**3GPP TSG SA WG3 Security — SA3#35** **S3-040727**

**October 5-8, 2004**

**St Paul's Bay, Malta**

**Agenda Item:** 6.5, 6.9.2

**Source:** QUALCOMM Europe

**Title:** Modifying the MAC in AKA

**Document for:** Discussion and Decision

# 1. Background and introduction

At SA3#34 in Acapulco it was proposed to modify the MAC in AKA to indicate that a GBA_U run is taking place; using the AMF for this purpose has the drawback that the AMF would require standardization. In this contribution we propose instead modifying the MAC to indicate that the AMF (or some field of the AMF) is to be interpreted in a standardized way. Some values of the AMF may then be reserved to indicate that a run is GBA_U. Thus if other applications requiring a standardized AMF are determined at a later date they may be accommodated.

# 2. Discussion

In [1], Axalto propose modifying the MAC in order to indicate that a USIM should carry out GBA_U specific key derivations, modifying the MAC for example by taking an XOR. Subsequent discussions suggested the MAC might be replaced by a hash of MAC and CK.

In this contribution we propose a slight modification to this scheme, namely that the MAC be modified to indicate that the AMF (or some field of the AMF) is to be interpreted in a standard way, and that the AMF in turn will indicate if a run is to be GBA_U. It is proposed that this will enable future possible applications of a standardized AMF should they arise.

So for example if the HSS is producing an AV with the normal, proprietary AMF then it computes MAC in the normal way.

If on the other hand a standardized AMF* is to be used, it first computes a MAC assuming (for example) an all-zero AMF. The HSS, BSF or other party wanting to replace the AV with AV* using a standardized AMF* then replaces the MAC by computing something like MAC* = Hash(MAC, AMF*, CK,IK).

The UICC, receiving RAND and AUTN, first determines if the MAC is correct in the traditional sense. If not it determines if the MAC is of the form MAC* = Hash(MAC if all-zero AMF were used, AMF*,CK,IK). In the latter case it then interprets AMF* in a standard way.

Other modifications are possible; for example the HSS and UICC could simply use a different f1 function to compute MAC; however the approach above has the advantage that the BSF may determine AMF* and the resulting MAC* if this independence is desirable.

# 3. Conclusion

Using a modification of MAC to indicate a standardized interpretation of the AMF provides a more flexible and future-proof approach than simply using it to indicate a GBA_U run, and the ideas presented herein warrant further consideration and discussion.

# 4. References

[1] Axalto, TD S3-040475 Alternative to Special Random or AMF indication for GBA_U: MAC indication, SA3#34, Acapulco.