the terminal has two network connections which are used in parallel. In case of inter technology mobility two NICs may be used for this purpose. In case of multihoming, different IP addresses can be assigned to the NIC(s) at the same time. In this case release of the IP-address of interface 1 runs in parallel with the assignment of a new IP-address to interface 2. For seamless mobility of real-time sessions the provision of soft handover is a must.

7.1.1.1 Handover for support of intra-/inter-technology mobility

Handover for the support of intra-/inter-technology mobility are referred as horizontal and vertical handover respectively. Especially vertical handover between ANs using different technologies is a big challenge for MM. As network parameters may differ significantly the MM process must take care for proper buffering to avoid data losses and disturbing the latency of data packets.

Depending on the use case HO mechanisms have to cope with a wide range of requirements. For performance reasons in many cases mobility management is based on a federation of HO mechanisms, which work in different network layers. Especially for wireless ANs layer 2 HO is very specific to the network type, e.g. WLAN (specified in IEEE 802.11 standards) or WMAN (specified in 3GPP/ ETSI standards). IP-based HO support, however, is independent of the underlying network type and can be used in a more flexible way, but may have an adverse impact performance. An overview of suitable mobility management enabling protocols for IP-networks is given in 7.1.2.

To get the best of both approaches IP mobility management protocols can cooperate using the IEEE standard IEEE 802.21 [30], a media independent HO protocol that supports seamless handover between wireless access networks with different wireless technology. It supports network discovery and selection and has some support for optimizing the authentication process.

7.1.1.2 Handover for support of intra-/inter-domain mobility

The main issue with handovers for intra-/inter domain mobility is the exchange of security information between the involved networks. Especially in roaming scenarios, where inter-domain mobility in foreign networks is requested, achieving seamless handovers is critical. Due to the lack of or a weak trust relationship between the enterprise network and the foreign network the authentication and authorization processes get complex and time consuming. Localized mobility management with assistance of special handover protocols, e.g. IEEE 802.21 [30] can help to relax the problem.

7.1.2 Mobility management support for IP-networks

The performance of mobility management is strongly dependent on the mobility service of the underlying signalling and transport protocols of the IP-network. Roughly speaking there are two types of protocols for mobility management in IP networks, according in which OSI layer the management function takes place at:

- network level mobility management;
- application level mobility management.

The pro and cons of these approaches are evaluated below.

7.1.2.1 Network-level mobility management

Protocols for network level mobility manage the provision of mobility types at the network level (OSI layer 3). The most dominant representative is currently Mobile IP (MIPv4/ MIPv6) [8], [11].

Mobile IP defines a home network where the terminal/user is assigned to a fixed IP address and a visited network that the terminal/user visits. It introduces two new entities, the Home Agent (HA) and Foreign Agent (FA), to relay data traffic between the terminal/user (Mobile Node MN) and the other end-point the so-called Correspondent Node (CN). The basic idea of MIP is that although the MN is at a visited network, it is still reachable at the IP address of its home network. Data traffic destinated to the MN arrives at the home network where the HA sends the data via a IP-tunnelling technique to the FA, which removes the IP encapsulation and delivers it to the MN. Data from the MN to a CN can be sent directly by using the FA as the default router. The MN is addressable at the visited network by a Care of Address (CoA), which is assigned to the MN by the visited network (e.g. by a DHCP service). Before starting any communication the MN has to register his current CoA with its HA.

NOTE For the sake of more efficient mobility management a visited network may provide a temporary home network. An example for this is home network emulation in Proxy MIPv6 [20].

One of the merits is making the mobility of a terminal transparent to the application levels (OSI layer 5-7) by keeping the same IP address. However a ubiquitous deployment of MIP is needed in the case of global mobility management. Because an application cannot recognize available bandwidth and delay of the involved networks before or during a handover, it cannot adjust buffers accordingly. As a result it comes with high handover latency, inefficient data traffic and no support for multihoming.

7.1.2.2 Application-level mobility management

Protocols for application level mobility manage mobility at the application level (OSI layer 5-7). The Session Initiation Protocol (SIP) [7] is one of the most prominent representatives. This protocol can support terminal, user and session mobility. It works as follows: The mobile user/terminal registers the IP address which got assigned at his current PoA with the SIP registrar of the access network. The registrar provides anchor functionality and the mapping between the public user identity (SIP address) and the IP address. In case of terminal mobility two modes for handover can be distinguished:

- Pre-call mobility, which requires the terminal/user to register his new IP-address with the registrar server before establishing a new session.

- Mid-call mobility, where the terminal/user re-registers with the registrar server during a session. All end-ponts involved in this session have to be informed on the new IP address for media by re-INVITE messages.

The main advantage of SIP is that it does not require any support from the network level for handover; just IP-connectivity is needed. .According to [41] SIP is not appropriate for supporting mobility of real-time applications since considerable handover latency and overhead may occur.

7.1.2.3 Standardization efforts in mobility management

Beyond the already mentioned MIP and SIP, the IETF has specified other mobility management protocols that are complementary to the widely implemented MIP solution, as well protocols that are disruptive technologies. An example of a disruptive technology is the current work of the IETF 'Network-based Localized Mobility Management (netlmm)' working group. The group is investigating a network-based local mobility management protocol [19] where local IP mobility is handled without involvement from the mobile terminal. This enables the terminal to move across multiple access routers without encountering a change in its IP address, thereby hiding the mobility from the network layer and above.

