3GPP TSG SA3-SA2 Joint Meeting **Tdoc S3z010035**
Madrid, Spain 26th April, 2001

Source: Motorola
Title: SIP Headers and Messages for Security in 24.228 Flows
Document for: Discussion and Decision

1 Introduction

At the last SA2-SA3 joint meeting held in Gothenburg SA3 outlined that their agreed approach to security for IM subsystem SIP signalling would use AKA authentication and encryption rather than using PGP that is outlined in the IETF RFC2543bis. Since the RFC does not currently specify which SIP headers and mechanisms are used to provide security using AKA these will need to be specified by 3GPP and then should be documented in 24.228 and also worked through the IETF.

2 Discussion

Sip draft RFC2543bis-02 states that although all implementations SHOULD support PGP based encryption they MAY implement other schemes. However only the PGP scheme is described.

The bis draft specifies the following security related headers:

Authorization;
Encryption;
Proxy-Authenticate;
Proxy-Authorization;
Response-Key;
WWW-Authenticate

In addition the following security related responses are also specified:

401 Unauthorized;
407 Proxy Authentication Required

Some Current Examples of Header Syntax using PGP:

Authorization: PGP version="5.0"
realm="3GPP IM ID",
nonce="913082051",signature="YHJU=G+HK=fdyehgFOcgRPhgjhdf6210"

Encryption: PGP version="5.0",encoding= "ascii"
qdGFHxGytfyfye+=TYYytHJU+GHKfdyehgJKQ=WShgjhdf62109clkHJYFYE2099
0jfoij9lOJU9jkjlkjbvjhjfojv

Proxy-Authenticate: PGP version="5.0"

realm=”3GPP IM ID”, algorithm=md6,nonce=”913082051”

Proxy-Authorization: PGP version=”5.0”
realm=”3GPP IM ID”,
nonce=”913082051”,signature=”YHJU=G+HK=fdyehgFOcgRPhgjhdf6210”

Response-Key: PGP version=”5.0”, encoding=”ascii”,
key=”YHJU=G+HK=fdyehgFOcgRPhgjhdf6210”

WWW-Authenticate: PGP version=”5.0”
realm=”3GPP IM ID”, algorithm=md6,nonce=”913082051”

We need to understand if these existing headers and responses are sufficient for implementing security using AKA for authentication and encryption or do we need new ones. Which headers and responses are required and specify how they are used and what extensions are required to incorporate AKA.

We also need to understand if and how SIP and/or SDP signalling is involved in the key exchanges needed for encryption of media streams, (bearer) during Session Initiation. In particular are any extensions required for SIP or SDP for this?

Another issue that requires closure for 24.228 is on the use of the Private User Identity. It has been assumed by SA2 and CN1 that the Private User Identity will only be required to be included in the SIP REGISTER Message. However at the Gothenburg joint meeting SA3 colleagues were not prepared at that time to conclude that the Private User Identity was definitely not required in other SIP messages such as INVITE. This issue is important because a requirement to pass the Private User Identity in other messages will require extensions to IETF SIP.

The assumption of SA2 and CN1 that the Private User Identity is only required in REGISTER messages is based on the fact that during registration an association is made between the Public User Identity and the Private User Identity within the network and the UE is passed a mechanism to authenticate itself during subsequent session initiations. During session initiation the Public User Identity is passed to the network in the **From** header of the SIP request. It has been assumed by SA2 and CN1 that since the network has already an association between the Private User Identity and the Public User Identity as a result of registration the Invites and other messages can be authenticated using the mechanism passed at registration. Periodic Re-registration (Using the Private User Identity) can take place (if required) during long active sessions for the purpose of periodic update of keys, although the likely frequency of these re-registrations needs to be understood since they may have an impact for instance on Audio Quality in GERAN using “optimised voice’. Feedback and comment from SA3 experts on these assumptions is most welcome.

3 Decision

It is proposed that the joint meeting consider the above issues for discussion and make a decision on the following points:

1. SIP level flows and parameters related to security should be included in TS 24.228 based on the work conducted by SA3.
2. The identification of SIP headers, responses and mechanisms required for AKA authentication and encryption of SIP messages, should be pursued by SA3 as a high priority item since this information is needed by SA2 and CN1.
3. The identification of SIP and/or SDP headers, and mechanisms required for key exchanges needed for encryption of media streams, (bearer) during Session Initiation, should be pursued by SA3 as a high priority item since this information is needed by SA2 and CN1.
4. Use of the Private User Identity during registration and a decision on whether the Private User Identity is required also during Session Signalling, should be pursued by SA3 as a high priority item since the current SIP signalling flows in TS 24.228 are based on the assumption that the Private User Identity is not required in any other messages other than REGISTER.