International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2811

(07/2012)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Generalized mobility

Framework of the mobile virtual private network service in next generation networks

Recommendation ITU-T Y.2811

ITU International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	**Y.2800–Y.2899**
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.2811

Framework of the mobile virtual private network service in next generation networks

Summary

Recommendation ITU-T Y.2811 describes the functional architecture of the mobile virtual private network (VPN) service based on the host-based mobility framework in next generation networks (NGNs), and defines the corresponding reference points. This Recommendation focuses on remote access VPNs and community-based VPNs where mobile user equipment (MUE) is directly involved. The high-level mobile VPN service procedures on the functional architecture are also described.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2811	2012-07-29	13

Keywords

Mobile VPN, NGN.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.2811

Framework of the mobile virtual private network service in next generation networks

1 Scope

There are several types of virtual private network (VPN) services such as remote access VPN (or client-to-server VPN), site-to-site VPN, community-based VPN, etc. This Recommendation focuses on the mobile VPN framework in NGN based on the host-based mobility framework in which mobile UEs are directly involved in the VPN. The mobile VPN framework is based on the mobility-related ITU-T Recommendations [ITU-T Q.1706], [ITU-T Q.1707], [ITU-T Q.1708], [ITU-T Q.1709] and [ITU-T Y.2018], as well as on the VPN requirements described in [ITU-T Y.2215]. This Recommendation covers the following:

– requirements of mobile VPN;

– mobile VPN architecture in terms of high-level functions, functional architecture and reference points;

– high-level mobile VPN procedures based on host-based mobility.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T G.1000] Recommendation ITU-T G.1000 (2001), *Communications Quality of Service: A framework and definitions*.

[ITU-T M.1400] Recommendation ITU-T M.1400 (2006), *Designations for interconnections among operators' networks*.

[ITU-T Q.1706] Recommendation ITU-T Q.1706/Y.2801 (2006), *Mobility management requirements for NGN*.

[ITU-T Q.1707] Recommendation ITU-T Q.1707/Y.2804 (2008), *Generic framework of mobility management for next generation networks.*

[ITU-T Q.1708] Recommendation ITU-T Q.1708/Y.2805 (2008), *Framework of location management forNGN*.

[ITU-T Q.1709] Recommendation ITU-T Q.1709/Y.2806 (2008), *Framework of handover control forNGN*.

[ITU-T X.1035] Recommendation ITU-T X.1035 (2007), *Password-authenticated key exchange (PAK) protocol*.

[ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.

[ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.

[ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks.*

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.

[ITU-T Y.2014] Recommendation ITU-T Y.2014 (2008), *Network attachment control functions in next generation networks*.

[ITU-T Y.2018] Recommendation ITU-T Y.2018 (2009), *Mobility management and control framework and architecture within the NGN transport stratum*.

[ITU-T Y.2091] Recommendation ITU-T Y.2091 (2007), *Terms and definitions for Next Generation Networks*.

[ITU-T Y.2111] Recommendation ITU-T Y.2111 (2006), *Resource and admission control functions in Next generation Networks*.

[ITU-T Y.2215] Recommendation ITU-T Y.2215 (2009), *Requirements and framework for the support of VPN services in NGN, including the mobile environment*.

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application [ITU-T Y.101]: A structured set of capabilities, which provide value-added functionality supported by one or more services.

3.1.2 functional architecture [ITU-T Y.2012]: A set of functional entities and the reference points between them used to describe the structure of an NGN. These functional entities are separated by reference points, and thus, they define the distribution of functions.

NOTE – The functional entities can be used to describe a set of reference configurations. These reference configurations identify which reference points are visible at the boundaries of equipment implementations and between administrative domains.

3.1.3 functional entity [ITU-T Y.2012]: An entity that comprises an indivisible set of specific functions. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.

3.1.4 host-based mobility management [ITU-T Q.1707]: A mobility management scheme in which the MM signalling is performed based on (or controlled by) the user equipment (UE).

3.1.5 mobility [ITU-T Q.1706]: The ability for the user or other mobile entities to communicate and access services irrespective of changes of the location or technical environment.

3.1.6 next generation network (NGN) [ITU-T Y.2001]: A packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

3.1.7 quality of service (QoS) [ITU-T G.1000]: The collective effect of service performances, which determine the degree of satisfaction of a user of the service.

3.1.8 service stratum [ITU-T Y.2011]: That part of the NGN which provides the user functions that transfer service-related data and the functions that control and manage service resources and network services to enable user services and applications (see also clause 7.1 of [ITU-T Y.2011]).

3.1.9 service [ITU-T Y.2091]: A set of functions and facilities offered to a user by a provider.

3.1.10 service provider [ITU-T M.1400]: A general reference to an operator that provides telecommunication services to customers and other users either on a tariff or contract basis. A service provider may or may not operate a network. A service provider may or may not be a customer of another service provider.

3.1.11 transport stratum [ITU-T Y.2011]: That part of the NGN which provides the user functions that transfer data and the functions that control and manage transport resources to carry such data between terminating entities (see also clause 7.1 of [ITU-T Y.2011]).

3.1.12 virtual private network (VPN) [ITU-T Y.2215]: A VPN is a communication network, built over public and/or private network resources, used to support controlled and secure communications within a group of users as if they were on a private network.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BID	Binding Identification
e-MCF	enterprise Mobility Control Function
e-NAF	enterprise Network Attachment Function
e-RACF	enterprise Resource Admission and Control Function
GW	Gateway
HBM	Host-Based Mobility
IKE	Internet Key Exchange
IPsec	Internet Protocol security
MLM-FE	Mobility Location Management Functional Entity
MM	Mobility Management
MMCF	Mobility Management and Control Functions
MOBIKE	Mobile IKE
MP-t-MP	Multipoint-to-Multipoint
MUE	Mobile User Equipment
NACF	Network Attachment Control Functions
NGN	Next Generation Network
PAK	Password-Authenticated Key exchange
PD-FE	Policy Decision Functional Entity
P-t-P	Point-to-Point
PW	Password

QoS	Quality of Service
RACF	Resource Admission and Control Functions
SCF	Service Control Functions
TID	Tunnel Identification
VPN SCF	VPN Service Control Functions
VPN	Virtual Private Network
VTF	VPN Transport Functions

5 Conventions

None.

6 Requirements

The basic requirements of mobile VPN follow the NGN VPN requirements listed in [ITU-T Y.2215]. This clause identifies and focuses on the mobile VPN service and mobility requirements.

The VPN in the NGN mobile environment is required to support the following service requirements:

– the mobility protocol and related security association mechanisms are required to establish secure mobile VPN tunnels;

– the secure mobile VPN tunnels should be released and set up seamlessly as an MUE moves;

– a point-to-point/multipoint-to-multipoint (P-t-P/MP-t-MP) VPN tunnel should be created among peers in a community group;

– the VPN service control function is required to provide VPN service by extending the NGN service control function;

– allow mobile users to access the VPN resources in and out of their networks while supporting seamless mobility;

– resource provisioning and re-provisioning for mobile VPN tunnels in the initial attachment and handover cases should be considered.

7 Mobile VPN architecture

7.1 High level functions

The NGN architecture is a general service- and technology-independent architecture that can be later instantiated in customized architectures that can respond to specific contexts in terms of the services offered and the technologies used, according to [ITU-T Y.2012]. To provide mobile VPN services, several functions in both the service stratum and the transport stratum would be required to extend their functionalities and/or define new ones, as illustrated in Figure 7-1.

