3GPP TSG SA WG3 Security — SA3#37 **S3-050097**
February 21-25, 2005 **(response to S3-050053)**
Sophia Antipolis, France

Source: Qualcomm

Title: Alternative approach to 2G GBA

Agenda item: 6.9.1 (GAA)

Document for: Discussion/Decision

1 Introduction

In [1], Nokia introduce an approach to extend GBA [2] to subscriptions based on SIM, noting the wide deployment of SIMs in the market today. This response contribution proposes alternate cryptographic principles for consideration.

2 2G GBA

We propose to agree the key Ks by means of mutually authenticated Diffie-Hellman. It is assumed that the UE is provisioned with some server certificate enabling the UE to establish TLS sessions with the BSF or by means of a digital signature, as is assumed below:

1. The BSF receives a GSM triplet (RAND,SRES,Kc) from the HSS. It then computes a Diffie-Hellman public value g^x and sends (RAND,g^x,SIG) to the UE. Here SIG is some digital signature over RAND and g^x.
2. The UE verifies from SIG that the challenge comes from the BSF, and passes RAND to the SIM to retrieve SRES and Kc. It then computes a Diffie-Hellman g^y and sends (g^y,MAC) to the BSF, where MAC is some MAC of g^y keyed with SRES and Kc.
3. The BSF verifies MAC using SRES and Kc, and sends an OK message to the UE.
4. The BSF and UE now agree on Ks=Hash(g^(xy))

Thus the UE and BSF agree Ks based on SIM credentials. Provided the BSF uses fresh triplets, there is no requirement for the UE to remember which RANDs were used during the bootstrapping procedure, and the approach is not vulnerable to man-in-the-middle attacks provided the terminal does not support A5/2. (Note that SRES and Kc are used only as short-term keys, so it is assumed that the BSF may set a policy that the (g^y,MAC) response must be received in less time than it would reasonably take to break A5/1.)

3 Conclusion & Proposal

There are potential security benefits to using mutually-authenticated Diffie Hellman for key agreement between UE and BSF, and it is proposed that SA3 consider the feasibility of this alternative in the event that there is support for a 2G GBA work item.

References

[1] S3-050053, Introducing 2G GBA, 3GPP SA3#37, Nokia.

[2] 3GPP TS 33.220 "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".