3GPP TSG SA WG3 Security **S3z020020**

January 31 – February 1, 2002

Antwerp, Belgium

Agenda Item: TBD

Source: Ericsson

Title: SIP layer confidentiality between UA and P-CSCF

Document for: Informational

1. Scope and objectives

The scope of the document is to demonstrate how the confidentiality between the UA and P-CSCF could be protected at SIP layer. The proposed solution is based on the use of SIP S/MIME tunneling defined in the new version of SIP [sip-bis6].

2 Background

Ericsson is actively participating in SIP security work in IETF. Lately, IETF has started fixing the existing SIP layer authentication and integrity protection mechanisms to work for first and last hop protection. Problems related to SIP layer confidentiality protection have also been taken under discussion. The new SIP specification defines more clearly how to implement confidentiality at SIP layer [sip-bis6]. One of the proposed mechanisms will be so-called SIP S/MIME tunneling. This document demonstrates how this mechanism could be used for protecting the confidentiality between the UA and P-CSCF.

3 SIP layer confidentiality

SIP layer confidentiality will be based on S/MIME. MIME [mime1, mime2] has been originally developed for carrying non-ASCII data in e-mails. The basic idea is to encode any arbitrary data into ASCII and then transmit it in the body of standard e-mail message. Each MIME message includes information that tells the type of data and encoding used for the body. Nowadays, MIME can be used in several text based transport protocols, e.g. e-mails, HTTP or SIP, to carry arbitrary data blocks. S/MIME [e.g. smime] is just an extension to MIME including the ability to carry and interpret cryptographic data blocks in the message body. In theory, S/MIME is not limited to any specific cryptographic syntax. Most commonly used formats are Cryptographic Message Syntax (CMS) [cms] and Pretty Good Privacy (PGP) [pgp-mime].

In general, e-mail implementations utilising S/MIME assume the use of asymmetric cryptography and PKI. However, it is also possible to use previously distributed symmetric keys for encryption [smime, cms]. All e-mail implementations must support these if they are S/MIME compliant. There are also other interesting CMS content types which are relevant for implementations applying symmetric key cryptography, such as password based encryption [cms-psw], authentication with symmetric keys [cms] or compression [cms-compression], however, these features are not currently required from S/MIME implementations.

In general, the encryption of SIP message end-to-end is problematic because there are certain SIP entities, which need to view and modify the SIP headers and bodies. However, there will still be two standards ways how to encrypt SIP messages at SIP layer. Firstly, S/MIME can be used to encrypt the SIP bodies. This is the most common and traditional use of MIME. Secondly, S/MIME can also be used to encrypt confidential SIP headers together with SIP bodies using a special SIP S/MIME tunneling mechanism. In SIP S/MIME tunneling, a SIP message can be protected and wrapped in S/MIME. S/MIME is carried in a SIP body with the content type “message-sip” [sip-mime]. The outer SIP message includes all routing related SIP headers. In this way, confidential SIP headers as well as the SIP body are not revealed during the routing. The same mechanism applies to authentication and integrity protection with S/MIME.

4 Encryption between UA and P-CSCF

S/MIME can be used end-to-end between two communicating entities. What end-to-end really means, depends much on application area. In e-mail environment, S/MIME can be used between two end-users. However, it is also possible to use S/MIME to protect communication between two mail servers if they tunnel all e-mail messages between them in S/MIME bodies.

In normal SIP implementations, proxies do not check the S/MIME bodies because they assume that the S/MIME packet is directed for the UA at the other end. In other words, proxies automatically forward the S/MIME bodies without taking a look at them. CMS packet inside S/MIME includes key identifiers for the symmetric pre-shared keys. The basic problem is how to get the proxy interested in CMS packet so that it would realise that it has the key to decrypt it. If a proxy could assume that all certain types of SIP messages from certain direction must always be protected with S/MIME, then there is no problem implementing S/MIME also for proxies.

S/MIME can be used for encrypting the messages between the UA and P-CSCF if we decide that P-CSCF should check all S/MIME bodies under certain conditions, e.g. if the visited network requires that all messages must be encrypted between UA and P-CSCF. There must exist some additional headers outside the encryption, however, the amount of them can be minimised for the SIP method line, content-type header and content-transfer-encoding header. The basic message format would look like the example below:

```
INVITE sip:bob@biloxi.com SIP/2.0
     Content-Type: smime-type=enveloped-data
     Content-Transfer-Encoding: base64

*********************CMS_BEGINS:ENCRYPTION**********************
CMS specific data (e.g. encryption algorithm, key identifier)
   Content-Type: message/sip

   INVITE sip:bob@biloxi.com SIP/2.0
     Via: SIP/2.0/UDP 10.1.3.3:5060
     To: Bob <bob@biloxi.com>
     From: Alice <alice@atlanta.com>;tag=1928301774
     Call-ID: a84b4c76e66710@10.1.3.3
     CSeq: 314159 INVITE
     etc.
**********************CMS_ENDS*****************
```

The example above demonstrates tunneling in which the INVITE includes the same Request-URI as the original message. Another alternative would be to put P-CSCF as the Request-URI of the outer INVITE. In this case, there would not be any potential confusion of the proposed target of the S/MIME body.