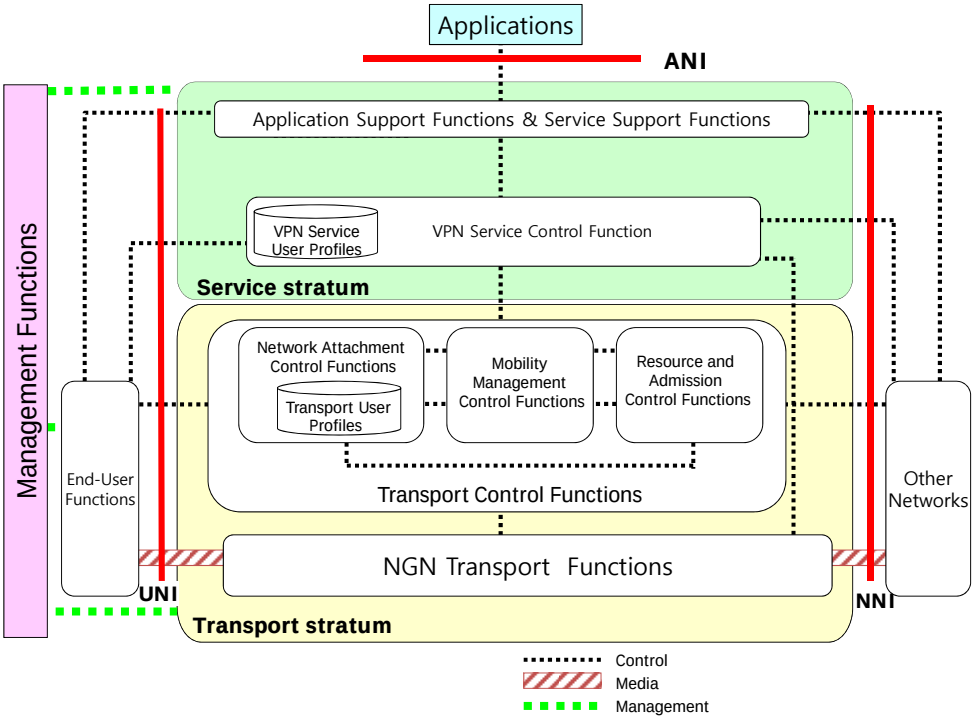

Figure 7-1 – High-level mobile VPN architecture

7.1.1 VPN control functions in NGN

7.1.1.1 VPN transport control functions

The transport stratum provides mobile VPN connectivity services to NGN users under the control of transport control functions, including the network attachment control functions (NACF), the resource and admission control functions (RACF) and the mobility management and control functions (MMCF).

The NACF provides the registration function to allow registration of NGN users at the access level and also provides the initialization of the end-user functions so that the users can access NGN services including the mobile VPN service. The function provides network-level identification/authentication for NGN users. The function could also deliver user profiles to RACF so as to configure basic policies for the users in the related network elements. More detailed information on NACF in NGN can be found in [ITU-T Y.2014].

The RACF manages NGN resources to support resource reservation for traffic flows. The function provides admission control and gate control for traffic flows based on user profiles, SLA, operator specific policy rules, service priority and resource availability within access and core transport networks. More detailed information about RACF in NGN can be found in [ITU-T Y.2111].

The MMCF provides mobility for traffic flows. The mobility mechanism for mobile VPN service in this Recommendation is based on the host-based mobility architecture which is defined in [ITU-T Y.2018]. More detailed information about MMCF can be found in [ITU-T Y.2018].

According to [ITU-T Y.2012], NGN transport control functions are able to support different types of NGN services in a common way. Mobile VPN service is expected to be supported by those functions as well.

7.1.1.2 VPN service control function

The delivery of mobile VPN services to the end-user is provided by utilizing the application support functions and service support functions, and related service control functions. The VPN service control function (VPN SCF) is a subset of the service control function in the NGN service stratum to support mobile VPN services. It provides the following functions:

– management of VPN membership including authentication and authorization for the VPN service;

– request of resource and admission control to RACF for VPN service requests from VPN users;

– management of VPN identification and VPN path information, and fault management of VPN path.

7.1.2 VPN control functions in enterprise networks

An enterprise network could have its own VPN control functions which would be used for a remote access mobile VPN service which is not managed by NGN.

7.1.2.1 VPN transport control functions

An enterprise network could have corresponding transport control functions with the network attachment control functions (NACF), the resource and admission control functions (RACF) and the mobility management and control functions (MMCF); enterprise network attachment functions (e-NAF), enterprise resource and admission control functions (e-RACF) and enterprise mobility control functions (e-MCF).

The e-NAF is responsible for allocation of IP addresses to the MUEs cooperating with the NACF in the NGN.

The e-RACF provides resource management to support resource reservation for traffic flows within an enterprise network. The function provides admission control and gate control for traffic flows based on user profiles, enterprise network specific policy rules, service priority and resource availability within the enterprise networks. The e-RACF may interact with the RACF in NGN.

The e-MCF provides mobility management for traffic flows. The mobility mechanism in this Recommendation is based on the host-based mobility architecture.

7.1.2.2 VPN service control function

An enterprise network could have its own VPN service control functions which would be used for the remote access mobile VPN service which is not managed by NGN. The VPN service control functions inherit service control function in the NGN service stratum to support mobile VPN services and provide the following functions:

– management of VPN membership including authentication and authorization for VPN service;

– request of resource and admission control to e-RACF for VPN service requests from VPN users;

– management of VPN identification and VPN path information, fault management of VPN path, etc.

7.1.3 VPN transport functions

The VPN transport functions (VTF) is a subset of the transport functions in the NGN transport stratum that support mobile VPN services, which provides the following functions:

– VPN tunnel encapsulation and decapsulation;

– VPN traffic engineering mechanisms such as service priority control, packet filtering, traffic classification, rate limiting, resource reservation and admission control at the transport stratum;

– handover execution.

7.1.4 VPN end-user functions

The VPN end-user functions provide the following functions:

– Host-based mobility protocol supporting security association for data packets;

– VPN registration/deregistration functions.

7.2 Functional architecture

7.2.1 Remote access mobile VPN

The remote access mobile VPN model is a VPN service model for the MUEs which connect remotely from outside an enterprise network to the resources inside an enterprise network or to the other corresponding MUEs outside the enterprise network. For example, an MUE may try to connect to the enterprise resources which are located in the head office site while moving around outside the network.

There are two types of remote access mobile VPNs depending on whether the VPN service control and mobility control are performed by a public NGN service provider or an enterprise network: the remote access mobile VPN with public service control and the remote access mobile VPN with enterprise network control.

7.2.1.1 Remote access mobile VPN with public service control

This is a mobile VPN service type in which a public NGN service provider offers mobile VPN service. The NGN service provider controls the VTF and performs VPN service management and mobility control as well as access and service authentication for the remote mobile VPN users. The remote mobile VPN users, however, may need to go through an additional authentication procedure internal to the enterprise.

As defined in [ITU-T Y.2018] and related ITU-T Recommendations, an MUE may require two IP addresses: the persistent IP address and the temporary IP address. The persistent IP address is allocated either statically or dynamically, and the temporary IP address is allocated by the current NGN access network at network attachment time.

The VPN SCF will manage VPN identification and VPN path information, and will provide fault management for the paths. The resource control for the VPN should be processed by RACF after receiving a request from VPN SCF, and once after RACF provisions quality of service (QoS) for the VPN paths, VPN SCF should manage the status of the paths.

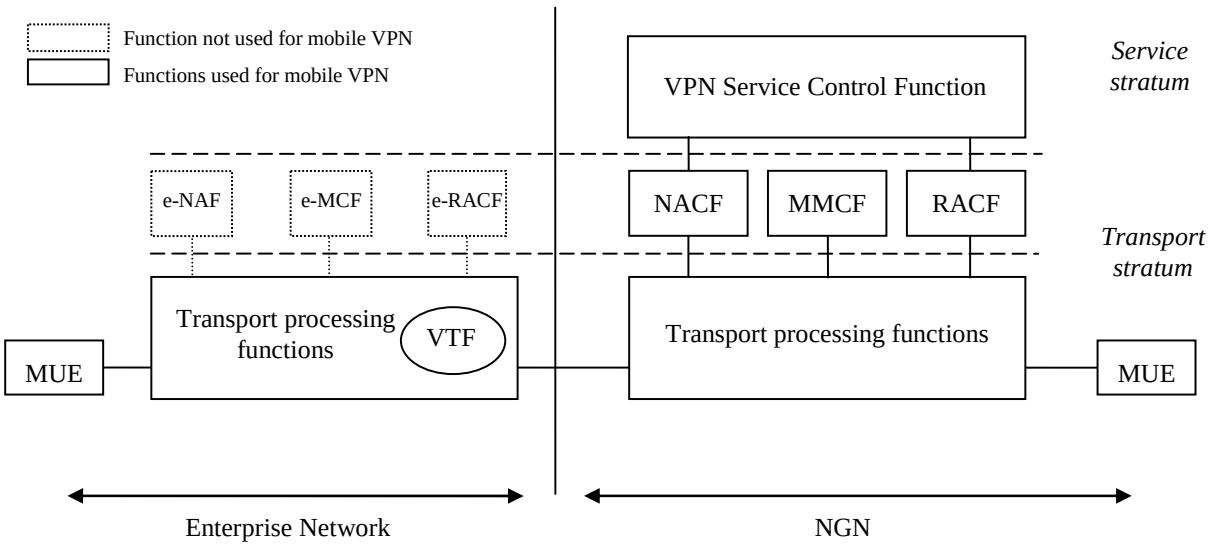

Figure 7-2 – Functional architecture of remote access mobile VPN with public service control

7.2.1.2 Remote access mobile VPN with enterprise service control

This is a mobile VPN service type in which an NGN enterprise network itself provides VPN service. The NGN enterprise network controls the VTF and performs VPN service management and mobility control. However, the access authentication for the remote user is provided by a public NGN service provider, while VPN service authentication is performed through VPN SCF in the NGN enterprise network.

