3GPP TSG SA WG3 Security — S3#15 **S3-000588**

12-14 September, 2000

Washington D.C., USA

Source:	**Nokia**
Title:	**Authentication and key agreement in IM CN subsystem**
Document for:	**Discussion / Decision**
Agenda Item:	**9.9**

This is an outcome of a brief email discussion held before S3#15 about authentication mechanisms in IM CN subsystem. It was decided to have such a discussion in Oslo meeting S3#14.

The baseline document for the discussion was Tdoc S3-000447 (by Siemens) where the matter is studied among other issues, i.e. confidentiality and integrity protection mechanisms.

First, we list briefly pros and cons of various approaches. This list covers the issues that have come up during the discussion.

Secondly, a compact analysis of the situation follows.

Finally, we recommend a way forward. It should be noted that this recommendation was not yet discussed by email.

Pros and cons of various methods

RFC 2617 methods:

+ quite simple methods
- do not seem to meet requirements

PGP:

+ meets other requirements except it is not a 3-party protocol
- PKI mandated

TLS:

+ meets other requirements except it is not 3-party protocol
+ widely deployed in Internet
- does not work with UDP
- PKI mandated

IPSEC/IKE:

+ meets other requirements except it is not a 3-party protocol
+ IM CN is based on IPv6 hence all nodes support IPSEC
- not clear how to be used as a 3-party protocol

UMTS AKA:

+ meets all requirements

+ already implemented in UMTS environment in both USIM and AuC. It may even be possible to use R99 USIMs without any updates.

+ protocol between CSCF and AuC can be chosen freely (e.g. DIAMETER)

- not clear how to be used with other access networks than UTRAN or GERAN

A completely new mechanism from scratch:

+ can be tailored for the purpose

- big specification and implementation effort needed

Analysis

The two basic criteria used to evaluate various approaches are:

1) How well the requirements are met by the solution?

2) How feasible the solution is ?

We discuss first (1) with respect to each mechanism and then we study (2) respectively.

As the requirements for authentication and key agreement method are not yet frozen it is not possible to give a final judgement regarding criterion 1. However, based on the understanding we have about the requirements (see Tdoc S3-000513) the following can be summarized:

RFC 2617 methods fall short of the requirements. Also, there seems to be no natural way to enhance these mechanisms in such way that the requirements would be met.

More advanced Internet mechanisms, i.e. PGP, SSL/TLS, IPSEC/IKE fall short in one requirement: they are not 3-party protocols. Instead, they are designed to fulfil the requirement of entity authentication between two parties. Otherwise, these mechanisms seem to meet the requirements.

Our judgement can now be based on the following two aspects:

- How important is the requirement of being a 3-party protocol ?

- Is it possible to enhance the mechanism to cover the case of a 3-party protocol ?

The architecture of the IM CN subsystem is stable enough to be able to conclude that a 2-party protocol is not sufficient for authentication. Therefore, the judgement must be based on the latter issue: potential extensions. At first sight, there seems to be no easy way to do these extensions but, on the other hand, it is surely not impossible.

UMTS AKA meets all requirements identified.

The same is, of course, true for any potential new mechanism.

As regards feasibility issues it is difficult to give final answers.

Clearly, RFC 2617 methods are simple enough to be feasible to implement in IM CN environment.

For more advanced Internet mechanisms, the extension to 3-party case probably restrict their feasibility considerably. Both PGP and SSL/TLS require PKI support which decreases their feasibility. The wide deployment of SSL/TLS in the Internet communications is a big advantage from the feasibility point of view. The same will most probably be true for IPSEC/IKE in the future. For all these methods, the feasibility on the UE side has to be studied carefully.

The UMTS AKA solution seems feasible as it has direct support from the legacy solutions in both USIMs and AuCs. The open questions are the extendability to cover other access technologies (other

than UTRAN/GERAN) and interoperation with the chosen confidentiality and integrity protection mechanisms.

A completely new mechanism approach can hardly be seen feasible.

Proposal

Based on the analysis above it is proposed that use of UMTS AKA also in IM CN subsystem is kept as a working assumption and further specification work is based on this assumption.

In addition, the approaches based on use of either SSL/TLS or IPSEC/IKE are seen as fall-back solutions if it turns out that the open questions with UMTS AKA cannot be solved. However, it must be noted that these fall-back solutions contain also open questions and further development requires substantial amount of effort.