Source:	**Huawei Technologies CO., LTD / CWTS**
Title:	Update Proposal on Security Domain
Document for:	Discussion / Decision
Agenda Item:	

1 Introduction

A problem on security domain in NDS/IP model is pointed out and a corresponding update is proposed in this proposal.

2 Analysis

2.1 Background

In TS of NDS/IP, the statements on security domain are as the following

(1) In section 4.1:

"The scope of this section is to outline the basic principles for the network domain security architecture. A central concept introduced in this specification is the notion of a network security domain. The security domains are networks that are managed by a single administrative authority. Within a security domain the same level of security and usage of security services will be typical. Typically, a network operated by a single operator will constitute one security domain although an operator may at will subsection its network into separate sub-networks and hence separate security domains."

(2) In section 4.4.1:

"The UMTS network domain shall be logically and physically divided into security domains. These control plane security domains may closely correspond to the core network of a single operator and shall be separated by means of security gateways." (Here, security gateway is referred to SEG)"

In table 1, Za interface is defined as " Network domain security interface between SEGs. The interface is used for both the negotiation of security associations and for the set-up of ESP protected tunnels between SEGs (no third party negotiation)."

(3) In section 5.6.2:

"**Za-interface (SEG-SEG)**

The Za-interface covers all secure IP communication between security domains. The SEGs uses IKE to negotiate, establish and maintain a secure tunnel between them. Subject to roaming agreements, the inter-SEG tunnels would normally be available at all times, but they can also be

<u>established as needed.</u> The tunnel is subsequently used for forwarding secured traffic between security domain A and security domain B.
<u>One SEG can be dedicated to only serve a certain subset of all roaming partners.</u> This will limit the number of SAs and tunnels that need to be maintained. The number of SEGs within a network will normally be limited and should normally not be larger than the numer og BGs in the network. "

2.2 Analysis

Please note the underlined statements. Clearly, there are some problems with it. If an operator subsections its 3G network into separate sub-networks, hence it owns some separate security domains. The SEGs shall be used for protection between these security domains.
Hence, it seems incorrect that these SEGs are subject to roaming agreement. The security relation between these SEGs should be defined by the operator who owns them. It may be independent of roaming agreement.
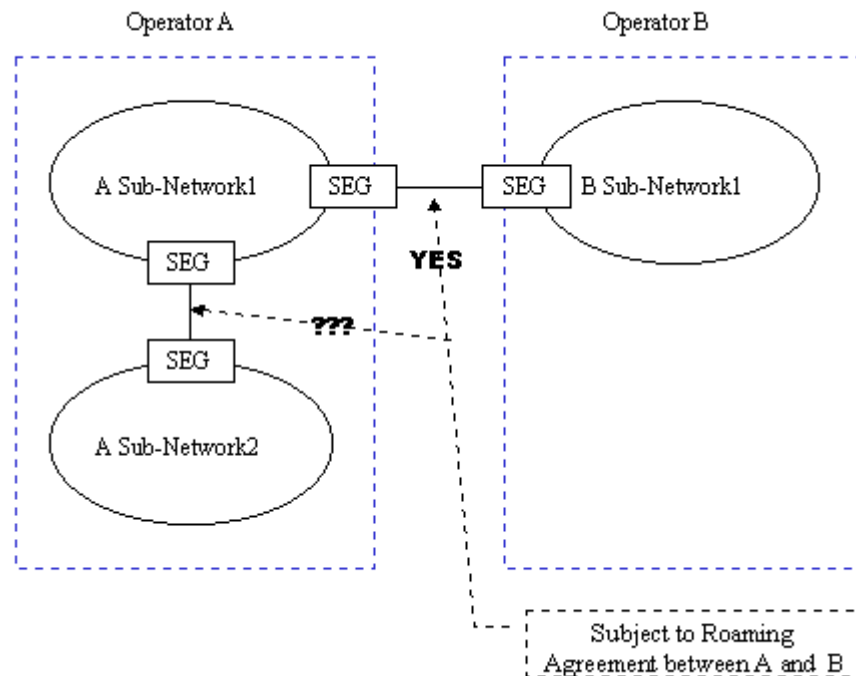

Figure 1, SEGs between security domains

2.3 Solutions

We suggest updating the statement in section 4.1.

 "……, Typically, a network operated by a single operator will constitute one security domain although an operator may at will subsection its network into separate sub-networks ~~and hence separate security domains.~~"

3 Conclusions

A problem on security domain in NDS/IP model is pointed out and a corresponding update is proposed in this proposal.

	CR-Form-v3
CHANGE REQUEST	

⌘	**33.XXX** CR **CR-Num** ⌘ rev **-** ⌘ Current version: **0.5.0** ⌘

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

Proposed change affects: ⌘   (U)SIM ☐   ME/UE ☐   Radio Access Network ☐   Core Network ☒

Title:	⌘	Update on statement for security domain		
Source:	⌘	Huawei Technologies CO,.LTD / CWTS		
Work item code: ⌘		Security	***Date:*** ⌘	8/08/2001
Category:	⌘ **F**		***Release:*** ⌘	R5

Use one of the following categories:	*Use one of the following releases:*
F (essential correction)	2 (GSM Phase 2)
A (corresponds to a correction in an earlier release)	R96 (Release 1996)
B (Addition of feature),	R97 (Release 1997)
C (Functional modification of feature)	R98 (Release 1998)
D (Editorial modification)	R99 (Release 1999)
Detailed explanations of the above categories can	REL-4 (Release 4)
be found in 3GPP TR 21.900.	REL-5 (Release 5)

Reason for change:	⌘	The statement that "Typically, a network operated by a single operator will constitute one security domain <u>although an operator may at will subsection its network into separate sub-networks and hence separate security domains</u>" in section 4.1 is conflicting with the idea that Za interface (SEG-SEG) is subject to roaming agreement in other place such as the statement about Za interface in section 4.4.1.
Summary of change: ⌘		Alignment of concept
Consequences if not approved:	⌘	Inconsistent in specification and easy misunderstanding.

Clauses affected:	⌘	4.1 Introduction
Other specs Affected:	⌘ ☐	Other core specifications ⌘
	☐	Test specifications
	☐	O&M Specifications
Other comments:	⌘	

How to create CRs using this form:

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

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

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

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

4 Overview over UMTS network domain security for IP based protocols

4.1 Introduction

The scope of this section is to outline the basic principles for the network domain security architecture. A central concept introduced in this specification is the notion of a network security domain. The security domains are networks that are managed by a single administrative authority. Within a security domain the same level of security and usage of security services will be typical. Typically, a network operated by a single operator will constitute one security domain although an operator may at will subsection its network into separate sub-networks and hence separate security domains.