The MUE may require two IP addresses: a persistent IP address and a temporary IP address, as defined in [ITU-T Y.2018] and related ITU-T Recommendations. The persistent IP address is allocated from the enterprise network either statically or dynamically, and the temporary IP address is allocated from the current NGN access network.

The VPN service provisioning between MUE and VTF is performed by VPN SCF in the NGN enterprise network, and the resource control for the VPN service in VTF is performed by the e-RACF in the NGN enterprise network. If the resource control in the transport functions in public NGN is needed for the VPN service, the VPN SCF function in the NGN enterprise network may need to interact with the corresponding function in the public NGN. The detailed interfaces between the control functions in the enterprise network and the ones in NGN are out of scope of this Recommendation.

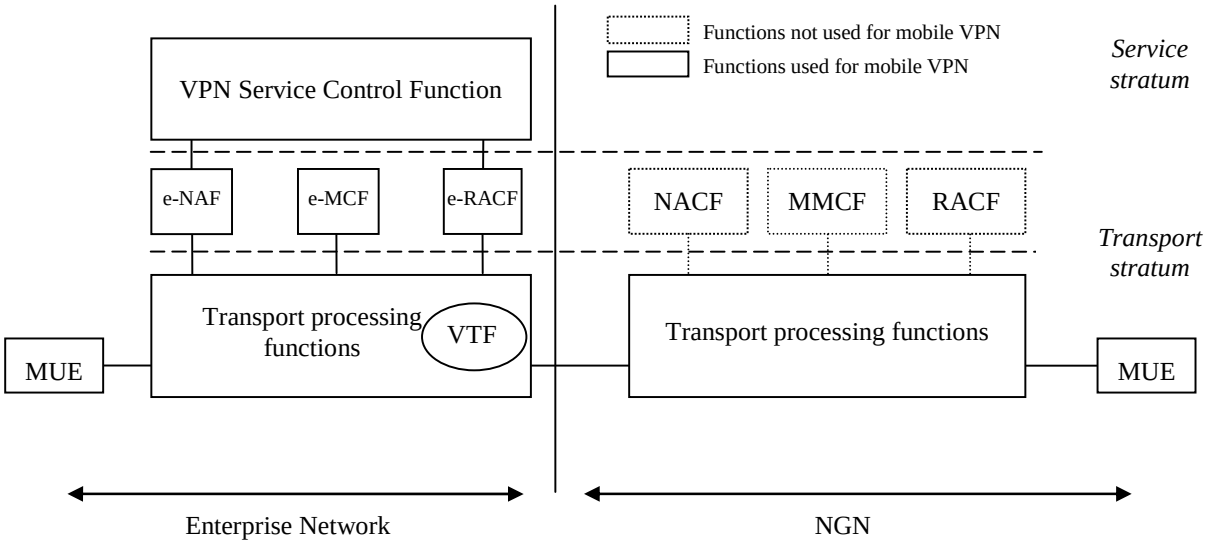

Figure 7-3 – Functional architecture of remote access mobile VPN with enterprise service control

7.2.2 Community-based mobile VPN

This is a mobile VPN service type for the MUEs that want to share information securely with each other. The MUEs themselves are secure tunnel end points. This service, however, may still need VTF in the public NGN for initial data transfer before the direct communication among the multiple MUEs.

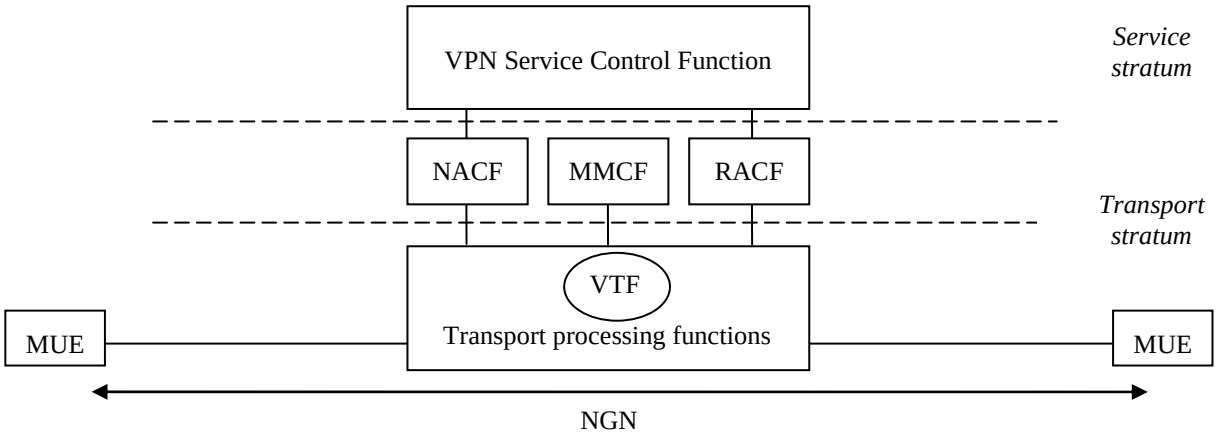

Figure 7-4 – Community-based mobile VPN functional architecture

An MUE creates a secure tunnel, with other MUEs directly and through the VTF as well, which is not associated with a specific enterprise network but open to public for MUEs having common interests to create their own VPN networks, for the secure data communication among them. The MUE will have a persistent IP address which may be allocated at the VPN registration procedure from the network attachment function, and a temporary IP address which is allocated from the current NGN access network. The MUE will interact with MMCF to support the host-based mobility protocol.

