3GPP TSG SA WG3 Security — S3#37 **S3-050035**
February 21 - 25, 2005
Sophia Antipolis, France

Source: ZTE Corporation

Title: security architecture of early IMS

Document for: Discussion and decision

Agenda Item: early IMS

1 Introduction

In current specification of early IMS, there is not a security architecture figure to describe the security relationship among the network entities. It is necessary to include an architecture of early IMS security in TS 33.878 specification. The architecture of early IMS security is discussed in this paper. We propose to add the architecture in TS 33.878 specification.

2 Architecture of early IMS security

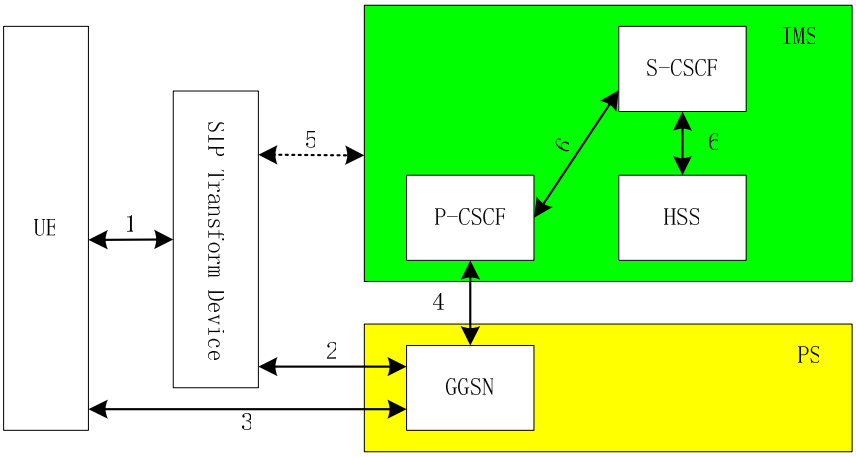

Figure 1: Architecture of early IMS Security

Architecture of early IMS security is shown in Figure 1. The network entities are described as follows:

(1) UE: An UE may support SIP or not.

(2) SIP Transform Device: In current specification, UE must support SIP. However, it should be taken into account in early IMS that UE without SIP module can access the IMS service. A SIP

Transform Device can transform other message into SIP message so that the UE without SIP module can access the IMS service. The SIP Transform Device should support the security mechanism of early IMS. It should support GGSN to perform source IP address spoofing check. We can set following rules in SIP Transform Device to support the early IMS security mechanism:

a) the IMS identity of UE is included in SIP message
b) the IP source address in IP packet which is sent by SIP Transform Device should be the IP address of UE
c) the value of "send by" in SIP message should be IP address of UE

(3) GGSN: GGSN performs the source IP check.

(4) IMS: The network entities should support the early IMS security mechanism.

There are six different security associations and different needs for security protection in security architecture of early IMS and they are numbered 1, 2, 3, 4, 5 and 6 in figure 1 where:

1. Provides the security protection of message exchanged between UE and SIP transform device. The security mechanism may be out of early IMS specification.

2. Provides to check the binding between the IP address that the GGSN allocated the UE in the PDP context activation and the source IP address in subsequent packets.

3. Provides security in GPRS bearer level

4. Provides security between SIP capable nodes. This security association is covered by TS 33.210.

5. Provides to check the binding between the IP address on the bearer level, and the user identities.

6. Provides security within IMS. This security association is covered by TS 33.210.

3 Proposal

Security architecture of early IMS is beneficial to future study of early IMS. We propose SA3 to consider the security architecture presented in paper. A related CR implementing change is also provided.