3GPP TSG SA WG3 Security — S3#18 **S3-010219**

21-24 May, 2001

Phoenix, Arizona, USA

Source:	**Nokia**
Title:	**Integrity protection mechanism between UE and P-CSCF**
Document for:	**Discussion / Decision**
Agenda Item:	**9.3**

Proposal

During last S2/S3 ad hoc in Madrid, Spain, it was set open how to provide the integrity protection to the Security Association (SA) between UE and P-CSCF. Nokia proposes here to provide integrity protection by a method similar to the one used in UTRAN. Furthermore the message authentication code function can be defined to be the Kasumi f9 used in UTRAN [33.102].

Since it was decided that the protection is done in hop-by-hop manner, the P-CSCF should be able to understand the whole SIP messages. Therefore it is suggested to protect the whole message (message body and headers) instead of a partial message. If the same mechanism is used (e.g. in later releases) for end-to-end integrity protection then its usage over part of the message can be specified later.

Definition of parameters in new proposal

- The same IK may be used for both outbound and inbound messages of a session. Therefore it should be delivered to the visited network together with other parameters during the authentication.
- COUNT-I is 32 bits long. Suppose the interval of sending a SIP message is ~100ms per message, it equals to 4971 days or 13.619 years. So it is long enough.
- The MESSAGE is the whole SIP message which is sent to/from the P-CSCF via signalling PDP context. Since a protected message can be set to have the same length as the UDP packet, the MESSAGE is maximum 1500-32-8=1460 bytes. 32 bytes is the length of MAC-I to be attached, and 8 bytes is the length of UDP header.

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, i.e. the direction of transmission to be protected, i.e. uplink or downlink.
- Nonce FRESH is 32 bits long.

The FRESH can be sent together with authentication parameters so that it is available to do integrity protection already when UE sends the RES message to the P-CSCF.

Evaluation and considerations

- During the authentication procedure, the UE can derive the IK from pre-shared master key and random number RAND, therefore no extra work is needed to deliver integrity key.
- No PKI involved. PGP and S/MIME both involve public-key certificate to authenticate the sender, and to provide message integrity and authentication by signature.
- Security of f9 Kasumi was reviewed in [33.908]
- MAC-I is 32 bits long according to [33.908]. The Internet often uses HMAC SHA-1 which is 160 bits long.
- The tricky part is management of the parameter COUNT-I. It has to be maintained in a synchronized manner both in UE and in P-CSCF. Also here, the mechanisms used in UTRAN can be adapted.

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

References

[33.102] Security Architecture.

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

ANNEX: Kasumi usage in Radio interface

In Uu interface, the Kasumi algorithm is used to provide integrity protection of control messages. The [33.102] describes the MAC generation against the message depicted in Figure 1:

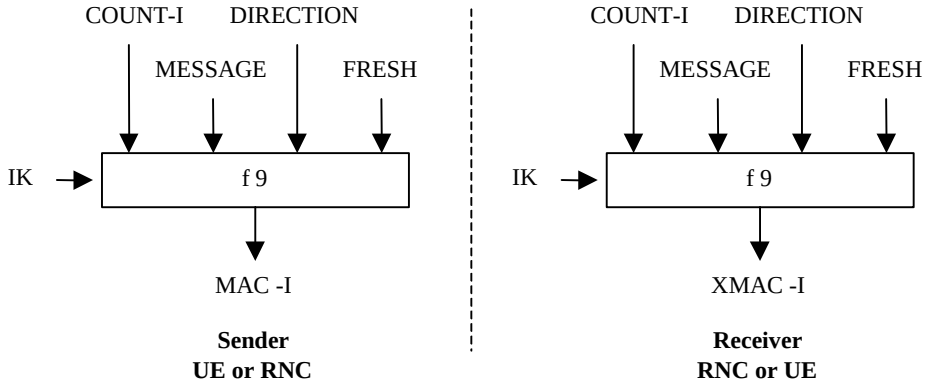

Figure 1: Derivation of MAC on signalling message

Each parameters are defined as below:

- the Integrity Key (IK), 128 bits.
- the integrity sequence number (COUNT-I), which is 32-bits long. It is used to protect against replay during a connection. For each message, the value is incremented by one.
- the direction bit DIRECTION. DIRECTION means the direction of transmission to be protected, i.e. uplink or downlink . The same integrity key may be used for uplink and downlink channels simultaneously associated with a UE. The length of DIRECTION is 1 bit.
- a random value generated by the network side (FRESH), FRESH is a random number generated by the SRNC. This allows the network to be capable of controlling the MAC-I value and detecting replay attack. There is one FRESH parameter value per user. At connection set-up the RNC generates a random value FRESH and sends it to the user in the (RRC) *security mode command*. The value FRESH is subsequently used by both the network and the user throughout the duration of a single connection. This mechanism assures the network that the user is not replaying any old MAC-Is. At handover with relocation of the S-RNC, the new S-RNC generates its own value for the FRESH parameter and sends it to the ME in the RRC message that indicates a new UTRAN Radio Network Temporary Identity due to a SRNC relocation.
- the signalling data MESSAGE.