7.3 Reference points

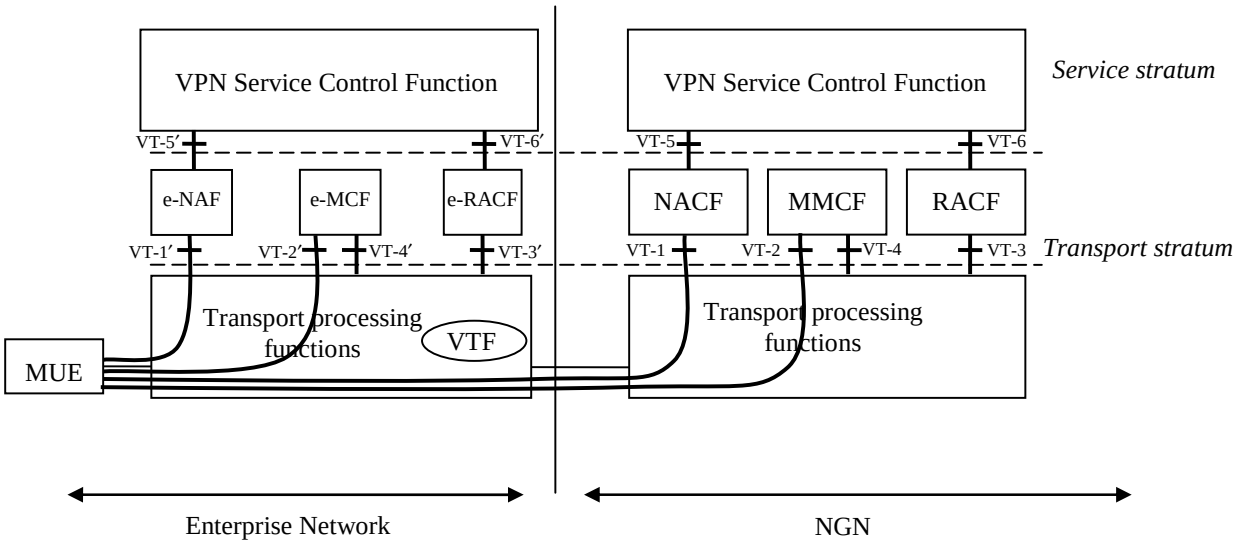

Figure 7-5 – Reference points of the mobile NGN functional architecture

7.3.1 VT-1 reference point

The VT-1 reference point is defined between MUE and NACF. The NACF provides IP addresses (IPv4 or IPv6 addresses) and some configuration information for the MUE in an NGN access network (typically through DHCP) through this reference point. This reference point is also defined for MUE authentication and authorization, and mobile VPN security association including security key exchange. This reference point is mapped to a combination of TU-1 and TC-1, which are defined in [ITU-T Y.2014].

7.3.2 VT-1′ reference point

The VT-1′ reference point is defined between MUE and e-NAF. The e-NAF is a function in an enterprise network which can be matched to NACF in NGN and has the corresponding functionalities as the NACF in NGN. Therefore, the reference point may be defined similarly to the matching NGN reference point, VT-1.

7.3.3 VT-2 reference point

The VT-2 reference point is defined between MUE and MMCF. The MMCF provides a host-based mobility protocol for MUEs in an NGN access network through this reference point. This reference point is mapped to a combination of M3, M4, and M5, which are defined in [ITU-T Y.2018].

7.3.4 VT-2′ reference point

The VT-2′ reference point is defined between MUE and e-MCF. The e-MCF is a function in an enterprise network which can be matched to MMCF in NGN and has the corresponding functionalities to the MMCF in NGN. Therefore, the reference point may be defined similarly to the matching NGN reference point, VT-2.

7.3.5 VT-3 reference point

The VT-3 reference point is defined between transport functions in NGN and RACF. Note that VTF could be controlled via this interface in remote access mobile VPN with managed service from NGN even though it is located in enterprise network. The RACF provides real-time application-driven and policy-based transport resource management in support of end-to-end QoS, gate control, network address translation, and traversal of remote network address translators through this

interface. This reference point is mapped to a combination of Rw and Rc, which are defined in [ITU-T Y.2011].

7.3.6 VT-3′ reference point

The VT-3′ reference point is defined between transport functions and e-RACF. The e-RACF is a function in an enterprise network which can be matched to RACF in NGN and has the corresponding functionalities to the RACF in NGN. Therefore, the reference point may be defined similarly to the matching NGN reference point, VT-3.

7.3.7 VT-4 reference point

The VT-4 reference point is defined between transport functions and MMCF. This reference point is used to activate handover at the related layer 2 and 3 transport functions. This reference point is mapped to a combination of M6 and M7, which are defined in [ITU-T Y.2018].

7.3.8 VT-4′ reference point

The VT-4′ reference point is defined between transport functions and e-MMCF. The e-MMCF is a function in an enterprise network which can be matched to MMCF in NGN and has the corresponding functionalities to the MMCF in NGN. Therefore, the reference point may be defined similarly to the matching NGN reference point, VT-4.

7.3.9 VT-5 reference point

The VT-5 reference point is defined between a service control function and NACF. This reference point is used for the service control function to query geographical location information to NACF. This reference point is mapped to S-TC1, which is defined in [ITU-T Y.2014].

7.3.10 VT-5′ reference point

The VT-5′ reference point is defined between transport functions and e-NAF. The reference point may be defined similarly to the matching NGN reference point, VT-5.

7.3.11 VT-6 reference point

The VT-6 reference point is defined between a service control function and RACF. This reference point is used to authorize and reserve QoS resource for VPN service sessions. This reference point is mapped to Rs, which is defined in [ITU-T Y.2011].

7.3.12 VT-6′ reference point

The VT-6′ reference point is defined between a service control function and e-RACF. The reference point may be defined similarly to the matching NGN reference point, VT-6.

8 High-level mobile VPN procedures

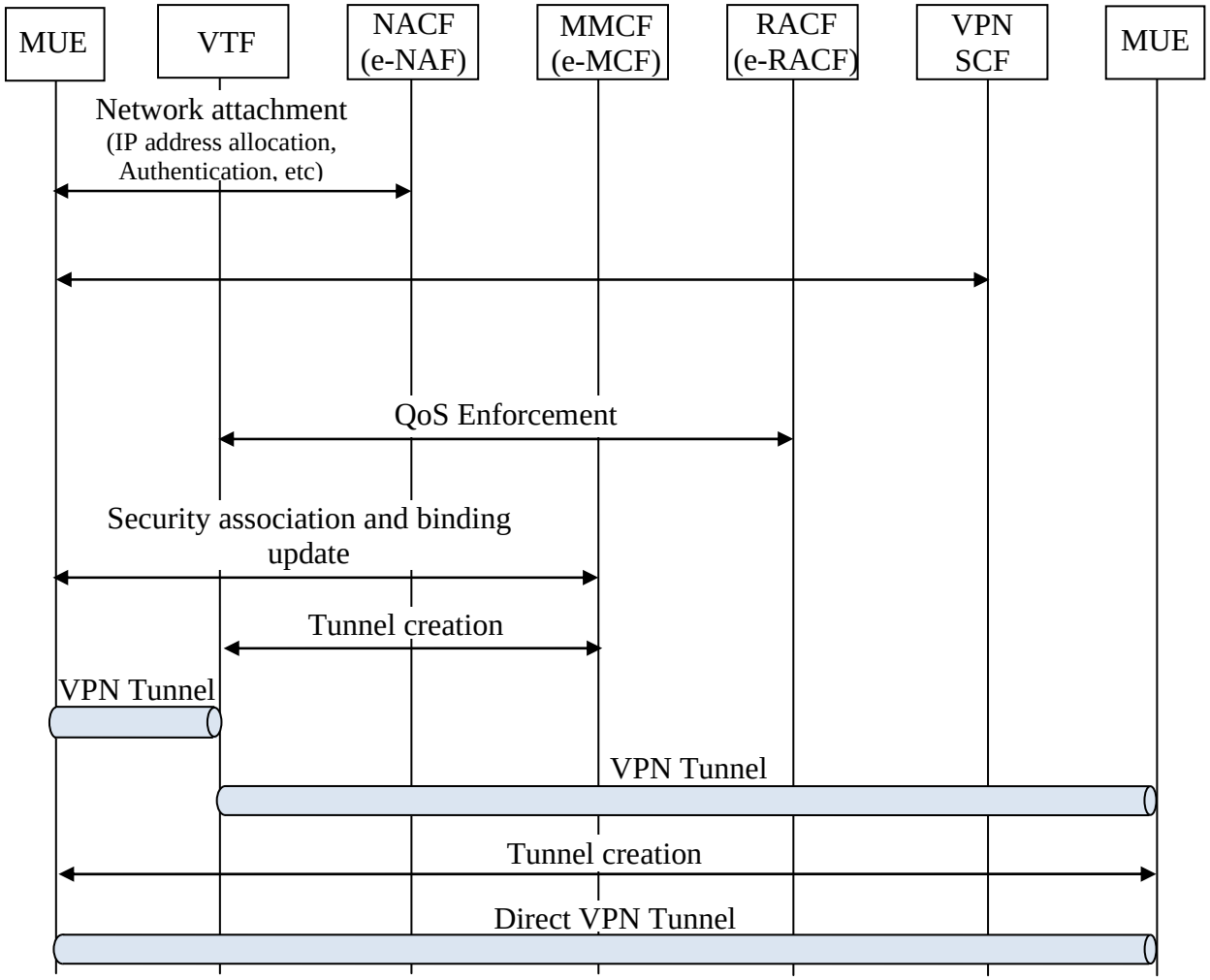

Figure 8-1 – Service registration and initial attachment procedure for mobile VPN service based on host-based mobility protocol

8.1 VPN service registration/de-registration

An MUE should register itself to VPN SCF if it wants to be a member of a VPN. The registered addresses or identifiers of the MUEs should be available to the other nodes (other MUEs and VTF) to create secure VPN tunnels. The MUE could de-register itself from the VPN SCF when it does not want to be a member of the VPN anymore.