An example is Proxy Mobile IPv6 (PMIPv6) [20], which has been developed based on Mobile IPv6. With this protocol, unmodified IP nodes may change access routers within a given administrative domain without having to change the IP address.

A more detailed analysis of mobility support in IP-based networks can be found in [41].

7.2 Identity and access management

Security is a continuing concern in mobility services, especially in cases where the PoA is a foreign network. In general, remote access has to address all the security requirements of an enterprise network. Key issues are:

- confidentiality: no unauthorized information leakage or access;
- integrity: no unauthorized data modification;
- non repudiation: performed actions cannot be denied;
- availability: no Denial of Service/ accessibility of services or data;
- privacy: no unauthorized profiling and disclosure;
- authentication and authorization to verify the identity of a terminal/ user and to manage the access rights.

A detailed elaboration on NGCN security issues, including mobility use cases, can be found in [3].

Authentication and authorization play a central role in mobility management and are covered by the identity and access management (IAM) of the mobility architecture. In most cases the corresponding ASA and MSA roles are embedded into the central AAA (Authentication, Authorization, Accounting] system of the access network provider and of the mobility service provider respectively.

The authentication and authorization process has a significant impact on the latency of handovers. Therefore mobility management, IAM processes and handover protocols have to be carefully aligned. The prime source for time delays is the access of the ASA and of the MSA to their respective AAA servers, especially in roaming scenarios that require seamless mobility. The 'claims-based IAM' approach [42], which is based on Microsoft's Active Directory Federation Services (AD FS) and Web Services Federation standard [32], introduces a new IAM architecture where the user/terminal can prove his identity by a security token (e.g. Kerberos tickets, SAML tokens, certificates). This token includes a signed collection of security identifiers (SID) that represent claims associated with the identity. Claims may represent besides identity, roles, permissions or access rights and even general information about the user/terminal. The tokens may be issued to users/terminals by the ASA and MSA or by a global certificate authority. The architecture allows direct requests for service access at the ASP and MSP without involving the ASA or MSA for authorization (token-based authorization). An additional benefit of using a claims-based identity model is that it supports federated and single sign-on scenarios across organizations.

In the following clauses, the main concepts and functionalities of IAM are briefly introduced.

7.2.1 User and terminal identification

For unique characterisation of a specific user/ terminal or other object (e.g. software, hardware, service) a so-called identity is assigned, the concept of identity relates to a collection of identifiers, permissions and other

authentication data necessary to gain access to services. Most telecommunications identification schemes use a single *identifier* to perform (at least) two distinct functions, namely routing and identification. An identifier is a set of data that comprises the claims for an identity. Within the area of communications, a large variety of identifier types exist associated with users, devices, network layers and services. Examples are:

- email address, SIP address, IP address, phone number, MAC address;
- credentials, like account name and password;
- possession of a token (e.g. X.509 certificate, Kerberos ticket), PKI based digital signature) which may be provided by a SIM-card.

Identity Management takes care of the life-cycle management of the identity information involving creation, (re)assignment, integrity maintenance and destruction/revocation of identifiers.

For support of ubiquitous mobility identity federations, also known as Single-Sign-On (SSO) is desirable. SSO extends the validity and use of Identities across the borders of several trust networks, services or applications without central registration or control. It generally requires:

- prior establishment of trust amongst a network of identity providers;
- agreement on protocol standards for the communication of claims (assertions), e.g. SAML;
- agreement on identifiers and attribute types/syntax/semantics, and/or equivalence mappings.

SSO is currently covered by several standards, e.g.: SAML [34], WS-Federations [32], OpenID [36] and the Identity Federation Framework [31]. For the interoperability of roaming services, the IETF has defined the Network Access Identifier NAI [16] as a standardized method for identifying users.

7.2.2 Authentication

Authentication is the process of raising the confidence/assurance level for identification, often as a prerequisite for authorization. It is usually based in an enterprise environment on the use of captive web portal, a centralized LDAP directory service [18], IEEE 802.1X [29] etc. In general authentication involves four roles:

1. Requestor, normally proxied by a client application, e.g. a browser, presenting claims/assertions in return for access to some resource.
2. Relying party (identity consumer), offering some resource (data, application, service) to which a claimant seeks access.
3. Identity authority, called on by the relying party to verify the claimed identity (in the mobility management architecture performed by the ASA and the MSA).
4. Identity provider, for initially verifying a claimant's identity, creating and issuing this identity.

NOTE 1 Identity Management systems and standards differ in the protocols used between these roles.

NOTE 2 Roles 3 and 4 are often fulfilled by the same party.

NOTE 3 A trust relation exists between relying party and identity authority/provider.

NOTE 4 Claims may be presented by use of a physical (e.g. SIM Card) or software token (e.g. cryptographic key).

A common means for secure authentication of mobile terminals and users in a LAN, MAN, and WMAN is the IEEE standard 802.1X [29]. Its core is based on the IETF Extensible Authentication Protocol (EAP) [10]. For WLAN deployment the authentication and encryption standard WPA2 [38] of the WiFi Alliance is widely used. Whereas WPA2 is used in most cases with a global password for all users, the so-called WPA2-enterprise function allows a higher security level using individual user registrations based on standardized variants of EAP. Suitable EAP derivates are EAP with Transport Layer Security (EAP-TLS) [22] or EAP with Tunneled TLS (EAP-TTLS) [23].

