INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2005-2008

NGN-GSI

NGN-GSI-C-1285

English only

Original: English

Question(s): 15/13 Geneva, 1-11 September 2008

CONTRIBUTION

Source: ZTE Corporation

Title: Some clarifications for media independent mobility security for NGN

1 Introduction

In the May 2008 meeting, some of the conclusion for "***[C-920]***, *Proposal for initiating the study on IP based mobility security for NGN*" are as "*To this end, the author and others are invited to bring a set of contributions to further develop the concept and outline technical material and delineate the differences with 3GPP work.*". In response to this conclusion, this contribution proposes some clarification for the differences between NGN and 3GPP work in the topic of mobility security.

2 Discussion

2.1 Heterogeneous access systems mobility

3GPP

Figure 1 describes that EPS supports mobility between heterogeneous accesses. The EPS supports service continuity between 3GPP access (E-UTRAN) and non-3GPP access (3GPP2, WiMax, Fixed access) [9].

TSB Note: All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

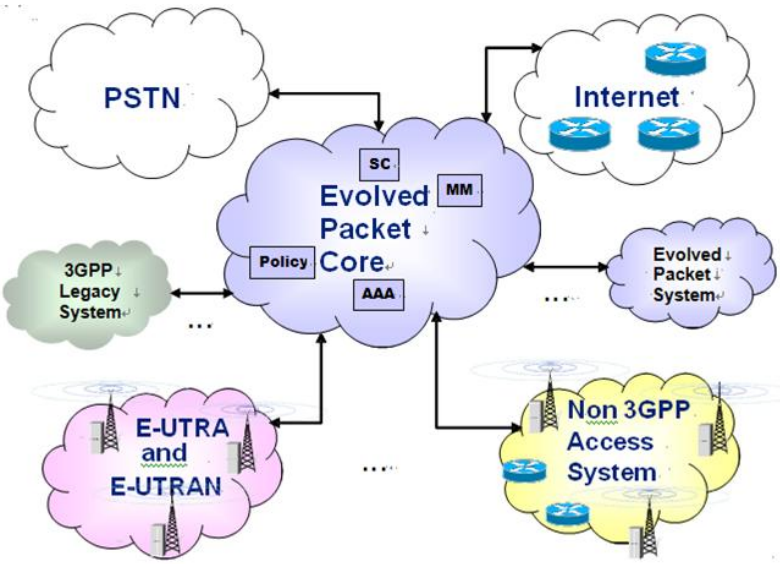

Figure 1 Heterogeneous access system mobility between 3GPP Legacy Systems or E-UTRAN and non 3GPP Access Systems including Fixed Access systems [9]

TS 23.402 [10] specifies mobility management procedures for handling mobility between E-UTRAN and CDMA2000 access, and mobility between 3GPP accesses and WiMax. MIPv4 [17], PMIPv6 [19], and DSMIPv6 [21] are used to support IP based mobility management. TR 24.801 [12] specifies MIH is one of candidate protocols for network discovery and selection.

NGN

Mobility support is one of the features in NGN, which includes normadicity, handover. NGN supports multiple access technologies, such as IEEE 802.11, IEEE 802.16, 3G RAN etc. In NGN R2, handover covers Inter-access networks and Intra-access networks scenarios [2][3][4].

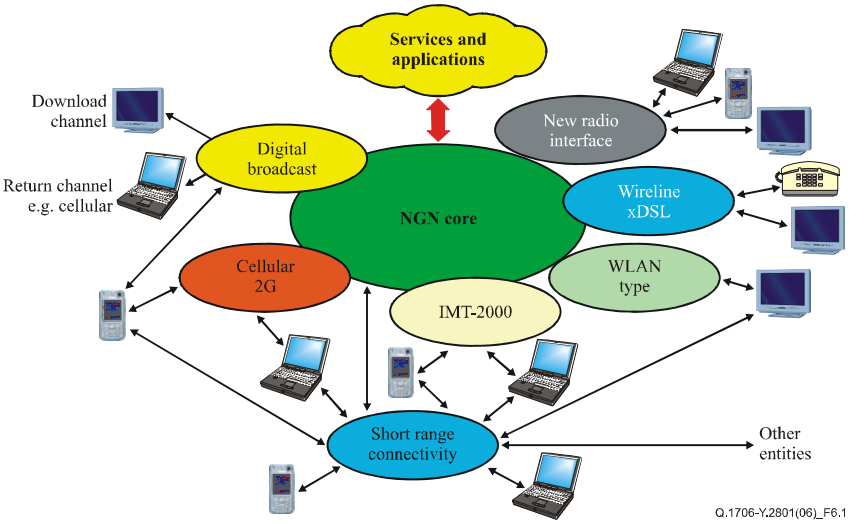

Figure 2 Q.1706/Y.2801 – Envisioned network environment of NGN [1]

Y.MMCF [6] describes mobility management and control functions for NGN. MIPv4 [17], MIPv6 [18], PMIPv6 [19], and HMIPv6 [20] can be used to support IP based mobility management. Handover decision may be based on MIH.