8.2 QoS provisioning and enforcement for VPN tunnel

The VPN SCF will trigger RACF (or e-RACF) to provision QoS for the VPN tunnels as the MUE resisters itself to the VPN SCF. Then the RACF (or e-RACF) enforces QoS for VPN tunnels into VTF and related network elements. The VPN SCF will also trigger RACF (or e-RACF) to release QoS for the VPN tunnel as the MUE deregisters itself from the VPN through the VPN SCF.

8.3 Initial network attachment

When an MUE is powered on, it will perform the initial attachment process defined in [ITU-T Y.2014]. Then the host-based mobility (HBM) protocol is used to establish a mobile VPN tunnel between an MUE and a VTF as well as between two different MUEs.

8.3.1 Security association establishment and binding registration

The MUE may support the various key exchange protocols such as IKEv2 [b-IETF RFC 5996] and password authenticated key exchange (PAK) [ITU-T X.1035] for negotiating the security association which will be used for securing mobility control signalling and data packets. The security associations for control packets and data packets are performed independently. The MMCF (or e-MCF) needs to take care of the security association only for control packets in general mobility cases but the MMCF (or e-MCF) for mobile VPN service should take care of the security association for data packets as well. During this security association procedure, the MUE may request the allocation of a persistent IP address or prefix if it is not pre-configured manually or in the service registration procedure.

8.3.2 VPN tunnel creation

After establishing the security association and obtaining the persistent IP address, the MUE should exchange mobility location binding update messages in order to register its persistent IP address and temporary IP address at the mobility location management functional entity (MLM-FE) of MMCF (or e-MCF), if it detects the change of its location. In order to support IP version independent mobility in access networks, the MUE may have multiple persistent IP addresses of different IP versions as well as multiple temporary IP addresses of different IP versions.

When the MMCF (or e-MCF) receives the location binding update from an MUE, it will first set up a secure VPN tunnel to VTF and then send the location binding acknowledgement back to the MUE. If the location binding acknowledgement indicates that the location binding update request is accepted, the MUE should create and manage a binding entry for the persistent IP address and the temporary IP address. After this, a mobile VPN tunnel is established between the MUE and VTF.

8.3.3 Direct VPN tunnel creation

If both communication entities are MUEs, these can create a direct mobile VPN tunnel which does not necessarily go through VTF. The two MUEs should set up a security association between them to establish a direct VPN tunnel which will provide an optimized and secure communication path between the MUEs.

8.4 Handover

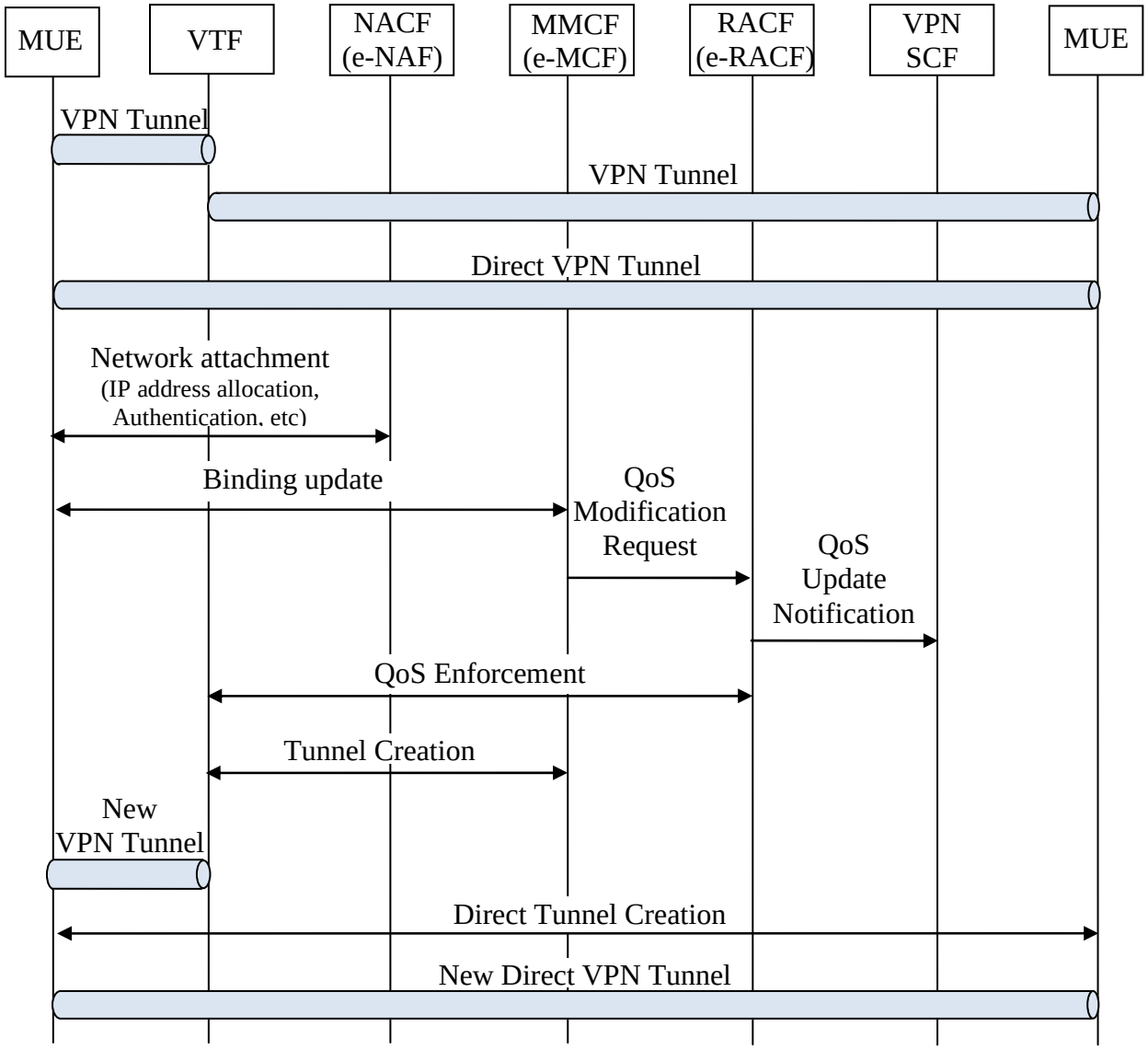

Figure 8-2 – Handover procedure for host-based mobility protocol based mobile VPN

The handover procedure is performed by the MUE according to the HBM protocol to update its temporary IP address to the MMCF (or e-MCF) after detecting a movement between two different access networks, which implies a change of the temporary IP address. When this procedure takes place, the MUE already has a valid registration at the MMCF (or e-MCF), which implies that the MMCF (or e-MCF) has a binding entry for that MUE and a security association to secure HBM protocol signalling is in place between the MUE and the MMCF (e-MCF).

The procedure involves performing the movement detection and exchanging of location binding update and location binding acknowledgement between the MUE and the MMCF (or e-MCF). For the handover procedure, it is assumed that the MUE has already set up a security association with the MMCF (or e-MCF) in the initial attachment procedure described in the previous clause and the security association remains valid even after handover to the other access network.

When the MMCF (or e-MCF) receives the location binding update from the MUE, the MMCF (or e-MCF) will interact with RACF (or e-RACF) to re-provision QoS for the new location and create a new tunnel to VTF. The QoS update information may be notified to VPN SCF to update its QoS provisioning information for the VPN tunnel.

After a new mobile VPN tunnel is created between the MUE and VTF, the MUE will create a new direct tunnel to the corresponding MUE after creating security association between them for an optimized communication path.