7.2.3 Access management

Access to enterprise ICT resources by an identified user/ terminal must be granted by a server, which is usually under full control of the enterprise administration. The degree of authorized access follows in general the enterprise's security policies. Besides identity-based access control, zone-based & role-based access policies may be applied with granular access control to logical groups of systems and users. Further tasks of access management are capturing of audit logs of user activities and capturing of charging information General rules on the access to applications and services may be provided with the service/ application. However user-specific or role-based rules are provided and maintained as part of the user/ terminal profile. The profile itself may either reside at the terminal itself or be available at a server of the user's or terminal's home domain.

Typically access to business applications is granted by system and/or network-based functions without involving the application itself. However, integrated business applications in service oriented architectures often use technologies that bypass or tunnel through system or network security infrastructure, making it impossible to leverage identity-based access control mechanisms. The same problem arises when passing technology and/or administrative borders in the communication path. An alternative is embedding the access control point into the application software. Service-oriented approaches allow centralized management of access policy.

For access management standard authorization protocols have been developed, e.g. the IETF protocol OAuth [25]. The OAuth token-based authorization system allows users/ applications to access protected resources via an API without disclosing their credentials. Another important standard for granular access management solutions is XACML (Xtensible Access Control Marker Language) [33]. A detailed overview on authorization architectures can be found in chapter 2.3 of the ENABLE project report [41].

7.3 Device/ configuration management and policy enforcement

Device management (DM) is a function of the enterprise network to manage mobile/ portable devices, e. g. laptops, smart phones, and to enforce that only devices that correspond to the current enterprise security policies can get access to enterprise ICT resources, especially when they are remote. Examples of DM functions are:

- provisioning – enabling/disabling a device's feature sets;
- configuration – changes to a device's settings and parameters;
- software Upgrades/ Updates – providing new software and/or bug fixes to be loaded onto the device, including applications and system software;
- monitoring – reporting the status of a device.

Usually the functions of DM are fixed, but with the knowledge of the terminal's location, DM functions can be made location-dependent, e.g. to cope with different security conditions or different service environments.

Standardization efforts are the OMA DM [35], OSGi Alliance [37] and the IETF SIP Configuration Framework activities.

A common way to control terminal mobility in an enterprise ICT infrastructure is to restrict to dedicated devices with special client software and the use of VPNs for remote access. VPNs provide end-to-end security by interconnecting the terminal to the enterprise intranet across a shared network infrastructure by using an OSI layer 2, layer 3, layer 2/3 or layer 5 tunnelling technology. When the shared infrastructure is an IP network, the tunnelling technologies that are typically used follows the IETF standards IPsec [17] and TLS/ SSL [21].

However this approach comes with serious drawbacks, such as lack of flexibility and vulnerability of clients when using foreign networks without VPN. Besides, due to the fast emergence of new mobile devices and applications, the restriction to enterprise approved hardware and software is often not in-line with the working behaviour and processes of the mobile workforce. On the other hand, allowing a larger degree of freedom on the choice of devices and application software would significantly increase the costs of device management. A

way out is to restrict the access to enterprise resources to machines inside the enterprise network domain, e.g. the desktop computer of the enterprise user. With a remote control protocol, e.g. Microsoft's RDP (Remote Display Protocol) or a VNC (Virtual Network Computing) protocol; the user can remotely control his desktop over a secure connection from any mobile terminal. Although efficient implementations of remote control protocols exist, like RealVNC. TightVNC, the support of real-time services (audio/video) is not their prime purpose and therefore limited. A more sophisticated solution is the virtualisation of the desktop computer, which is referred as Virtual Desktop Infrastructure and elaborated in more detail in 7.6.

7.4 Location management

The location of mobile terminals/ users and keeping track of movements are not only important for mobility management but also for the efficiency of business processes (e.g. ERM and CRM), and not to forget emergency cases. The mechanism for reliable and timely notification of the current location of a user/terminal to system entities that need it is called location management. For mobility management purposes, location information refers to topological network data e.g. link and transport identifiers, addresses of serving and neighbouring gateways in a LAN or of base stations in a radio network. Another deployment of location management is the determination of geographical position. More information on this aspect can be found in [4].

To protect a user's privacy, location-related information should not be disclosed to untrusted third parties that are not intentionally involved in the communication.

7.5 Reachability management

An important component in the mobility architecture of an enterprise is the provision of a presence service by reachability management. Presence denotes a means to monitor, recognize and broadcast status (online/ offline), availability, contactability and geographic location of a user and his terminals (or a group of users/ terminals) to communicate. In addition the service provides access to the presence information of other users, e.g. colleagues or customers.

User profiles may contain preferences and 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.

Several standardized solutions for presence are available. One solution is the SIP-based SIMPLE [12] approach of the IETF, which has been adopted as presence service for the IMS service architecture [27] deployed by 3GPP and by ETSI TISPAN. Enterprise- and Internet-based communication systems often use XMPP, which also has been standardized by the IETF [14], [15].

