3GPP TSG SA WG3 Security — S3#23 **S3-020205**

14-17 May 2002

Victoria, BC, Canada

Source: **QUALCOMM**

Title: **Comment on R2 Group Release Security Solution**

Document for: **Discussion**

Agenda Item: **T.B.D.**

S3-020178 (R2-020797) proposes a mechanism whereby a "group release" message may be authenticated. Initially, a message containing a group release indicia is sent to the mobile and stored. When the Group Release Key is sent in a subsequent message, the mobile checks to see whether the provided key can be used to authenticate the "indicia" message, and if it can, proceeds to do the release.

The proposed authentication mechanism seems to be reasonable, using *Kasumi* to encrypt a known quantity U_RNTI (repeated twice to form a 64-bit block) using the newly revealed key to match the "indicia".

For three reasons, Qualcomm proposes a slight modification to this scheme. We would prefer that, instead of using *Kasumi* directly, the message authentication function *f9* should be used, with constant values for the other required inputs to *f9*. These reasons are:

1. The required functionality is that of message authentication, not encryption.
2. Some manufacturers may have chosen to implement *f8* and *f9* as hardware units without directly exposing the functionality of *Kasumi*.
3. No direct interface to *Kasumi* is revealed in any existing standards, requiring significant alterations to documents.