9 Security considerations

Basic considerations on security architecture for NGN are addressed in [ITU-T Y.2001], and the security requirements of the NGN are described in [ITU-T Y.2701]. Concerning the specifics of mobile VPN, the various kinds of terminals, devices and contents that can be involved will have to conform to the security requirements of the network to which they are willing to attach. When attaching to the NGN, corresponding authentication and authorization requirements in [ITU-T Y.2702] should be applied.

Appendix I

Use case of mobile VPN based on the IP-based mobility protocol

(This appendix does not form an integral part of this Recommendation.)

I.1 Secure tunnel set up

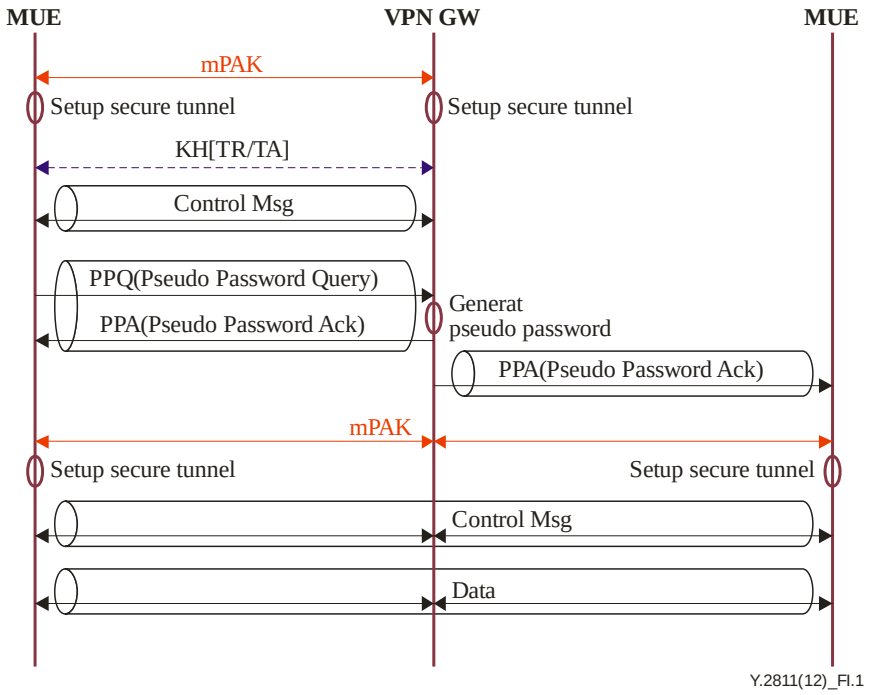

Figure I.1 – Modified PAK-based secure tunnel creation

Figure I.1 shows how the secure tunnel between the MUEs can be set up using modified PAK. The PAK is a protocol to establish a shared secret with a party whose identity has been assured by the password. In this scenario, the original PAK is extended to exchange security policy configuration information between two nodes. Every MUE is assumed to have an ID and password in order to use modified PAK (mPAK). Every MUE should exchange key information with the VPN service control function through the mPAK.

Using the key information and keyed-hash (KH) mechanism, the MUE will set up a tunnel by exchanging tunnel request (TR) and tunnel acknowledgement (TA) messages with the VPN transport function which is normally located in VPN gateway. Through the tunnel, the MUEs and VPN gateway can exchange secure control messages.

Then, MUEs will request a pseudo ID and password using "pseudo password query" and then the VPN service control function will generate a pseudo ID and password for the MUEs. The newly generated pseudo ID and password will be delivered to all the VPN members through the secure tunnels between the VPN transport function (also known as VPN gateway) and MUEs that were already set up.

Then, the MUEs could exchange key information with the other MUEs using their pseudo IDs and passwords through the mPAK.

I.1.1 Key exchange between MUE and VPN gateway

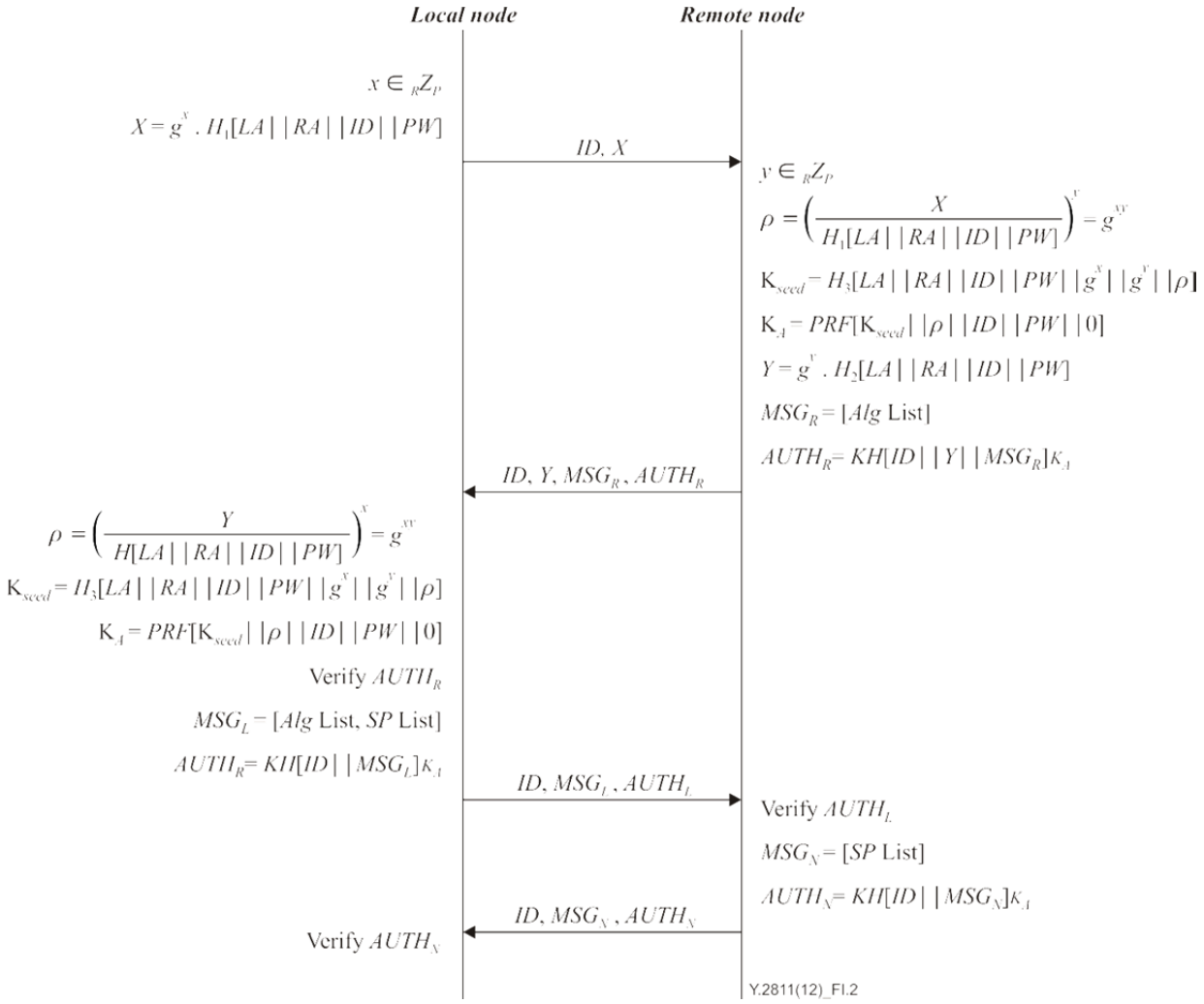

Figure I.2 – Modified PAK algorithm

First, a random number is generated (g^x) from a number set ($_RZ_p$) and the value is multiplied by the hash value of the concatenation of local address (LA), remote node address (RA), MUE's identifier (ID) and password (PW) using a hash function H_1, to finally obtain a value X. This way only the nodes that know the password can calculate the key. Then the local node sends the message including ID and X to the remote node.

