3GPP TSG SA WG3 Security — S3#26 **S3-020633**
19- 22 November 2002
Oxford, UK

Source: Nokia

Title: Proposal for Annex H by extending HTTP Digest for SA management

Document for: Discussion and approval

Agenda: Tbd.

Abstract

The discussion paper explains the status of Sec-agree draft in IETF, and proposes another alternative solution for Annex H of TS 33.203, which is the extension of HTTP Digest. The rationale is explained in section 2.

1 Introduction

The Annex H in TS33.203 depicts details of IPsec SA attributes that should be communicated between the UE and the P-CSCF. Original plan is that SA attributes shall be transferred via [Sec-agree] negotiation. Later in S3 #25 plenary meeting (October, Munich), it is recognized the risk that Sec-agree draft may not achieve approval in IETF within 3GPP R5's timeframe. It was then agreed if the status of Sec-agree draft is approved during October, 2002, S3 specification shall remain unchanged; otherwise, another solution that is independent of IETF standardisation shall be developed.

2 The rationale of the backup solution

This paper presents an alternative solution . It utilizes the extension of HTTP Digest for carrying SA attributes. Figure 1 depicts the message flow and status transaction. It is in line with TS33.203 design.

It is understood that this solution is derived from HTTP Digest syntax, which allows further extension for different purposes.

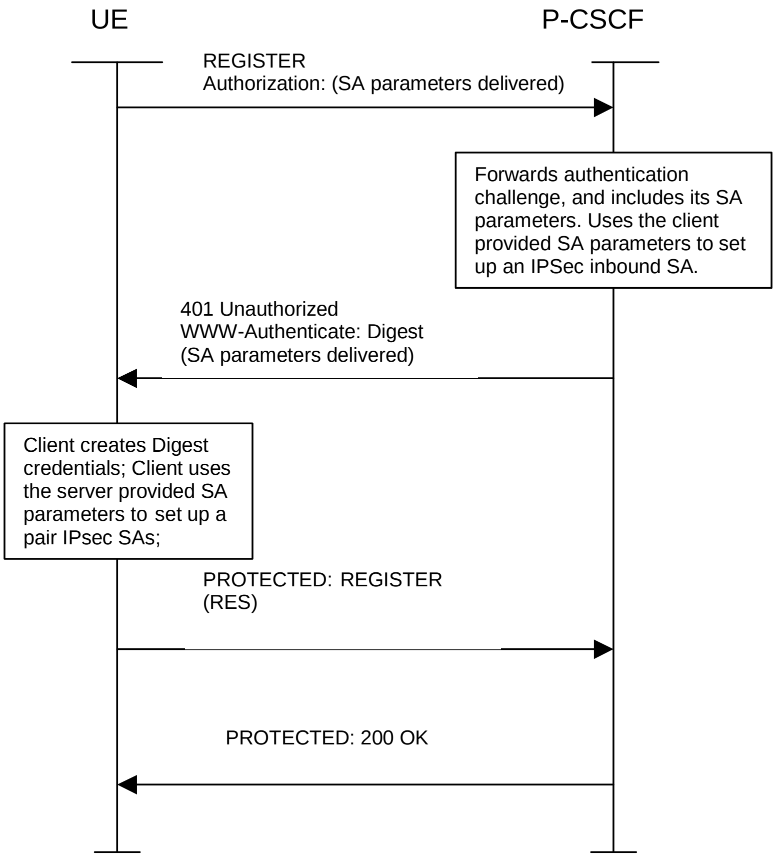
UE
P-CSCF
REGISTER
Authorization: (SA parameters delivered)
Forwards authentication challenge, and includes its SA parameters. Uses the client provided SA parameters to set up an IPSec inbound SA.
401 Unauthorized
WWW-Authenticate: Digest
(SA parameters delivered)
Client creates Digest credentials; Client uses the server provided SA parameters to set up a pair IPsec SAs;
PROTECTED: REGISTER
(RES)
PROTECTED: 200 OK

Figure 1: Message flow representing a successful authentication and SA creation

3 The detail of syntax

The BNF presented below is copied from [Sec-agree] Appendix A. Therefore it is exact the same information of SA to be communicated. It follows BNF of the [SIP] specification for headers "WWW-Authenticate", "Proxy-Authenticate", "Authorization", and "Proxy-Authorization":

```
auth-param    = 1 * ( algorithm / protocol / mode / encrypt-algorithm

                  / spi / port1 / port2 )

algorithm         = "alg" EQUAL ( "hmac-md5-96" /
                              "hmac-sha-1-96" )
 protocol         = "prot" EQUAL ( "ah" / "esp" )
 mode             = "mod" EQUAL ( "trans" / "tun" )
 encrypt-algorithm  = "ealg" EQUAL ( "des-ede3-cbc" / "null" )
 spi            = "spi" EQUAL spivalue
 spivalue         = 10DIGIT; 0 to 4294967295
 port1           = "port1" EQUAL port
 port2           = "port2" EQUAL port
 port           = 1*DIGIT
```

The explanation of parameters:

- Algorithm

This parameter defines the used authentication algorithm. It may have a value of "hmac-md5-96" for HMAC-MD5-96 [13], or "hmac-sha-1-96" for HMAC-SHA-1-96 [14]. The algorithm parameter is mandatory.

- Protocol

This parameter defines the IPsec protocol. It may have a value of "ah" for AH [6], or "esp" for ESP [7]. If no Protocol parameter is present, the protocol will be ESP by default.

- Mode

This parameter defines the mode in which the IPsec protocol is used. It may have a value of "trans" for transport mode, or a value of "tun" for tunneling mode. If no Mode parameter is present the the IPsec protocol is used in transport mode.

- Encrypt-algorithm

This parameter defines the used encryption algorithm. It may have a value of "des-ede3-cbc" for 3DES, or "null" for no encryption. If no Encrypt-algorithm parameter is present, encryption is not used.

- Spi

Defines the SPI number used for inbound messages.

- Port1

Defines the port number for inbound messages.

- Port2

Defines the port number for outbound messages. If no Port2 parameter is present port1 is also used for outbound messages.

3 The compliance of specifications

The backup solution could be a part of R5. The CR and this discussion paper should be submitted to CN1 meeting #27, for information. The reason is that no more CN1 meeting in this year after S3#26. In case the solution presented here is approved in S3, CN1 can absorb it to their specification without further plenary meeting.

An informational RFC maybe needed to state IETF about this solution later.

4 Proposal

—If an approval of [Sec-agree] has not received till S3 #26 plenary meeting, we propose the S3 meeting endorse this proposal.

If [Sec-agree] got approval in IETF before coming SA plenary meeting, this solution is withdrawn by SA3 WG.

5 Reference

[Sec-agree] Security Mechanism Agreement for the Session Initiation Protocol, Arkko et al. draft-ietf-sip-sec-agree-05. October 28, 2002.

[SIP] RFC3261.