3GPP TSG SA WG3 Security — S3#20 **S3-010427r**

16-19 October, 2001

Sydney, Australia

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)"

(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 established as needed. The tunnel is subsequently used for forwarding secured traffic between security domain A and security domain B.
One SEG can be dedicated to only serve a certain subset of all roaming partners. 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, a question occurs that these SEGs be subject to roaming agreement. Clearly, the answer is NO, because it should be the operator who defines the security policy in force on these SEGs. It is independent of roaming agreement.

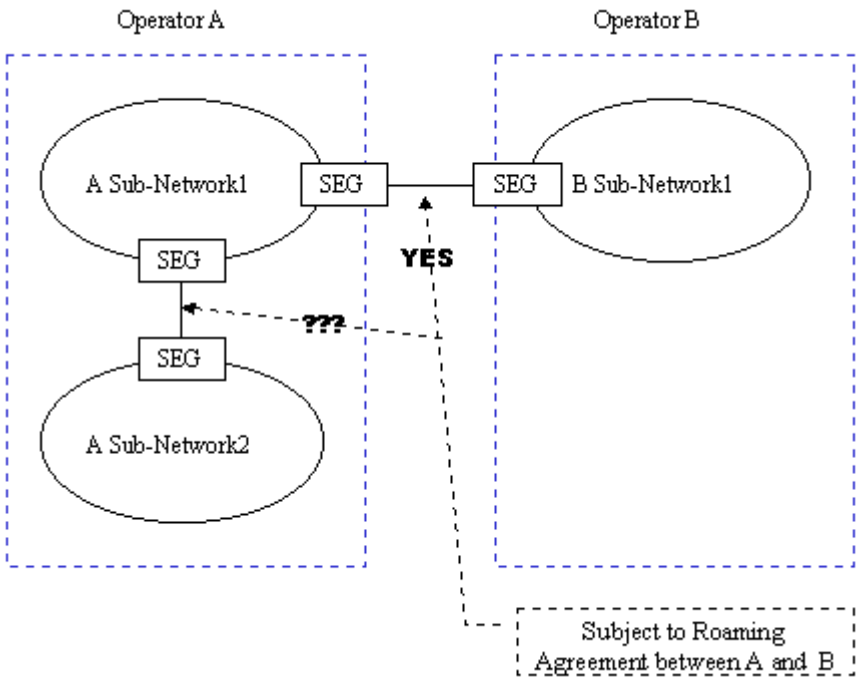

Figure 1, SEGs between security domains

2.3 Solutions

We suggest that:

(1) Update 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.~~”

(2) The concept of NE needs to be clarified and be added to section 3.1.

Network Element: an individual network equipment or a sub-network which is considered be secure by an operater.

3 Conclusions

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

3GPP TSG SA WG3 Security — S3#20 **S3-010XXX**

16-19 October, 2001

Sydney, Australia

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:
- ***F*** *(essential correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(Addition of feature),*
- ***C*** *(Functional modification of feature)*
- ***D*** *(Editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	(1) The statement that "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" in section 4.1 is conflict 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. (2) The concept of NE should be clarified for easy understand
Summary of change:	⌘	Alignment of concept
Consequences if not approved:	⌘	Inconsistent in specification and easy misunderstand

Clauses affected:	⌘	4.1 Introduction 3.1 Definitions
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~~.

3 Definitions, symbols and abbreviations

3.1 Definitions

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

Anti-replay protection: Anti-replay protection is a special case of integrity protection. Its main service is to protect against replay of self-contained packets that already have a cryptographical integrity mechanism in place.

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data integrity: The property that data has not been altered in an unauthorised manner.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

Network Element: an individual network equipment or a sub-network which is considered to be secure by an operater.

Security Association: A unidirectional logical connection created for security purposes. All traffic traversing an IPsec SA is provided the same security protection. The IPsec SA itself is set of parameters to define a unidirectional security protection between two entities. An IPsec Security Association includes the cryptographic algorithms, the keys, the duration of the keys, and other parameters.

Transport mode: Mode of operation that primarily protects the payload of the IP packet, in effect giving protection to higher level layers

Tunnel mode: Mode of operation that protects the whole IP packet by tunnelling it so that the whole packet is protected