2.2 Trust model

3GPP

Non-3GPP access network has two types: one is trusted access network; the other is un-trusted access network [10][11]. For the trusted case, UE can direct communicate with PDN Gateway (PGW). For the un-trusted case, UE shall communicate with PGW via security gateway (ePDG). As shown in **Figure 3**

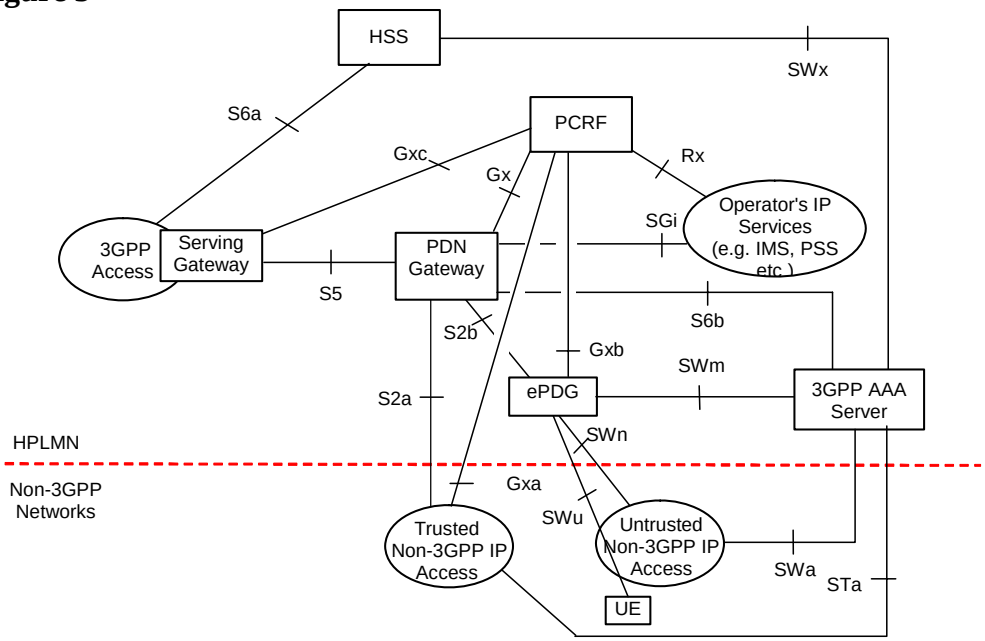

Figure 3 Non-Roaming Architecture within EPS using S5, S2a, S2b [10]

NGN

NGN security trust model defines three security zones: trusted, trusted but vulnerable, un-trusted [7]. As shown in **Figure 4**.

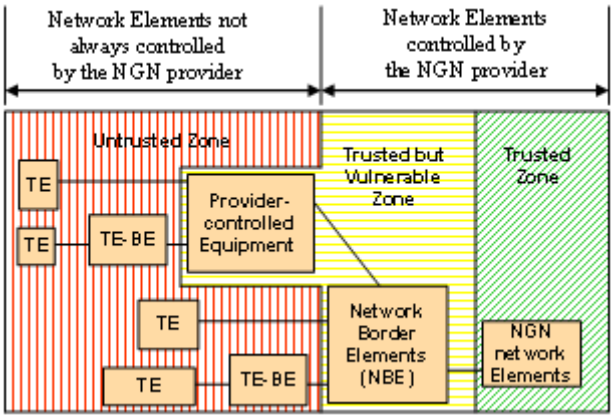

Figure 4 Security trust model [7]

A “trusted zone” is a zone where a NGN provider’s network elements and systems reside and never communicate directly with customer equipment or other domains.

A “trusted but vulnerable zone” is a zone where the network elements are operated by the NGN provider. The elements in this zone communicate with elements both in the trusted zone and with

elements in the un-trusted zone. Their major security function is to protect the NEs in the trusted zone from the security attacks originated in the un-trusted zone.

An "un-trusted zone" that includes all network elements of customer networks or possibly peer networks or other NGN provider domains outside of the original domain, which are connected to the NGN Provider's network border elements.

2.3 Authentication and key agreement

3GPP

Access authentication for non-3GPP access in EPS shall be based on EAP-AKA or EAP-AKA within IKEv2, which EAP-AKA also supports fast re-authentication [11]. AKA algorithm is used to generate MSK.

NGN

In NACF, several access authentication methods are provided, e.g. PPP (EAP), DHCP, PANA (EAP), which is supported by TAA-FE [5].

Identification and authentication mechanisms in Y.secMechanisms are concerning SIP-based service. The mechanisms concerning other services are for further study [8].

Some considerations

For supporting heterogeneous access system mobility, media independent authentication mechanisms are preferable. Some candidate mechanisms are EAP-based methods [22], hokey [16], MPA [14], EAP-IKEv2 [23], which hokey [16] can also support re-authentication, key-derivation.

