3GPP TSG SA WG3 Security S3010190
Meeting #18
Phoenix, 21 – 24 May, 2001

Source: Siemens AG

Title: Structure of Initialisation Vector in MAPSec

Document for: Discussion / Decision

Work item: MAP security

Agenda item: tba

Abstract

This contribution proposes a structure for the initialisation vector needed for confidentiality and integrity protection schemes for MAP messages with the aim to minimise the number of bits which need to be transmitted. It also says what needs to be standardised and what not.

1 Introduction

No decision has been taken yet on the cryptographic schemes to be used for the provision of confidentiality and integrity of MAP messages, mostly due to the fact that the modes of operation for the AES have not yet been defined. But modes under discussion which may be considered candidates for use with MAPSec (e.g. CBC-mode, OFB-mode, Counter-mode, CBC-MAC) all require an initialisation vector (or counter respectively). Stream cipher modes (OFB-mode, Counter-mode) in addition strictly require the initialisation vector (or counter respectively) to be unique over the lifetime of the key.

It is clear that a final decision on the use of the initialisation vector (IV) can be taken only after a decision on the AES modes to be used, but agreement on a working assumption regarding the structure of an initialisation vector may be useful to progress the discussion, also for other 3GPP working groups (N4).

This contribution assumes that it is a requirement that the IV is never repeated in any network entity of a PLMN over the lifetime of the key ("uniqueness of the IV"). Such a solution would then also be applicable to a mode for which uniqueness of the IV is not required. It also assumes that the same IV may be used for encryption and MAC computation as there are different keys for confidentiality and integrity.

Contribution S3z010031 to S3#17bis (Madrid, 23-26 April, 2001) showed in a slide a possible structure for an initialisation vector. This contribution elaborates on this structure of the IV and lists open problems.

2 Structure of Initialisation Vector

The following structure is proposed to be used in the computations of the appropriate AES mode.