Due to the multitude of presence solutions used, aggregation of heterogeneous presence information has become another important task for reachability management of an enterprise.

7.6 Virtual Desktop Infrastructure

Virtual Desktop Infrastructure (VDI) takes the processing off the user's mobile terminal and brings it onto a virtual machine (VM) residing on a data center server that hosts a virtual desktop, including all its applications, configurations and preferences. Besides the virtual desktop, further main components of the architecture are the virtualization hypervisor, which controls the virtualization processes, and a thin client on the user's terminal by which the user interacts with his virtual desktop via a remote control protocol over a secure link (e.g. TLS or IPsec).

VDI is often accomplished with the virtualization of the data center on distributed server farms, so-called clouds. Enterprises use one of the following:

- private clouds, which are owned and operated by the enterprise;
- Virtual private clouds (VPC), where a 3rd party provides server resources;
- federations of both types.

VDI comes with a couple of benefits for mobility of enterprise communications. Because the virtual desktop server resides in the enterprise realm and communicates with the terminal via a thin client, a high level of security is ensured, whereas the efforts for device management for remote users are significantly reduced. Besides, VDI relaxes the constraints for the support of session mobility: as the mobile terminal acts just as a console device to the virtual desktop, the number of sessions to be maintained is reduced to one: the connection session with the VDI server. Therefore an interruption of the communication session would not kill unintentionally application and service sessions running on the virtual machine. Control of these sessions can be resumed by reestablishment of the connection with the same terminal or even with a different device.

From a technical viewpoint VDI allows the use of any kind of terminal for secure enterprise communication, even terminals provided by internet cafés. However some enterprises enforce, for security reasons, a strict separation between the virtual desktop and local non-trusted peripheral devices, e.g. the local hard disk or USB devices. Users may consider this as a serious limitation as it impacts their working methods. Possible ways around this are certified devices or trusted services.

Another issue associated with VDI is that insufficient QoS and traffic management on the network link between the remote terminal and the VM significantly impairs the performance, because screen refresh, keystrokes and video/audio data must be delivered to/from the terminal in real time. Although the major VDI control protocols, e.g. Microsoft Remote Display Protocol (RDP) or Citrix's ICA protocol, are highly optimized, solving the contention of VDI traffic with other traffic types is still an open issue, especially on low-bandwidth links. This applies especially for conversational services over asymmetric data links, e.g. Asymmetric DSL, that provide high downlink data rates but significantly lower uplink rates.

A promising approach to VDI, which solves a couple of problems mentioned above, comes from the open project SPICE 'Simple Protocol for Independent Computing Environments' (www.spicespace.org). The project has defined a multi-tiered VDI architecture and a rendering protocol to connect users/ terminals with their virtual desktop [39]. Due to load balancing between thin client, virtualization hypervisor and virtual desktop the data traffic between thin client and hypervisor can be significantly reduced. Therefore the approach can support besides computing services also conversational audio-/video services with high quality. The SPICE protocol also allows the use of local USB devices by USB redirection to the virtual desktop.

In general, VDI is lacking of open standards that allow some kind of interoperability between the components involved. The SPICE deliverable, the "Virtual Device Interfaces (VDI) provides a standardized way to publish interfaces of virtual devices. This enables e.g. the graphical interface of a mobile terminal to interact with the virtual device and vice versa [40].

A less strict solution than VDI is the provision of critical applications by a remote server (Software as a Service SaaS), which can also provide realtime communication services. Examples are so-called webapps, which execute services/applications on a remote server farm (cloud) and communicate with the terminal via a common web-browser using application protocols such as HTTP, WEBDAV etc. For secure transport TLS [21] is used. The user's access to the server is usually secured by an enterprise web portal.

8 Requirements and standardization gaps

The provision of mobility types and their attributes and usage modes is strongly dependent on the application requirements and the network infrastructure. Table 1 presents mobility characteristics of typical enterprise users according their user roles.

NOTE 1 An individual will always have more than one role, having at least working and idle time modes.

NOTE 2 Where voice is mentioned, other real-time media might also be possible.

Table 1 — Mobility characteristics of typical enterprise users

	Campus Nomad	Teleworker/ Day Extender	Road Warrior
Application description	Workers with frequent on-campus or inter campus movements	Small/ Home office (SOHO) workers or workers temporarily working at home	Workers with frequent off-campus movements, e.g. in the area of field service, sales, transport/ logistics
Point of network attachment	On campus e.g. enterprise premises, hospital, manufacturing, retail	Off campus e.g. home office, branch office	Off campus e.g. external enterprise premises, hotel, airport, Internet cafe
Typical. mobility modes	Mobile Nomadic, Portable	Nomadic	Mobile Nomadic Portable
Access networks	Corporate LAN, WLAN	Public WAN (carrier, ISP) Public WWAN Private LAN/ WLAN	Public WAN (carrier, ISP) Public WWAN Private LAN Public WLAN/ WiFi (hotspot)
Terminals	Office PC (voice & data) Office laptop (voice & data) Office wired phone (voice) WLAN-phone (voice) Mobile phone (voice) Smart phone (voice & data)	Office PC (voice & data), Private PC using virtual desktop (voice & data) Office laptop (voice & data) Wired phone (voice) Mobile phone (voice) Smart phone (voice & data)	Private PC using virtual desktop (voice & data) Office laptop (voice & data) Wired phone (voice) WLAN-phone (voice) Mobile phone (voice) Smart phone (voice & data)
Reachability, Presence	Reachable under company identity	Reachable under company identity (includes mobile phone, phone emulation on desktop and even wired phone at home)	Reachable under company identity (includes mobile phone, phone emulation on laptop and even wired phone in the hotel)

For a more detailed elaboration of functional requirements of enterprise mobility and the associated standardization issues, mobility deployments scenarios have been classified according the following mobility modes:

- Nomadic mode,
- Portable mode,
- Mobile mode.

