3GPP TSG SA WG3 Security — S3#23 **S3-020239**

14 - 17 May, 2002

Victoria, Canada

Source: **Nokia**

Title: **Security negotiation procedure for IPsec**

Agenda item: IMS

Document for: DISCUSSION**/APPROVAL**

Abstract

Since for IMS Release 5, S3 has decided that IPsec without IKE is the preferred mechanism for UE's first hop protection, this paper proposes the security negotiation procedure for IPsec usage between UE and P-CSCF in IMS. The goal is to enable both nodes handling SA establishment and management in formulated way. The suite concept is proposed to pre-define the algorithms and parameters of SA establishment and to be negotiated during initial authentication.

1 Introduction

This proposal aims at introducing a security negotiation procedure for SIP [Sec-agree] into TS 33.203. For R5, S3 has decided that IPsec without IKE is the preferred mechanism for UE's first hop protection. Correspondingly, the IPsec and Security Association relevant attributes shall be then negotiated in the SIP level instead of by ISAKMP [RFC2408] or IKE [RFC2409].

The paper proposes to pre-define the attributes for IPsec usage and SA establishment as an attribute suite which can be negotiated in the SIP level using a pointer. Eventually, this pointer is transferred from the SIP application to the IPsec. Figure 1 shows the modules and functions delivered via interfaces.

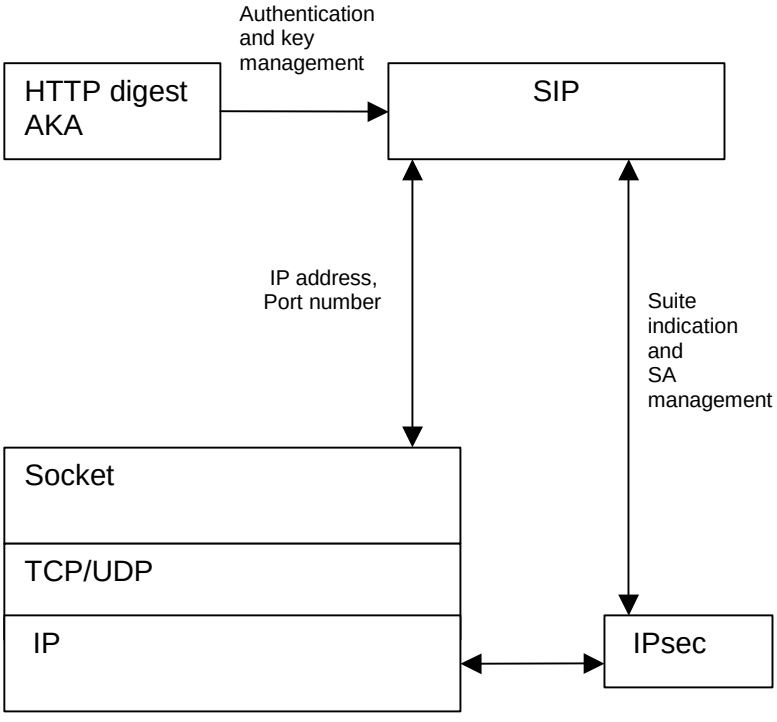


Figure 1: SIP and IPsec Module and functions

The IPsec SA management requires that the used algorithm settings and security parameters are shared between the two ends. This section proposes that algorithms and parameters for establishing SA are marked with a suite number, which is communicated in the security mechanism negotiation procedure. One suite groups together algorithms, which are able to interact properly with each other, so as to avoid the situation where combining algorithms do not interact well. This approach allows adding new algorithms to the defined usage of IPsec, regardless of the release. So it fulfils our intension of providing a forward migration path to better algorithms, and reducing the number of correlated document so as to simplify the approval procedure.

This proposal contains a basic subset of *Domain of Interpretation for ISAKMP* [RFC2407], which specifies the IPsec naming scheme registered in the Internet Assigned Numbers Authority (IANA). The new parts unsupported by [RFC2407] are in line with the Internet Draft *Security Negotiation Procedure for SIP* [Sec-agree], e.g., the mechanism called 'Digest'. Those new attributes unspecified by neither of the two references, are defined as the token extension in the [Sec-agree] syntax. An example of such an extension is the SA_ID.

