3GPP TSG SA WG3 Security — S3#22 **S3-020104**

25 - 28 February 2002

Bristol, UK

Source:	**Alcatel**
Title:	**Use of one-way hash function for CHAP in OSA**
Document for:	**Adoption**
Agenda item:	**T.b.d.**

1 Introduction

This contribution identifies an issue in TS 29.198-3 v4.2.0 with regards to the one-way hash function (MD5) to be used to realize CHAP-based authentication.

2 Issue

TS 29.198-3 relies on the use of a challenge-based mechanism (CHAP as per IETF RFC 1994) for authentication of the client application by the framework, and vice-versa. CHAP is chosen as the authentication scheme when the authentication type in the initiateAuthenticate() method is set to P_OSA_AUTHENTICATION.

As it currently stands, the text merely states that, when using CHAP for authentication, a CHAP mechanism as per IETF RFC 1994 is to be used. RFC 1994 describes on one hand the format of packets for exchanging the challenge and the response and one the other hand specifies the use of MD5 for CHAP, in which the input into the MD5 function (or any other one-way function for that purpose) is made of the concatenation of the Identifier, the shared secret and the challenge string.

2.1 Issue#1: use of RFC 1994 packet formats

Because of the lack of detailed reference to RFC 1994 in TS 29.198-3, it is not clear whether CHAP-based OSA authentication must format the challenge and response in packets as described in RFC 1994 or must merely follow the rule given for MD5 processing.

If the Challenge and Response packets as defined in RFC 1994 must be used to format the challenge and the response values, then it is not clear as to what the Name field of the Challenge packet must contain. The Name field must indeed be used to identify the sending system. There is no information in the TS as to which value must be put in there.

If RFC1994 must only be followed for the MD5 processing rule it provides, then it should be clearly specified in the TS.

2.2 Issue#2: weak use of one-way hash function

The mechanism described in RFC 1994, and hence inherited in OSA authentication, for calculating the input into the one-way hash function MD5 has since then (1996) been shown to present some weaknesses wrt the level of security. New constructions for one-way hash functions, such as HMAC, have since then been developed to cope with such issues. The use of MD5 alone as described in RFC1994 is no longer safe. Alternatives based on HMAC (HMAC-MD5 or HMAC-SHA1) must be put in place for challenge-based authentication.

However, as it currently stands, P_OSA_AUTHENTICATION is only associated to the RFC 1994 CHAP mechanism. There is therefore no means to make use of another authentication mechanism in the context of P_OSA_AUTHENTICATION. A separate contribution discusses a proposed solution to enable the smooth negotiation of the authentication mechanism to be used between the client and the framework.

3 Solution

With regards to issue#1 above, it is suggested that the use of the packet format defined in RFC 1994 is clarified. In particular, the value to be used for the Name field of the Challenge and Response packets must be clarified.

With regards to issue#2, two new challenge-based authentication mechanisms are proposed: HMAC_MD5_96 and HMAC_SHA1_96. These are defined resp. in RFC 2403 and 2404. A separate contribution discusses a proposed mechanism to enable the definition of such new authentication schemes and their negotiation.

4 Required Modifications to TS 29.198-3

Sections 6.3.1.1 and 6.3.1.5 must specify clearly that the packet formatting as defined in RFC 1994 is used to exchange the challenge value and response between the verifier and the claimant in OSA authentication.