2.5 IP Mobility Security

3GPP

IP based mobility signalling include MIPv4, DSMIPv6, PMIP in non-3GPP access network.

(1) For MIPv4 security, access authentication based on EAP-AKA is mentioned above, the key EMSK that result from the EAP-AKA authentication procedure is used to derive bootstrapping keys using hokey [16], and the key distribution for MIPv4 is based on RADIUS/Diameter protocol.

(2) For DSMIPv6, EAP-IKEv2 is used for access authentication. The key is retrieved from AAA Server. IPsec ESP protects traffic between UE and PDN GW.

(3) For PMIP, IKE/IPsec is used to protect the mobility signalling.

MOBIKE is used for protecting the IPsec tunnel between UE and ePDG in mobility case.

NGN

Y.MMCF has not formally defined the IP mobility protocol used in the architecture. Some protocols are considered: MIPv4, MIPv6, PMIPv6, and HMIP [6].

Key materials are distributed from TAA-FE to MLMF to protect mobility signalling. Hokey is used for pre-authentication.

Some considerations

Those mobility security mechanisms, such as EAP-IKEv2 [23], MOBIKE [24], etc. should also be applicable to NGN mobility security.

2.6 Security Context Transfer

3GPP

TS 33.402 describes establishment of security context for non-3GPP access system, e.g. CDMA 2000, WiMax [11]. For each access technology, a specific method was developed.

NGN

The mechanisms of security context transfer have not been developed in the context of NGN.

Some Considerations

It is desirable that security context transfer is media independent and optimized. Some candidate technologies are developed in IEEE 8021.21 [13], mipshop [15].

3 Proposal

From the discussion above, it can be see that there exist some differences in the area of mobility security developed in 3GPP and NGN. Among them, media independent mobility security is one of distinct features in NGN, which is not covered in 3GPP.

It is proposed that Q.15/13 to consider whether it is necessary to study the topic of "media independent mobility security in NGN".

Abbreviations

DHCP	Dynamic Host Configuration Protocol
DSMIP	Dual-Stack MIP
EAP	Extensible Authentication Protocol
EPS	Evolved Packet System
HMIP	Hierarchical mobile IP
IKE	Internet Key Exchange
MIP	Mobile IP
MMCF	Mobility management and control framework
MSK	Master Session Key
PANA	Protocol for Carrying Authentication for Network Access
PDG	Packet Data Gateway
PDN	Packet Data Network
PGW	PDN Gateway
PMIP	Proxy MIP
PPP	Point-to-Point Protocol

References

[1] ITU-T Recommendation Q.1706/Y.2801 (2006), Mobility management requirements for next generation networks.

[2] ITU-T Draft Supplement, NGN release 2 scope

[3] ITU-T draft Recommendation Y.NGN-R2-Reqts, "Requirements and capabilities for ITU-T NGN release 2"

[4] ITU-T Draft Recommendation Y.NGN-FRA R2, functional requirements and architecture of the NGN of release 2

[5] ITU-T Recommendation Y.NACF R2, Network attachment control function in Next Generation Networks (release 2)

[6] ITU-T Recommendation Y.MMCFArch, "Mobility management and control functions in the NGN"

[7] ITU-T Recommendation Y.2701, “Security requirements for NGN release 1”

[8] ITU-T Draft Recommendation Y.secMechanisms, NGN security mechanisms and procedures

[9] 3GPP TS22.278 Service requirements for the Evolved Packet System (EPS)

[10] 3GPP TS23.402 Architecture enhancements for non-3GPP accesses

[11] 3GPP TS 33.402 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses

[12] TR 24.801 3GPP System Architecture Evolution (SAE); CT WG1 aspects

[13] IEEE 802.21 Media Independent Handover Services

[14] IRTF draft, draft-irtf-mobopts-mpa-framework-03, A Framework of Media-Independent Pre-Authentication (MPA) for Inter-domain Handover Optimization

[15] IETF WG mipshop, http://www.ietf.org/html.charters/mipshop-charter.html

[16] IETF WG hokey, http://www.ietf.org/html.charters/hokey-charter.html

[17] IETF RFC3344, IP Mobility Support for IPv4

[18] IETF RFC3775, Mobility Support in IPv6

[19] IETF RFC5213, Proxy Mobile IPv6

[20] IETF RFC4140, Hierarchical Mobile IPv6 mobility management (HMIPv6)

[21] IETF Internet-Draft, Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6), draft-ietf-mip6-nemo-v4traversal-06.txt

[22] IETF RFC3748 Extensible Authentication Protocol (EAP).

[23] IETF RFC5106 The Extensible Authentication Protocol-Internet Key Exchange Protocol version 2 (EAP-IKEv2) Method

[24] IETF RFC4555, IKEv2 Mobility and Multihoming Protocol (MOBIKE)

_____