Compression may be done at two phases. SIP message should be compressed before encryption at SIP layer. Compression is repeated before transmission over the wireless interface because there still are headers that has not been compressed, e.g. transport layer and IP layer headers. Compression of the SIP headers outside the encryption is FFS. It can be assumed that these headers are rather static and they can be compressed into few bytes if required.

This solution does not restrict the end-users or mobile operators from using S/MIME also for end-to-end authentication and integrity protection. It is possible to carry end-to-end protected S/MIME messages within hop-by-hop tunneling mechanism. The example in appendix 1 demonstrates that the use of S/MIME for encryption between UA and P-CSCF does not restrict end-users to use S/MIME at the same time for other purposes. The example has been taken and modified form an early version of the security part of SIP-bis6.

The use of S/MIME for end-to-end encryption is not possible if any proxy between the end points must view or modify the SIP message body. This restriction has no relation to the solution described in this document.

5 Conclusions

This contribution has demonstrated how S/MIME could be used for protecting the confidentiality between the UA and P-CSCF. The solution utilised SIP S/MIME tunneling. The solution also assumed that P-CSCF is able to distinguish the message coming from the network from the messages coming from the access domain.

References

[cms] Housley R., Cryptographic Message Syntax, IETF, 1999, RFC 2630.

[cms-compression] Gutmann P., Compressed Data Content Type for CMS, IETF, Work in progress, November 2001, draft-ietf-smime-compression-07.txt.

[cms-psw] Gutmann P., Password-based Encryption for CMS, IETF, 2001, RFC 3211.

[mime1] Freed N. & Borenstein N., Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, IETF, 1996, RFC 2045.

[mime2] Freed N. & Borenstein N., Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types, IETF, 1996, RFC 2046.

[pgp-mime] Elkins M. et al, MIME Security with OpenPGP, IETF, 2001, RFC 3156.

[sip-bis6] Rosenberg, J. et al, SIP: Session Initiation Protocol, IETF, Work in progress, January 2002, draft-ietf-sip-rfc2543bis-06.txt.

[sip-mime] Sparks R., Internet Media Types message/sip and message/sipfrag, IETF, Work in progress, September 2001, draft-sparks-sip-mimetypes-01.txt.

[smime] Ramsdell B., S/MIME Version 3 Message Specification, IETF, RFC 2633.

APPENDIX 1: EXAMPLE

Alice wants to make a call to Bob. She wants to use her private PKI system to identify herself to Bob, and to provide additional integrity protection to the message. The following phases has been done before the message is ready:

1. UA constructs a SIP message to Bob (INVITE c).
2. Alice uses her private PKI system to sign the SIP message (signature d - this is external to IMS).
3. UA copies the INVITE (c) to a new INVITE (b), which includes the original INVITE (b) and signature (d) as S/MIME attachments.
4. UA compresses the result from the previous phases, and uses the IMS CK to encrypt it. The result is BER-encoded to CMS, and base64 encoded for S/MIME. The result is seen between the lines of asterisks characters.
5. UA add yet a new INVITE line (a) and tunnels the whole previous message as a S/MIME attachment to P-CSCF.

P-CSCF decrypts the message and forwards the INVITE (b) onwards in clear.

```
a) INVITE sip:bob@biloxi.com SIP/2.0
     Content-Type: smime-type=enveloped-data
     Content-Transfer-Encoding: base64

*********************CMS_BEGINS:ENCRYPTION**********************
CMS specific data (e.g. encryption algorithm, key identifier)
b) Content-Type: message/sip

   INVITE sip:bob@biloxi.com SIP/2.0
     Via: SIP/2.0/UDP 10.1.3.3:5060
     To: Bob <bob@biloxi.com>
     From: Alice <alice@atlanta.com>;tag=1928301774
     Call-ID: a84b4c76e66710@10.1.3.3
     CSeq: 314159 INVITE
     Contact: <sip:alice@10.1.3.3>
     Content-Type: multipart/signed;
       protocol="application/pkcs7-signature";
       micalg=sha1; boundary=boundary42

     --boundary42
     Content-Type: message/sip

c)   INVITE sip:bob@biloxi.com SIP/2.0
     Via: SIP/2.0/UDP 10.1.3.3:5060
     To: Bob <bob@biloxi.com>
     From: Alice <alice@atlanta.com>;tag=1928301774
     Call-ID: a84b4c76e66710@10.1.3.3
     CSeq: 314159 INVITE
     Contact: <sip:alice@10.1.3.3>
     Content-Type: application/sdp
     Content-Length: 147

     v=0
     o=UserA 2890844526 2890844526 IN IP4 here.com
     s=Session SDP
     c=IN IP4 100.101.102.103
     t=0 0
     m=audio 49172 RTP/AVP 0
     a=rtpmap:0 PCMU/8000

     --boundary42
     Content-Type: application/pkcs7-signature; name=smime.p7s
     Content-Transfer-Encoding: base64
     Content-Disposition: attachment; filename=smime.p7s

d)   ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
     4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
     n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
     7GhIGfHfYT64VQbnj756
     --boundary42-
***********************CMS_ENDS*****************
```