The security mechanism negotiation introduced in this proposal is only applied to the first hop, between UE and P-CSCF to negotiation protection mechanism. Since the IMS architecture relies on home S-CSCF to authenticate UE, the keying protocol and authentication protocol are not negotiable in this phase.

2 Attributes to be pre-defined

2.1 IPSEC Situation Definition

The IPsec situation definition provides information that can be used by the responder to make a policy determination about how to process the incoming Security Association request. Three types of situations are defined in [RFC2407], SA for authentication, encryption or integrity purpose. For R5 usage, integrity is selected which is defined as

SIT_INTEGRITY 0x04

2.2 IPsec protocol

IPsec ESP shall be used to provide integrity protection of SIP signalling. Corresponding name is defined in [RFC2407]:
PROTO_IPSEC_ESP 3

In 3GPP the ESP with NULL confidentiality shall be used. IPSEC ESP Transform Identifiers
ESP_NULL 11
ESP NULL is defined in RFC2410.

2.3 SA management and attributes

- SA lifetime

[RFC2407] defines that SA lifetime can be either measured by time (seconds) or by data amount (kilobytes). In the IMS architecture, SA lifetime is defined by the P-CSCF, with regards to the registration timer set by the S-CSCF. The concrete timer length as well as refreshing SA lifetime can be informed by the SIP application to the IPsec layer after a successful registration. The notification procedure from SIP to IPsec remains implementation specific.

When the UE generates session keys and the RES, it does not know how to establish the local SAs, so the SAs lifetime should always be established in seconds as default. The default SA lifetime may be equal to a pre-defined timer, e.g. non-INVITE transaction timeout timer (64*T1, T1=500ms, RTT Estimate timer). UA in the UE and the P-CSCF shall update the SA lifetime in IPSec SAD after receiving a successful acknowledgment from S-CSCF. The actual lifetime is based on the operator's local policy on how often to challenge the UE. The attributes below show an example of a UE establishing an SA valid in 32 seconds as default.

SA Life Type=1
SA Life Duration=32

Attribute #1:
0x80010001 (Address Family = 1, type = SA Life Type, value = seconds)

Attribute #2:
0x00020004 (AF = 0, type = SA Duration, length = 4 bytes)
0x00000040 (value = 0x00020 = 32 seconds)

- Other mandatory SA parameters are:

Authentication Algorithm=1

Two integrity algorithms are defined for IPsec, HMAC_MD5 and HMAC-SHA1, in [RFC2403] and [RFC2404] correspondingly. Since the latter one requests a fixed key length of 160 bits, only the former one is defined in this proposal. Algorithm is the field which contains the proposed algorithm. In the example, number 1 means HMAC-MD5.

- Encapsulation Mode=2

Encapsulation mode is the Transport mode which is defined as 2 in [RFC2407].

- Keying= Digest AKA

key lengths=128 bits.

2.4 Summary of suite definition

This clause collects the all necessary attributes into a suite 1. New combination of algorithms and parameters can be defined as separate suite later.

Suite 1:

a) IPsec protocol
   Protocol id=PROTO_IPSEC_ESP
   ESP Transform Identifiers= ESP_NULL

b) SA attributes
   Situation=SIT_INTEGRITY
   SA Life Type=seconds
   SA Life Duration=64s
   Authentication Algorithm= HMAC_MD5
   Encapsulation Mode=Transport
   Keying= AKA
   key lengths=128 bits

3 Security mechanism negotiation procedure for IPsec

The IPsec protection requires relevant algorithms, parameters to be transferred between UE and P-CSCF. The [Sec-agree] offers such possibilities to acknowledge the usage of IPsec and the corresponding parameters. Authentication and key agreement are referred to [Digest-AKA]. Figure 2 is copied from TS 33.203 as reference.

