3GPP TSG SA WG3 Security — S3#28 **S3-030260**
6 - 9 May 2003
Berlin, Germany

Source: **QUALCOMM Europe**

Title: **Network Authentication Failure in 33.203**

Document for: **Discussion and Decision**

Agenda Item: **7.1**

Abstract

This contribution raises a concern of a potential denial of service attack arising in 33.203 because an I-SCF clears registration information upon network authentication failure.

Network authentication failure in TS 33.203

The concern is raised of a possible denial-of-service attack arising from 6.1.2.2 of TS 33.203 causing the I-CSCF to clear registration information of a legitimate, registered IMPI: an attacker attempts to register, responding with an SM7 purporting to be the legitimate user and indicating an AuthenticationFailure. (Note as per 7.3.1.2 that integrity protection is not applied in the event of Network authentication failure as the UE cannot derive an IK.) The I-CSCF proceeds to clear any registration information related to the legitimate IMPI.

Therefore, the I-CSCF should not clear registration information in the event of Network Authentication Failure.