If a remote node (VPN gateway or corresponding MUE) receives the message from a local node, it generates a random number (g^y) from a number set ($_RZ_p$). Then, a hash value (K_{seed}) of the concatenation of LA, RA, ID, PW, g^x, g^y and g^{xy} is calculated using a hash function H_3. K_A is obtained by generating a pseudo random number from the concatenation of K_{seed}, ID and PW. The g^y value is multiplied by the hash value of the concatenation of LA, RA, ID and PW using a hash function H_2 to finally obtain a value Y. Finally, a keyed-hash value ($AUTH_R$) is generated using K_A from the concatenation of ID, Y and a security algorithm list (MSG_R) that the remote node can provide. Then, the node sends back the message including ID, Y, MSG_R and $AUTH_R$ to the local node.

The local node again calculates K_{seed} and K_A from the information that it received from the remote node and its password (PW), and verifies the $AUTH_R$. Then, it sends a keyed-hash value ($AUTH_L$) which is generated using K_A from the concatenation of ID and security algorithm and policy list (MSG_L) that the node can support. The node sends back the message including ID, MSG_L and $AUTH_L$ to the remote node.

The remote node sends a keyed-hash value ($AUTH_N$) which is generated using K_A from the concatenation of ID and security policy list (MSG_N) which is decided to be used. Then, the remote node sends the message including ID, MSG_N and $AUTH_N$ to the local node. Finally, the key exchange procedure ends by verifying the $AUTH_N$.

Through this procedure, a local node (MUE) and its remote node (VPN gateway or corresponding MUE) share the key information. The procedure follows the basic procedure in [ITU-T X.1035] and uses the keyed-hash mechanism to protect messages. The following are keys to be used for tunnel set up and control messages after the above procedure.

$K_{tun} = H[K_{seed} || K_A | g^{xy} || ID || PW || 1]$

$K_{ctrl} = H[K_{seed} || K_{tun} | g^{xy} || ID || PW || 2]$

K_{tun} is used as the key to protect tunnel request (TR) and tunnel acknowledge (TA) messages, and K_{ctrl} is used as the key to protect control messages.

I.1.2 Key exchange between MUEs

Once a secure tunnel between MUE and VPN gateway is created, the separate key should be exchanged to set up a direct secure tunnel between two MUEs. Since it is not appropriate to distribute an MUE's password to the others, a temporary ID and password are created for each MUE, which is only temporarily valid for the direct communication between MUEs.

The temporary ID and password are dynamically created for each MUE directly after setting up a tunnel between MUE and VPN gateway. MUEs will request a pseudo ID and password using "pseudo password query" and then VPN service control function will generate a pseudo ID and a password for each MUE. The newly generated pseudo ID and password will be delivered to the entire VPN member MUEs through the secure VPN tunnels between MUEs and VPN gateway functions which were already set up.

Then, the MUEs could exchange key information with the other MUEs using their pseudo IDs and passwords through the mPAK which is described in clause I.1.1.

I.2 Mobility

I.2.1 Mobility for the tunnel between MUE and VPN gateway

In order to support seamless mobility using the IP-based mobility mechanism, multiple interfaces are assumed to support make-before-break handover. One of the interfaces is used for active VPN tunnels and others are used for standby VPN tunnels.

Figure I.3 shows an example with two interfaces. The first interface is chosen to be a primary interface, which is determined the local node's policy or the network's policy. First, a tunnel is created between MUE and VPN gateway. A tunnel ID (TID) value is allocated for the tunnel and the TID value is used when an actual binding is performed. A tunnel is registered as an active tunnel through performing binding registration for the tunnel while setting the BID (binding ID) value to the TID value. As shown in the figure, a tunnel with a TID value of X is used as a primary tunnel for the VPN traffic and a tunnel with a TID value of Y is used as secondary tunnel.

If a handover is needed because of various reasons of the primary tunnel such as signal strength degradation, MUE will switch the secondary tunnel to the primary tunnel by setting BID to the TID of the secondary tunnel.

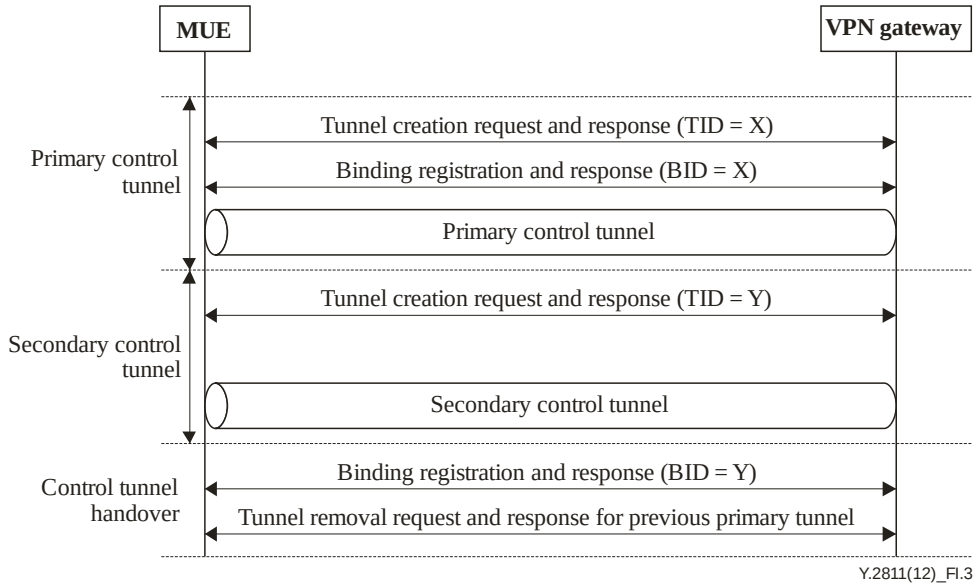

Figure I.3 – Signalling flow for mobility between MUE and VPN gateway

I.2.2 Mobility for the tunnels between MUEs

If multiple MUEs want to communicate through secure VPN tunnels, the MUEs create direct VPN tunnels between them. Before creating the direct VPN tunnel, the primary and secondary control tunnels are created between MUEs and VPN gateway. Once the control tunnels are created, the MUEs can create the direct VPN tunnels with other MUEs that they want to communicate with. If a handover is needed because of various reasons of the primary interface such as signal strength degradation, MUE will hand over the control tunnel as in clause I.2.1. Once the control tunnel is handed over the new interface, the data traffic also passes through the tunnel instead of the through the direct tunnel. And the traffic is again forwarded through the direct tunnel after deleting the old direct tunnel and creating the new direct tunnel through the new primary interface.

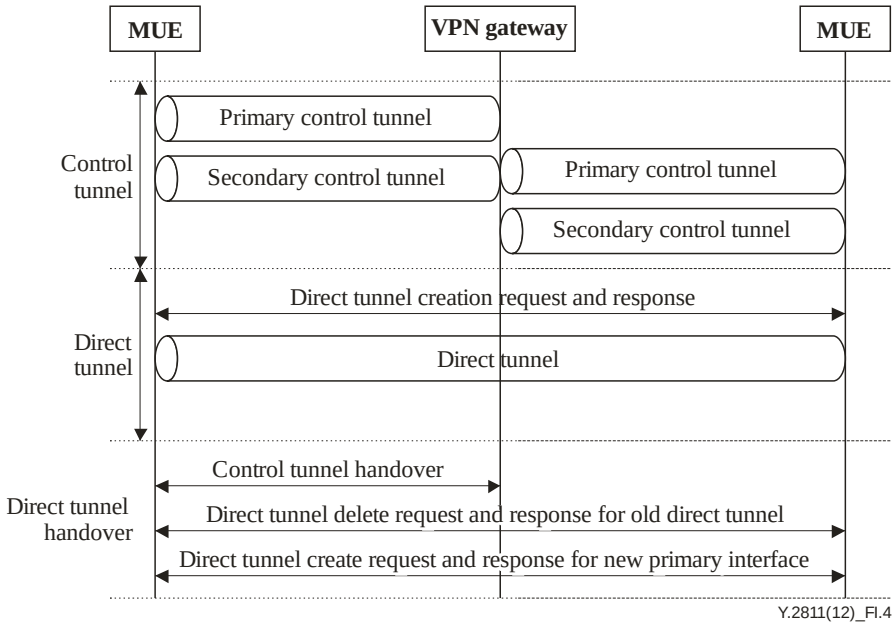

Figure I.4 – Signalling flow for mobility between MUEs

Appendix II

Use case of mobile VPN based on MOBIKE

(This appendix does not form an integral part of this Recommendation.)

