**3GPP TSG SA WG3 Security — S3#19** **S3-010357**

**3-6 July, 2001**

**London, U.K.**

**Source:** Nokia

**Title:** Integrity protection mechanism of SIP

**Document for:** Discussion / Decision

**Agenda Item:** TBD

## Scope and objectives

The scope of this document is to discuss the integrity protection for Session Initiation Protocol (SIP) running in IMS (IP Multimedia Subsystem).

## Background

During last meeting in Phoenix, Nokia submitted a proposal [1] of using Kasumi f9 to protect SIP message integrity between UE and P-CSCF. Ericsson also contributed the idea [2] of using CMS (Cryptographic Message Syntax) for the same purpose.

It was agreed during the meeting that the whole SIP message between UE and P-CSCF should be protected instead of partial message.

## Proposal

This proposal combines the two above contributions together to allow Kasumi f9 fit into the stage 3 SIP structure. The MAC (Message Authentication Code) shall be generated by f9, and to be inserted into the hop-by-hop SIP header, which should be standardised in 3GPP and in IETF. The procedure is as in figure 1:

C->S: INVITE sip:watson@boston.bell-tel.com SIP/2.0

Via: SIP/2.0/UDP kton.bell-tel.com

From: A. Bell ;tag=3pcc

To: T. Watson

Call-ID: 662606876@kton.bell-tel.com

CSeq: 1 INVITE

Contact:

Subject: Mr. Watson, come here.

Content-Type: application/sdp

Content-Length: ...

Integrity: f9, encoding=base64, MAC

v=0

o=bell 53655765 2353687637 IN IP4 128.3.4.5

s=Mr. Watson, come here.

t=3149328600 0

c=IN IP4 kton.bell-tel.com

m=audio 3456 RTP/AVP 0 3 4 5

a=rtpmap:0 PCMU/8000

a=rtpmap:3 GSM/8000

a=rtpmap:4 G723/8000

a=rtpmap:5 DVI4/8000

Figure 1: INVITE to be protected by integrity. (example copied from [3])

The red color text is the protection proof of the message. Proxy-integrity header should be specifically defined for hop-by-hop connection between UE (a SIP UA) and P-CSCF (a SIP proxy). F9 is to inform the P-CSCF about the protection algorithm. Finally the MAC code generated with f9 is attached, and the length is fixed as in [33.908], so it is easy to parse the received message.

The Integrity header adds 35 bytes. The contents of MAC adds 32 bits, i.e. 4 octets. After the base64 according to [4] it is 8 bytes. Therefore all together is 43 bytes.

It is worth of noting that a simpler format of the definition can be as small as 17 or 20 bytes (remove "f9," or not). However, the specification should use the SIP message compression based on pre-agreed dictionary instead of defining a too short and therefore an ambiguous format.

## Procedure

During authentication procedure, the UE and its home network generate the ephemeral IK (Integrity Key) based on a long-term secret key. P-CSCF shall get the same key from the home network protected by NDS (Network Domain Security) solutions.

When UE sends a SIP message to the P-CSCF, the calculation is done depicted in figure 2 left side. The verification is done as depicted on right side of figure 2.

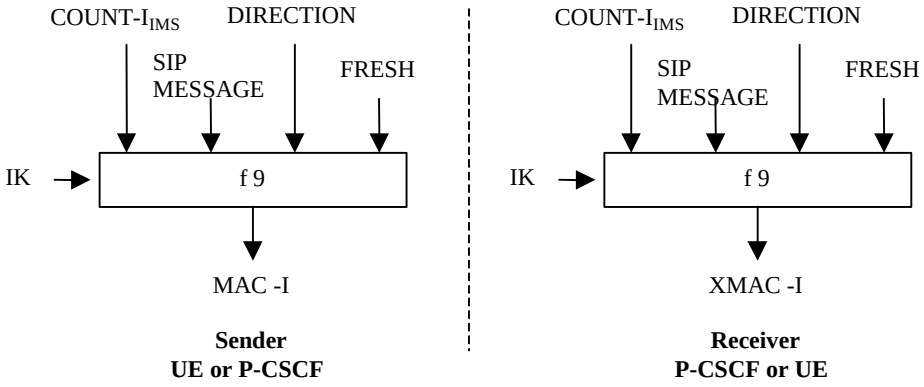


Figure 2: Generation of MAC at both ends.

The SIP MESSAGE is the whole message which is sent to/from the P-CSCF via signalling PDP context. The MAC is verified also based on whole SIP message in receiver side. This definition does not prohibit a SIP message longer than a UDP packet. In case a SIP message is longer than 1500 bytes, fragmentation and padding are needed.

The DIRECTION can be used in the same manner as the radio interface, i.e. uplink or downlink to be protected.

Nonce FRESH is 32 bits long. The FRESH can be sent together with other authentication parameters during authentication procedure so that it is available for integrity protection already when UE sends the RES message to the P-CSCF.

COUNT-$I_{IMS}$ is 32 bits long. Suppose the interval of sending SIP messages is ~100ms per message, it equals to 4971 days or 13.619 years. So it is long enough. COUNT-$I_{IMS}$ must be synchronized in both ends. It could reuse the same mechanism which is used to maintain the synchronization of connection. A START value can be saved to the USIM, and it contains the 20 most significant bits of COUNT-$I_{IMS.}$. The rest 12 bits on the least significant bits side are obtained from a SN (Sequence Number). The least significant bits shall be sent in each message. . The proposed structure of COUNT-$I_{IMS}$ is depicted in figure 3.

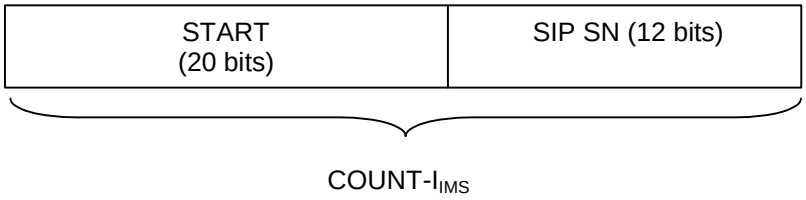


Figure 3: . The proposed structure of COUNT-$I_{IMS.}$

## Analysis

This proposal has a couple of merits based on discussions at S3#18 meeting. First of all, the algorithm Kasumi f9 was reviewed by 3GPP. Secondly, the integrity protection can be maintained based on the similar mechanism used for RRC connection. It is easy to manage START value in USIM for all these domains, CS, PS and IMS.

Finally, the mechanism does not add too much overhead . Hence, this does not deteriorate much of signaling delay, which is really a serious problem with current draft version in 3GPP.

Notes: The mechanism can be built in a way that other algorithms could be negotiated and used as well. Therefore the usage of Kasumi f9 does not prohibit the usage of other integrity algorithms.

## Reference:

[1] S3-0100219. Nokia contribution, Integrity protection mechanism between UE and P-CSCF. S3#18, Phoenix, AZ. U.S.A.

[2] S3-01000199. Ericsson contribution, Integrity protection for SIP signaling. S3#18, Phoenix, AZ. U.S.A.

[3] I-D draft-ietf-sip-rfc2543bis-03.txt, SIP. Handley/Schulzrinne/Schooler/Rosenberg. May 29, 2001. p.138.

[4] I-D draft-josefsson-base-encoding-02.txt, Base Encodings. S. Josefsson (editor). May 4, 2001, p. 5.

[33.908] General Report on the Design, Specification and evaluation of 3GPP Standard Confidentiality and Integrity Algorithms.