3GPP TSG SA WG3 Security — S3#23 **S3-020389**

9 - 12 July 2002

Helsinki, Finland

ETSI SAGE **SAGE (02) 27**

4 July 2002

Title: Advice on key expansion for HMAC-SHA-1-96
Response to: LS S3-020315 “Reply LS on key expansion for HMAC-SHA-1-96”
Source: ETSI SAGE
To: 3GPP SA3
Cc:

Contact Person:
Name: **Steve Babbage**
Tel. Number: + 44 1635 676209
E-mail Address: steve.babbage@vodafone.com

Attachments: None

Introduction

SA3 want to use RFC 2404 “The Use of HMAC-SHA-1-96 within ESP and AH”. RFC 2404 defines a specific profile of RFC 2104 “HMAC: Keyed-Hashing for Message Authentication”.

RFC 2104 “HMAC: Keyed-Hashing for Message Authentication”

RFC 2104 supports keys of any length up to 512 bits. Hence using a 128 bit key for HMAC-SHA-1-96 is supported.

There is a “health warning”, though, in Section 2 of RFC 2104:

> "In any case the minimal recommended length for K is L bytes (as the hash output length)";

which is repeated in Section 3:

> "The key for HMAC can be of any length (keys longer than B bytes are first hashed using H). However, less than L bytes is strongly discouraged as it would decrease the security strength of the function."

SAGE understands that the term “key length”, as used here, refers to the cryptographic strength of the key. In this sense, a 128-bit key K and the same 128-bit key expanded in some way to a 160-bit key are equally “long”.

In any case SAGE believes that the problem addressed by the health warning does not exist in the case under discussion, since although the hash output is 160 bits, it is truncated to 96 bits, which is less than the length of the key.

Technically, no advance padding of the key is required by the HMAC function. Section 2 of the specification contains a padding rule:

> “(1) append zeros to the end of K to create a B byte string (e.g., if K is of length 20 bytes and B=64, then K will be appended with 44 zero bytes 0x00).”

Hence, from the point of view of RFC2104, the following two options are equivalent and perfectly acceptable for security:

- use the 128-bit key “as is”;
- use the same key with 32 zero bits appended.

RFC 2404 “The Use of HMAC-SHA-1-96 within ESP and AH”

RFC 2404 does, however, specify that a 160-bit key must be used — hence the LS from S3. In SAGE’s opinion, RFC 2404 is misguided in this respect, as indicated above. However, it is assumed that S3 may have good reasons anyway to conform to RFC 2404.

CONCLUSION

SAGE advises that there is no significant difference between S3's two proposed methods of padding from a security point of view — both are perfectly acceptable. SAGE marginally prefers that the expansion to 160 bits be done by appending 32 zero bits, for conformity with the handling of a 128-bit key by RFC 2104. In any case, SAGE supports the use of very straightforward expansion methods such as the ones proposed by S3, rather than any attempt to make the result look more like a genuine 160-bit random key.

Alternatively, if conformity with RFC2404 is NOT required, then RFC2104 may be used with the 128-bit key "as is".

SAGE does not believe that there is any need to consider changes to the authentication procedures to obtain a key that is effectively longer than 128 bits.