**3GPP TSG SA WG3 Security — S3#13** **S3-000369**

**24-26 May, 2000, Yokohama, Japan**

**From:** **TSG SA WG3**

**To:** **ETSI SAGE**

**Copy:** **AHAG, GSMA SG**

**Title:** **Draft LS on consideration of SHA-1 for 3GGP(1) Authentication by ETSI SAGE**

**Contact**: Frank Quick, Vice-Chair TIA TR-45 Ad Hoc Authentication Group (AHAG)
E-mail: fquick@qualcomm.com
**Tel: +1-858-658-3608**

TSG SA WG3 has received and reviewed an input from AHAG, about the possible use of SHA-1 for the 3GPP(1) authentication algorithm. The document represents the latest proposal on the use of SHA-1 as a hash function in AKA.

SAGE is asked to consider this input when deciding on the possible (example) algorithms for 3GPP(1) authentication, as AHAG will be standardising on the use of SHA-1 for their standards, therefore optimising harmonisation efforts

The authors of the document are available for comments or clarifications, if required.

**Attached:**

| NUMBER | TITLE | SOURCE |
|---|---|---|
| S3-000315 | Use of SHA-1 for AKA f0-f5 | AHAG (F Quick) |