IV = TVP || NE-Id || Prop || Pad

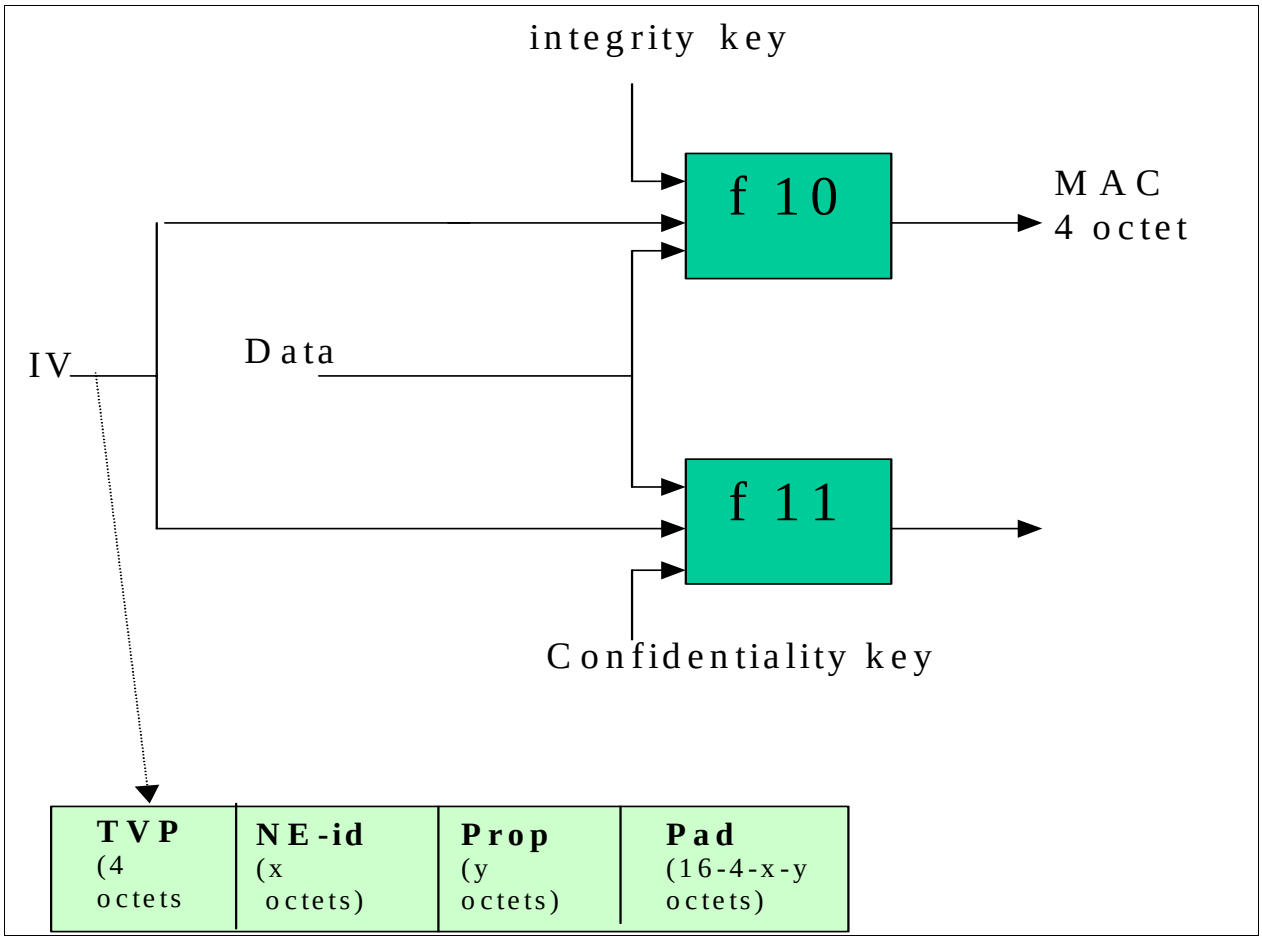

Figure 1: Structure of Initialisation Vector

Interpretation of the fields:

TVP: time variant parameter, a time-stamp which is used for replay protection. For replay protection it is required that the syntax and semantics of *TVP*, in particular the granularity of the clock, are standardised as *TVP* needs to be interpreted by the receiver when checking for replayed messages. The granularity of the clock has not been specified yet. There is a dependency between the granularity of the clock and the length of the *Prop* field: the finer the granularity of the clock the shorter the *Prop* field can be. To give an example, a granularity of 0.01 seconds (the “clock period”) would mean that *TVP* wraps around roughly every 1.3 years, i.e. MAP keys would have to be changed within that period.

NE-Id: this is an identity of the network entity (MAP node). It is necessary and sufficient that *NE-Id* is unique per PLMN. (This is sufficient because sending keys are unique per PLMN.) It would be possible for each operator to define their own scheme of allocating *NE-Ids* to the network entities in a PLMN, but it is strongly recommended to standardise the use of the *NE-Id* field as this reduces the administrative burden for the operator in a multi-vendor environment and makes the implementation of MAP security easier.

Prop: this is a proprietary field whose use is vendor-specific. The use of the field has to ensure the uniqueness of the *IV* for one *NE* during one clock period.

Pad: this is a padding field which is used to expand *TVP* || *NE-Id* || *Prop* to the *IV* length required by the cryptographic scheme in use. The padding rule shall be standardised so that *Pad* need not be transmitted.

Transmission format of *IV*: It should be noted that the *IV* is not necessarily transmitted in the form it is used in the cryptographic computations which was shown above. Firstly, if the time-stamp *TVP* is already transmitted in some other (unencrypted) part of the MAP message it need not be transmitted as part of the *IV* again. This is the advantage of using *TVP* as part of *IV*. Secondly, the padding field need not be transmitted.

3 Proposal

S3 shall adopt the structure of the IV proposed in section 2 as a working assumption.

4 Open Issues

Granularity of the TVP clock: this needs to be standardised for replay protection and has bearing on the definition of the IV, as mentioned above.

Standardised definition of NE-Id: it is not clear at the moment which Id to use and how to derive *NE-Id* from it. It should be remembered that *NE-Id* should be as short as possible.

Standardised padding rule: see section 2 above

Lengths of the fields: this has to be considered very carefully as the security may be affected by the repetition of *IVs*. So far, only the length of the *TVP* has been fixed (4 bytes). Any available Id for NEs probably is too long for the purposes of the *NE-Id* field and needs to be mapped to an acceptable length. The minimum length of the *Prop* field depends on (vendor-specific) considerations on node architectures and on assumptions on maximum MAP traffic during one *TVP* clock period.

Transmission format of IV: it has to be clarified in what part of a MAP message the TVP is most efficiently transmitted.