The selection of scenarios in the subsequent clauses is not considered as exhaustive but should represent the most relevant applications of enterprise mobility. Only full IP-based scenarios with stationary networks are considered. Technologies such as adhoc networks, meshed networks and moving networks are out of scope

of this report. As enterprise mobility has many stakeholders with different interests, the requirements reflect their particular perspectives in terms of mobility management, identity management, device management, reachability management and location management. 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);
- regulators, who set a legal framework for operating services in their area of responsibility.

In general an enterprise mobility solution has to meet the following requirements:

- compliance with security policies of the enterprise ICT infrastructure;
- support of heterogeneous networking, enabling roaming across external network domains and access network technologies;
- integration into the ICT infrastructure with minimal modifications;
- provision of enterprise-grade QoS;
- provision of availability and presence information;
- traffic optimization by minimizing signalling overhead and by routing optimization;
- availability of enterprise's PBX services on a mobile terminal;
- mobile access to enterprise contact data in groupware applications, SQL and/or LDAP databases;
- availability on the mobile terminal of additional caller identification information from enterprise directories;
- ubiquitous service access;
- efficient IP transport across different IP versions (IPv4, IPv6, IPv4 with NAT etc.) and across different access technologies.

8.1 Nomadic deployments

Nomadic mode refers to the provision/ use of mobility types just at distinct Point of Access (PoA). Terminal, user and service mobility, require connection set up and terminal/user registration each time the PoA and/or the terminal has changed. There is no support for session mobility...

Examples are:

- remote access from a non-enterprise location (Hotel, airport etc.);
- teleworking, a home user solution with e.g. Soft Client (or SIP Phone) and VPN;
- hotelling, a solution that allows visitors to a company to be assigned a visitor's cubicle with telephone and LAN access;
- hot-desking, where an employee can get LAN access and also log-on to a phone system to obtain his own phone service outside his office.

8.1.1 Scenario: Hot-desking within the enterprise network (NGCN)

An enterprise user accesses the enterprise resources (voice & data) via WLAN from a branch office that belongs to a different network domain than the user's home domain.

	Functional requirements
Mobility management	• Support of inter-domain user mobility • Support of inter-domain terminal mobility • Support of service mobility: dial plan of the enterprise, user profiles
Identity management	Support of Single Sign-On across domains of the enterprise network
Device management	No special mobility requirements
Reachability management	No special mobility requirements
Location management	No special mobility requirements

In this scenario the access network is provided by a domain of the enterprise network. The domain acts as ASA and ASP by authenticating and authorizing the terminal to use the WLAN of the branch office. For authorized terminals it usually provides a captive portal service, which allows the user to register for getting access to data resources and to phone services as in his home office. The network of the branch office is in most cases connected to the main office via a trusted network, e.g. a leased line provided by a public operator.

8.1.2 Scenario: Remote access from a public network

A mobile worker accesses the enterprise intranet via a LAN connection which is provided by a hotel.

	Requirements
Mobility management	• Support of intra-domain user mobility • Support of intra-domain terminal mobility • Support of intra-domain service mobility: (dial plan, call control services)
Identity & management	Ensure end-to-end security
Device management	No special mobility requirements
Reachability management	No special mobility requirements
Location management	Provision of geographic location information

The difference to the previous scenario is that the access network is non-trusted. Security policies of most enterprises require end-to-end security for the interconnection of terminal to the enterprise network. Due to incompatibilities of network control mechanisms and missing trust relationships of the involved network nodes, the use of a layer-2, layer-3 or layer-5 VPN has become a common solution. In a first step the user has to register his terminal to the hotel LAN to get access to the internet. In the next step the user sets up a VPN

connection between his VPN client and a VPN termination node of the enterprise home domain using identity-based authentication.

Any terminal can be used to get access to hotel LAN; however setting up a VPN connection is restricted to dedicated VPN clients on company-owned terminals. A less restrictive solution is the use of a virtual desktop is connected via a layer-5 VPN (SSL, TLS), which does not require dedicated company clients, but due to lack of standards this requires a thin client that is compatible with the VDI used in the enterprise (see 7.6 for details).

Traditional Internet VPNs have been based on IPsec to provide security over the Internet. Service providers are now beginning to deploy enhanced VPN services that provide features such as service differentiation, traffic management, Layer 2 and Layer 3 connectivity, etc. in addition to security. Newer tunnelling mechanisms have certain features that allow the service providers to provide these enhanced VPN services. The IETF working groups L2VPN and L3VPN are chartered on standardization of provider provisioned VPN services with layer 2 and layer 3 connectivity.

