**3GPP TSG SA WG3 Security — S3#12** **S3-000237**

**11-14 April, 2000, Stockholm, Sweden**

Technical Specification Group Services and System Aspects ***TSGS#7(00)0156***
Meeting #7, Madrid, Spain, 15-17 March 2000

| | |
|---|---|
| **Source:** | **3GPP TSG SA (drafting person)** |
| **Title:** | **DRAFT LS to GSM-A on Authentication Algorithm** |
| **Document for:** | **Decision** |
| **Agenda Item:** | **5.3** |

---

## Liaison Statement

| | |
|---|---|
| **To:** | **GSM Association** |
| | **GSM Association Security Group** |
| **From:** | **3GPP TSG SA** |
| **Subject:** | **3G Authentication Algorithm** |

TSG SA would like to inform the GSM Association that at its recent meeting TSG SA endorsed a proposal from TSG SA WG3 (Security Aspects) to develop a standard Authentication Algorithm for use in 3G networks by 3G operators.

TSG SA is aware that earlier indications from 3GPP has suggested that such an algorithm would not be developed within the auspices of 3GPP, however recent discussions have lead SA3 to believe that this would be the appropriate way forward, not least for the purpose to ensure that a strong and secure algorithm would be available world wide to any operator that would want to use it. It does not preclude, of course, that individual operators may chose to use a different algorithm, typically developed in-house by the operator itself. It is also to be noted that the standard algorithm will include an operator specific part allowing operators to differentiate themselves and thus potentially increase the security.

TSG SA is however of the understanding that the GSM Association may be in the process of starting development of an authentication algorithm for 3G, and is therefore keen on making sure that parallel development work is not launched.

The GSM Association is thus asked to confirm whether or not this is the case, and if so then to ensure that the GSM-A Security Group and TSG SA WG3 co-operate on this issue.

In addition, to ensure that highest possible level of security is ensured in networks around the world, TSG SA intends to make a statement somewhere in its specifications that as a minimum the standard algorithm should be used and that individually developed and used algorithms should therefore be at least as strong as the standard one. The GSM Association is asked to pursue a similar encouragement throughout its membership.

Finally, the preliminary time schedule for the algorithm development points at a delivery date in September 2000 however that is dependent on funding of approximately 200 kEuro being available. This funding has not yet been cleared in 3GPP.