**3GPP TSG SA WG3 Security — S3#22** **S3-020063**

**25 - 28 February 2002**

**Bristol, UK**

**Source:** **Siemens Atea**

**Title:** **A3/A8 based on Milenage**

**Document for:** **Discussion**

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

---

**Abstract**

*This contribution proposes a way to develop a new A3/A8 algorithm, based on the MILENAGE algorithm set. It is proposed that the conversion functions c2/c3, as specified in TS 33.102, are applied on the output of MILENAGE.*

# 1) Introduction

During SA3#21 in Sophia Antipolis, Charles Brookson reported that the COMP128-2 algorithm (generates a 54-bit Kc and is used as A3/A8 algorithm in GSM) has been upgraded to a COMP128-3 version to generate a 64-bit Kc. The following table contains a list of known A3/A8 version from the GSM-association.

| Algorithm identification | Characteristics |
|---|---|
| COMP128-1 | Officially secret, but code is available on the internet, should not be used anymore because flawed. |
| COMP128-2 | 54-bit Kc key, secret algorithm |
| COMP128-3 | 64-bit Kc key, secret algorithm |

Charles Brookson also mentioned that the GSM Association reserved some money to develop a A3/A8 algorithm based on Milenage. He added that this work may start after the A5/3-development has been finished.

# 2) Proposed way forward for defining an A3/A8 algorithm based on Milenage

This new A3/A8 algorithm code shall be made publicly available, which is not the case for the current versions of A3/A8 as listed in the table. It is therefor also proposed that the naming of this algorithm shall not be COMP128-x, to clearly indicate that there is a difference with the predecessors.

The new A3/A8 version based on Milenage can easily be defined in the following way:

- The 64-bit Kc is obtained by applying c3 on the output of f3 and f4 of Milenage
  - [TS 33.102] c3: $Kc_{[GSM]} = CK_1$ xor $CK_2$ xor $IK_1$ xor $IK_2$
- The SRES is obtained by applying c2 on the output of f2 of Milenage
  - [TS 33.102] c2: $SRES_{[GSM]} = XRES^*_1$ xor $XRES^*_2$ xor $XRES^*_3$ xor $XRES^*_4$

The advantageous are obvious:

- This code of this A3/A8-version is already publicly available: Milenage is based on Rijndael which did undergo a public review, the Milenage algorithm specification [Milenage] is public and the conversion functions are used in GSM/UMTS interworking and available to everyone. Therefor no algorithm secrecy exists.
- Both AuC and Card-manufactures can rely on already available running code for the implementation of this A3/A8 version.

# 3) 3GPP clarification needed towards the use of Milenage outside of 3G.

The 3GPP webside [3GPP] currently contains following text on the use of Milenage:

> *The 3GPP authentication and key generation functions (MILENAGE), have been developed through the collaborative efforts of the 3GPP Organizational Partners.*
>
> *They may be used only for the development and operation of 3G Mobile Communications and services. There are no additional requirements or authorizations necessary for these algorithms to be implemented.*

This statement should be adapted if it is allowed to use MILENAGE + conversion functions for 2G communications. It is currently unclear what is the reason for the restriction to only 3G.

# 4) Conclusion

It is proposed that SA3 adopts the proposal of clause 2 and informs both 3GPP and the GSM association about the optimal way of defining an A3/A8 version on the basis of Milenage + conversion functions c2/c3.

# 5) References


[TS 33.102] : 3GPP TS 33.102: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Architecture".

[S3-020002]: Draft report of SA WG3 meeting #21 Sophia Antipolis.

[Milenage] : 3GPP TS 35.206: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm Specification".

[3GPP] : http://www.3gpp.org/TB/Other/algorithms.htm