8.2 Portable deployments

Portable mode refers to the provision/ use of mobility similar to nomadic mode but with support of session mobility. This enables a terminal/ user to suspend an ongoing session and resume it at a new PoA or on a different terminal. As portable mode is a superset of nomadic mode, the requirements for nomadic deployments are also valid for portable deployments.

8.2.1 Scenario: Changing location of a terminal while keeping communication sessions alive

An employee disconnects his laptop from his office WLAN in the enterprise premises without closing running sessions and moves to the airport where he reconnects to a public WLAN and resumes his sessions.

	Functional requirements
Mobility Management	• Support of intra-domain user mobility • Support of intra-domain terminal mobility • Support of intra-domain session mobility • Support of intra-domain service mobility: (dial plan, call control services)
Identity Management	• Support of Single Sign-On across domains of the enterprise network • End-to-end security
Device Management	No special mobility requirements
Reachability Management	No special mobility requirements
Location management	Provision of geographic location information

This scenario can be solved with the similar approach to that described in 8.1.2. For session maintenance mobility management could in principle provide a proxy server, which keeps active sessions alive until the user reconnects. In case of using a non-enterprise terminal or using a different terminal to resume the session, the proxy solution won't work if sessions include bindings to the terminal. The use of a VDI approach appears more appropriate for portable deployments. As described in 7.6, disconnecting the mobile terminal does not affect active sessions running on the virtual desktop and there is no binding to a specific terminal.

8.2.2 Scenario: Changing terminal while keeping communication sessions alive

On the way to his office an employee has started a VoIP and a data session on a WLAN smart phone. At his office he transfers the sessions to his desktop PC to use extended features of this system.

	Functional requirements
Mobility management	• Support of intra-domain user mobility • Support of intra-domain session mobility
Identity management	No special mobility requirements
Device management	No special mobility requirements
Reachability management	No special mobility requirements
Location management	No special mobility requirements

The required functionality looks very similar to the call control 'Call Transfer' known from circuit-switched telecommunication networks. With a so-called unattended or blind transfer a user can transfer a call received on his terminal directly to another terminal whose number he has dialled.

Considering that SIP is the dominating signalling protocol in IP-based enterprise and public core networks and that the call transfer behaviour can be emulated to a large extent, SIP appears to be a suitable mobility management solution for this scenario. Based on the SIP specifications 'SIP Refer method [9]' and 'SIP Replaces Header [13]' call flows have been defined by the IETF [24] to transfer voice, data and other associated sessions from one SIP terminal to another one, which can be addressed by its SIP address. As SIP is a layer 5 protocol the transfer is independent of the underlying access network technology.

The call flows for Call Transfer implemented e.g. in an IMS-based [27] public network differ from the IETF specification [24]. Implementations in enterprise networks e.g. NGCNs [1], follow either the IETF or the IMS specification. Therefore, ubiquitous session mobility across public and enterprise networks may require interworking functions.

8.3 Mobile deployments

Mobile mode denotes the ability of the involved networks to provide continuous service to a mobile terminal/ user with virtually no interruption while moving. In cases where the delay or loss of data is not perceived by the user as degradation of quality of service, the mobility involved is called seamless. Mobile mode is typically provided by wireless cellular networks, e.g. WMANs.

8.3.1 Scenario: Continuous connection across different public networks with the same access technology

An employee is using information and communication services from his company via smart phone while travelling in a car. During his drive he traverses the coverage area of different public carrier mobile networks.

	Functional requirements
Mobility management	• Support of inter-domain user mobility • Support of inter-domain terminal mobility with seamless handover • Support of inter-domain session mobility • Support of inter-domain service mobility
Identity management	• User and terminal should have a unique ID across the public and enterprise networks • Handover of sessions related to security associations should involve only a few entities to reduce round trip times for signalling • Provision of local MM for roaming between foreign networks to reduce signaling traffic to/from the enterprise network
Device management	Support of device management signalling (e.g. for monitoring) and services by the public networks
Reachability management	Support of presence information across public domains
Location management	Provision of geographic location information

A common solution for this scenario is to leave the mobility management roles (ASA, ASP, MSA, and MSP) completely at the public mobile network operators. In this case the employee has a subscription at a mobile operator which entitles him to use voice services and to set up in parallel VPN tunnels to the enterprise's intranet. This means, that enterprise user has two home domains one with the public operator for receiving mobility and communication services in public networks and another one to use enterprise services. Roaming between mobile networks of different public operators follows the same rules as for any other public user.

The major drawbacks of this solution are that the mobility of the employees is out of direct control of the enterprise and that the mobile worker cannot use extended features of the enterprise network when relying on public access networks. Therefore it would be desirable for the enterprise network operator to set up a federated mobility management. However applying global mobility management a handover to or within a foreign network domain generates significant data traffic between the terminal, the visited network and the home network. This makes the requirement of seamless handovers very challenging. For traffic optimization the ENABLE project [41] has proposed a mobility architecture which makes more use of local mobility management when a user is roaming in a foreign network domain. The proposal is based on extensions to the IETF protocol NETLMM [19] with support of IEEE 802.21 [30], which provides a standardized technology-independent interface between the access network and the terminal. Further reduction of signalling overhead can be gained by using claim-based identity in combination with token-based authorization as described in 7.2. A step in this direction is a mobility architecture where the public operators locally manage handovers in their network access domains whereas the enterprise acts as the home network for global management of their employee's real-time communications and data sessions. A serious issue with this approach is however the lack of standards for efficient interworking and federations between public and enterprise networks, e.g. between IMS networks and NGCNs.