The MOBIKE-based mobile VPN provides only the case where an MUE accesses the enterprise resources, but does not provide the case of communication between MUEs.

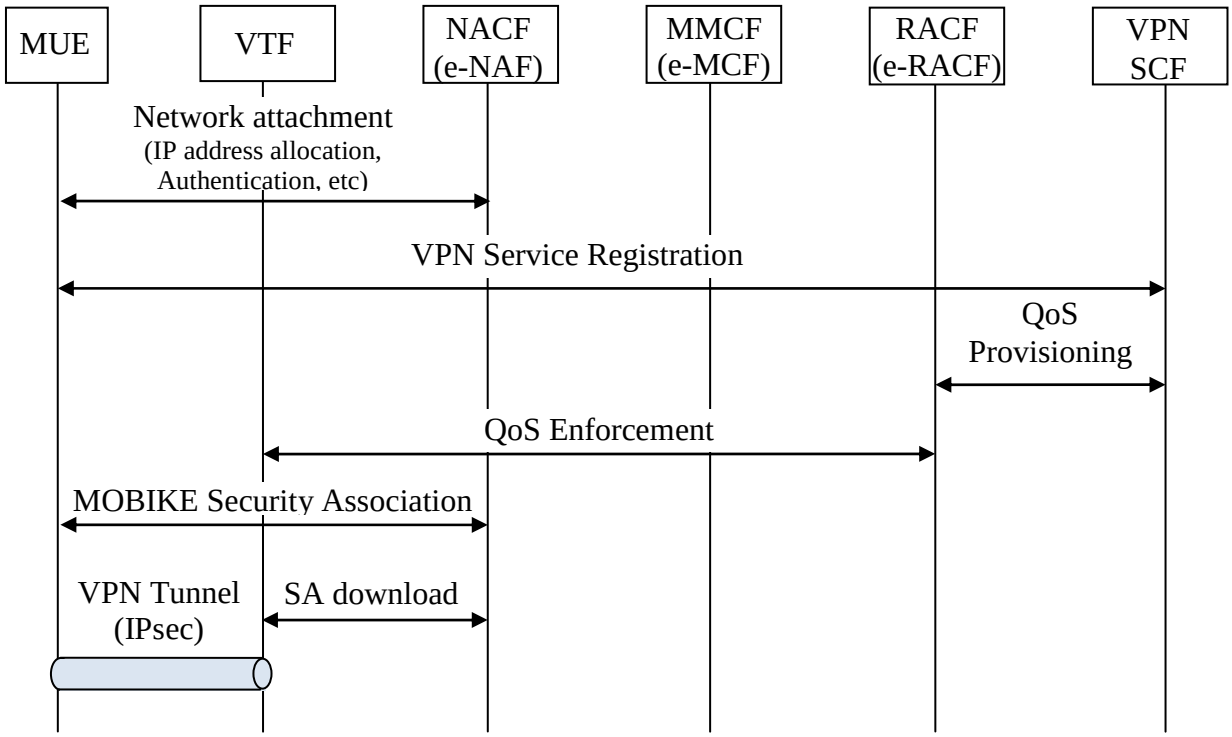

Figure II.1 – Service registration and initial attachment procedure for MOBIKE based mobile VPN

II.1 VPN service registration/de-registration procedure

The VPN service registration/de-registration procedure is basically the same as in mobile VPN service based on host-based mobility protocol.

II.2 VPN tunnel QoS provisioning

When the MUE registers itself to the VPN service control function (VPN SCF), the VPN SCF will trigger PD-FE in RACF to provision QoS for the VPN tunnel. Likewise, when the MUE deregisters itself from the VPN SCF, the VPN SCF will also trigger PD-FE in RACF to release QoS for the VPN tunnel.

II.3 Initial attachment procedure

The MOBIKE initial attachment is performed by the MUE to establish an IPsec tunnel with the tunnelling end-points as described in [b-IETF RFC 4555]. The MOBIKE client and server perform the IKE security association initialization procedure (IKE_SA_INIT) and the IKE authentication procedure (IKE_AUTH) to set up an IPsec tunnel. Once the IPsec tunnel has been established between the MOBIKE client and the VTF, the MUE may start sending and receiving data to/from its enterprise network.

II.4 Handover procedure

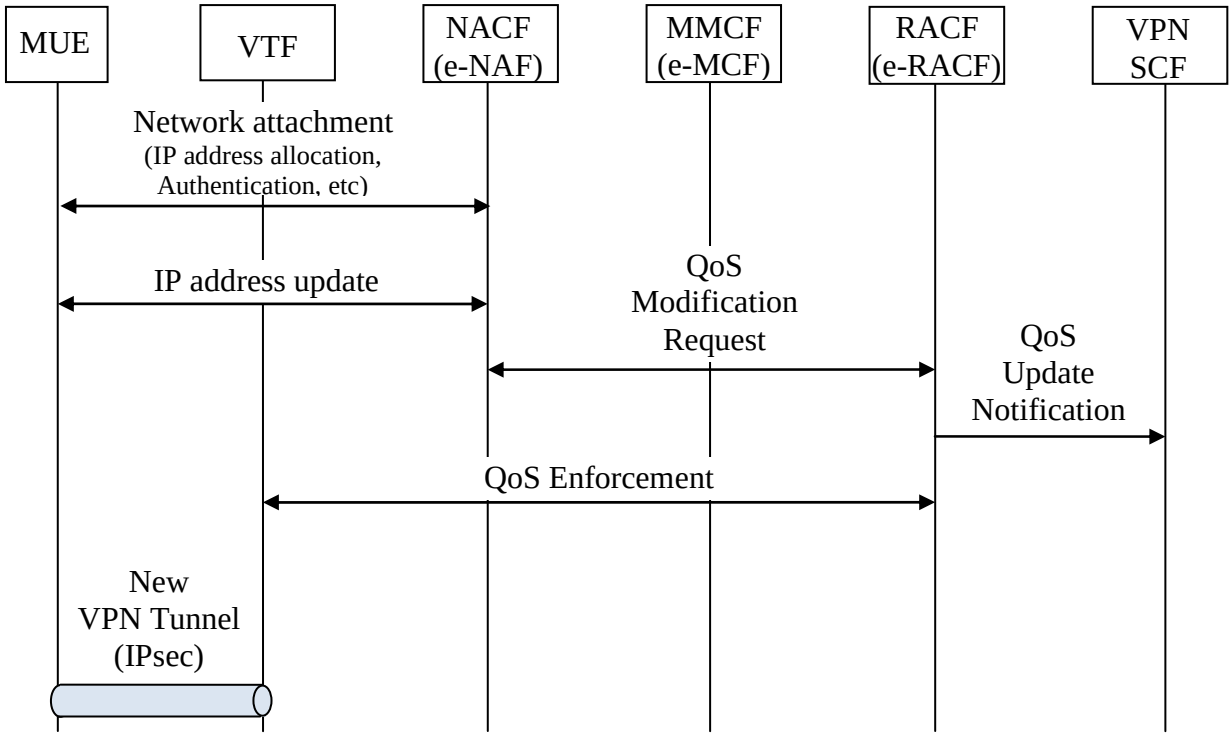

Figure II.2 – Handover procedure for MOBIKE based mobile VPN

While MUE is connected to an access network, if any of the handover conditions is met, such as signal strength degradation, the MUE may hand over to another wireless network. Once the handover decision is made, the MOBIKE client sends an INFORMATIONAL message to VTF to inform that its IP address has been changed. After the INFORMATIONAL message is exchanged, MUE's data traffic is sent and received through the target access network.

As in the initial attachment phase, when the NACF receives a security association request from an MUE, the NACF will interact with PD-FE in RACF to re-provision QoS. Optionally, the QoS update information may be notified to VPN SCF.

Bibliography

[b-IETF RFC 4555] IETF RFC 4555, *IKEv2 Mobility and Multihoming Protocol (MOBIKE)*.

[b-IETF RFC 5996] IETF RFC 5996, *Internet Key Exchange Protocol Version 2 (IKEv2)*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013