A part of the problem is addressed by the 3GPP technical specification group 'Services and System Aspects'. This group is working on a feasibility study on the support for 3GPP voice interworking with enterprise IP-PBX [28].

8.3.2 Scenario: Continuous connection across an enterprise and a public mobile network with different access technologies

An employee has received a call on his smart phone via the campus WLAN. During the call he left the coverage area of the enterprise WLAN and the connection is continued via a public carrier mobile network. In order to save costs, the opposite occurs when the employee moves back within the coverage area of the enterprise WLAN.

	Functional requirements
Mobility management	• Support of intra- and inter-domain user mobility with seamless handover • Support of inter-domain and inter-technology terminal mobility with seamless handover • Support of intra-and inter-domain session mobility with seamless handover • Support of intra-domain service mobility: dial plan, user profiles • The handover solution should work across NATs • Multihoming support for local and global mobility management
Identity management	• User and terminal should have a unique ID across the public and enterprise network (SSO) • Handover of security associations should involve only few entities to reduce round trip times for signalling
Device management	Support of device management signalling (e.g. for monitoring) and services by the public networks
Reachability Management	Support of presence information across enterprise and public domains
Location management	Provision of geographic location information

A common solution for this scenario is the use of dual-mode terminals which use multihoming to provide soft handovers when changing connection from the enterprise WLAN to a public WMAN or vice versa. The handover of the connection between the access networks can be controlled by the enterprise network using global or local mobility management protocols with support of IEEE 802.21 as described in 7.1.1.1. For handover of voice and data sessions SIP Call Transfer can be applied in a similar way as described in 8.2.2. In this case, however, the enterprise mobility management triggers the transfer.

Critical issues with this approach are:

- achievement of seamless handover for real-time sessions with SIP;
- lack of standardized specifications for efficient interworking and co-operation between public and enterprise IP-based networks;
- differences in multihoming process/routing for IPv4 and IPv6.

9 Summary of standardization gaps

In Clause 7 and 8 some potential standardization needs for mobility in enterprise communication have been identified. The subsequent clauses summarize these findings as they apply to the management functions of the mobility infrastructure. Filling the gaps is up to the affected stakeholders. Specifications can be done either by a standardization organization like Ecma International or even by industry initiatives.

9.1 General issues

As ubiquitous service access for the mobile workforce is an important feature, an enterprise mobility system has to interwork with different access network technologies and with different external administrative domains. To improve service delivery (e.g. end-to-end security), convergence of public and enterprise IP-based networks is desirable. Standards on the following subjects are missing:

- General network control mechanisms including generic control signalling interfaces, which are applicable across different domains (e.g. IMS-based networks (UMTS,NGN), NGCN) and are agnostic to access technology (WLAN, LTE etc.), For the sake of minimum impact on established standards a layered approach should be taken.

- Efficient IP transport across different IP versions (IPv4, IPv6, IPv4 with NAT etc.) and across different access technologies.

9.2 Mobility management

Mobility management for achieving seamless handovers for mobile deployments is a challenging issue. Standards are missing for federated mobility architectures involving public and enterprise networks, including an efficient balance of local and global mobility management. The main issue is the reduction of signalling overhead for the provision of session continuity and security associations.

9.3 Identity and access management

Identity and access management (IAM) becomes an issue in heterogeneous network environments, which can prevent identity-based security relationships. A way out is the design of multi-tier IAM architectures or SOA-based applications with built-in access control points. Currently proprietary products are available but no standardized approaches. Another issue comes with fast reauthentication and reauthorization in roaming scenarios. The use of authorization tokens looks promising but there are no open standards.

9.4 Device/configuration management

The increasing deployment of VDI in enterprise ITC infrastructures reduces the need of specific device management for remote terminals to zero. However, the current solutions are vendor specific, which do not allow interworking of thin clients and virtualisation servers (hypervisors) from different vendors. Another interoperability issue is the use of proprietary communication protocols between clients and servers. A first step towards relieving vendor lock-in has been made with the open source project SPICE (see 7.6).

9.5 Reachability management and location management

With the emergence of non-enterprise specific terminals the number of presence, availability and location tools used by the moving workforce will certainly increase. As the classical enforcement of a single tool is not acceptable for most employees the challenge is how to aggregate reachability information from different sources and how to make it available to business processes. Another challenge is how reachability information can reflect the QoS actually available at the user's terminal(s).

Bibliography

[1] ISO/IEC TR 12860, *Information technology — Telecommunications and information exchange between systems — Next Generation Corporate Networks (NGCN) — General*

[2] ISO/IEC TR 12861, *Information technology — Telecommunications and information exchange between systems — Next Generation Corporate Networks (NGCN) — Identification and routing*

[3] ISO/IEC TR 16166, *Information technology — Telecommunications and information exchange between systems — Next Generation Corporate Networks (NGCN) — Security of session-based communications*

[4] ISO/IEC TR 16167, *Information technology — Telecommunications and information exchange between systems — Next Generation Corporate Networks (NGCN) — Emergency calls*

[5] ECMA TR/102, Personal Networks – Overview and Standardization Needs
http://www.ecma-international.org/publications/techreports/E-TR-102.htm

[6] IETF RFC 2904, AAA Authorization Framework
http://tools.ietf.org/html/rfc2904

[7] IETF RFC 3261, SIP: Session Initiation Protocol
http://tools.ietf.org/html/rfc3261

[8] IETF RFC 3344, IP Mobility support for IPv4
http://tools.ietf.org/html/rfc3344

[9] IETF RFC 3515, The Session Initiation Protocol (SIP) Refer Method
http://tools.ietf.org/html/rfc3515

[10] IETF RFC 3748, Extensible Authentication Protocol (EAP)
http://tools.ietf.org/html/rfc3748

[11] IETF RFC 3775, IP Mobility support in IPv6
http://tools.ietf.org/html/rfc3775

[12] IETF RFC 3856, A Presence Event Package for the Session Initiation Protocol (SIP) http://tools.ietf.org/html/rfc3856

[13] IETF RFC 3891, The Session Initiation Protocol (SIP) ‘Replaces’ Header
http://tools.ietf.org/html/rfc3891

[14] IETF RFC 3920, XML streams, SASL, TLS, stringprep profiles, stanza semantics
http://tools.ietf.org/html/rfc3920

[15] IETF RFC 3921, XMPP extensions for basic instant messaging and presence
http://tools.ietf.org/html/rfc3921

[16] IETF RFC 4282, The Network Access Identifier
http://tools.ietf.org/html/rfc4282

[17] IETF RFC 4301, Security Architecture for the Internet Protocol
http://tools.ietf.org/html/rfc4301

[18] IETF RFC 4511, Lightweight Directory Access Protocol (LDAP): The Protocol
http://tools.ietf.org/html/rfc4511

[19] IETF RFC 4831, Goals for Network-Based Localized Mobility Management (NETLMM) http://tools.ietf.org/html/rfc4831

[20] IETF RFC 5213, Proxy Mobile IPv6
http://tools.ietf.org/html/rfc5213

[21] IETF RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2
http://tools.ietf.org/html/rfc5246

[22] IETF RFC 5247, Extensible Authentication Protocol (EAP) Key Management Framework
http://tools.ietf.org/html/rfc5247

[23] IETF RFC 5281, Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)
http://tools.ietf.org/html/rfc5281

[24] IETF RFC 5589, Session Initiation Protocol (SIP) Call Control – Transfer
http://tools.ietf.org/html/rfc5589

[25] IETF RFC 5849, The OAuth 1.0 Protocol
http://tools.ietf.org/html/rfc5849

[26] ITU-T Rec. G.1010, End-user multimedia QoS categories
http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.1010-200111-I!!PDF-E&type=items

[27] 3GPP TS 23.228, IP Multimedia Subsystem
http://www.3gpp.org/ftp/Specs/html-info/23228.htm

[28] 3GPP Technical Report 22.8de V0.1.0 (2010-08), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility Study on Support for 3GPP Voice Interworking with Enterprise IP-PBX (VINE)
http://www.3gpp.org/ftp/tsg_sa/WG1_Serv/TSGS1_51_Seoul/Docs/S1-102379.zip

[29] IEEE 802.1X, IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control
http://www.ieee802.org/1/pages/802.1x-rev.html

[30] IEEE 802.21, Media independent handover
http://www.ieee802.org/21/

[31] Liberty Alliance Identity Federation Framework V.1.2 (ID-FF)
http://projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications/?f=resource_center/specifications/liberty_alliance_id_ff_1_2_specifications

[32] OASIS, Web Services Federations
http://www.oasis-open.org/committees/documents.php?wg_abbrev=wsfed

[33] OASIS, XACML 2.0 Core: eXtensible Access Control Markup Language (XACML) V 2.0,
http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

[34] OASIS, Security Assertion Markup Language (SAML) 1.0/1.1/2.0
http://www.oasis-open.org/specs

[35] OMA Device Management V2.0
http://www.openmobilealliance.org/Technical/release_program/dm_v2_0.aspx

[36] OpenID Authentication 1.1/2.0
http://wiki.openid.net/OpenID_Authentication_2

[37] OSGi Alliance, JSR 232 Mobile Operational Management
http://www.osgi.org/JSR232/HomePage

[38] WiFi Alliance WPA2 (WiFi Protected Access 2)
http://www.wi-fi.org/knowledge_center/wpa2

[39] SPICE Project, Spice remote computing protocol definition v1.0
http://www.spicespace.org/docs/spice_protocol.pdf

[40] SPICE Project, VD Interfaces
http://www.spicespace.org/docs/vd_interfaces.pdf

[41] IST ENABLE Project Report, ENABLE – Enabling efficient and operational mobility in large heterogeneous IP networks, ISBN 978-84-691-0647-1 (http://www.ipv6tf.org/pdf/enablebook.pdf)

[42] Claims-based Identity for Windows, Report from David Chappell & Associates, 2009
http://www.davidchappell.com/writing/white_papers/Claims-Based_Identity_for_Windows_v2.pdf

ICS 35.110

Price based on 31 pages