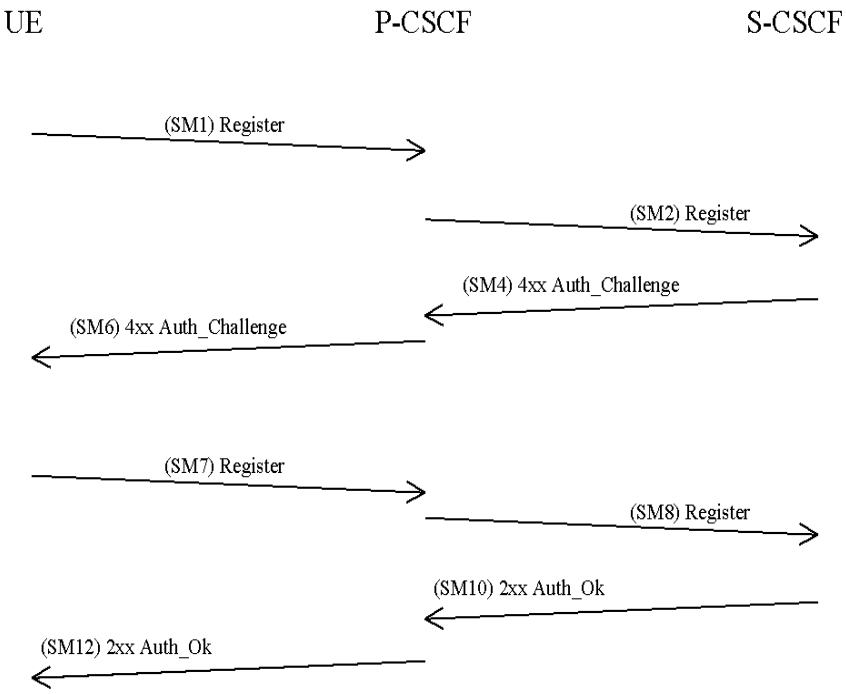


Figure 2: Security mechanism negotiation procedure (successful case)

Step 1: In the first registration, the UE shall announce a list of supported security mechanisms, among which the IPsec is the first preference. According to [Sec-agree], the UE should also add the option-tag 'sec-agree' to the Supported header so as to show P-CSCF that it supports security mechanism negotiation feature. The UE shall always uses port number 5060 for first REGISTER message, according to [SIP-IETF]. In P-CSCF, if a REGISTER message is received from 5060, it shall be marked as unprotected message and sent to S-CSCF. Any messages other than REGISTER sent to 5060 shall be only dropped.

SM1:
REGISTER(
Authorization: IMPI
Security-Mechanism: to-uri, from-uri, mech_list_UE)

Explanation:

- To_uri and from-uri are SIP URI defined in [Sec-agree], the receiver and initiator's identifier.
- Mech_list_UE is the supported algorithm listed by UE. It encapsulates the detail of each mechanism to be negotiated. In IPsec case, it is expressed as: mech=ipsec-man;pref=1;SA_ID_U=ABCD; Suite=1.
- The [Sec-agree] defines 6 types of mechanisms. The IPsec without automatic key algorithm (IKE) is named as 'ipsec-man'.
- Preference is 1 means the IPsec is the first preferred choice.
- Suite is the attribute suite, detailed definition see chapter 2.
- SA_ID_U is the UE's SA_ID. The The SA_ID_UE shall be chosen in such a way that it uniquely identifies the inbound SA (unidirectional) at the UE.

Step 2: Once the P-CSCF received the SM1, it understands the proposed IPsec for SIP is the first preference of the UE. The P-CSCF shall then send its own lists of supported algorithms to the UE regardless of what it had received. In particular, the list shall contain the IPsec parameters, such as SA_ID_P. The SA_ID_P shall be chosen in such a way that it uniquely identifies the inbound SA (unidirectional) at the P-CSCF. Digest AKA relevant parameters RAND and AUTN in WWW-authenticate header is generated by S-CSCF. The details of Digest AKA can be found in [Digest-AKA].

SM6:
4xx Auth_Challenge(
WWW-authenticate: IMPI, RAND, AUTN

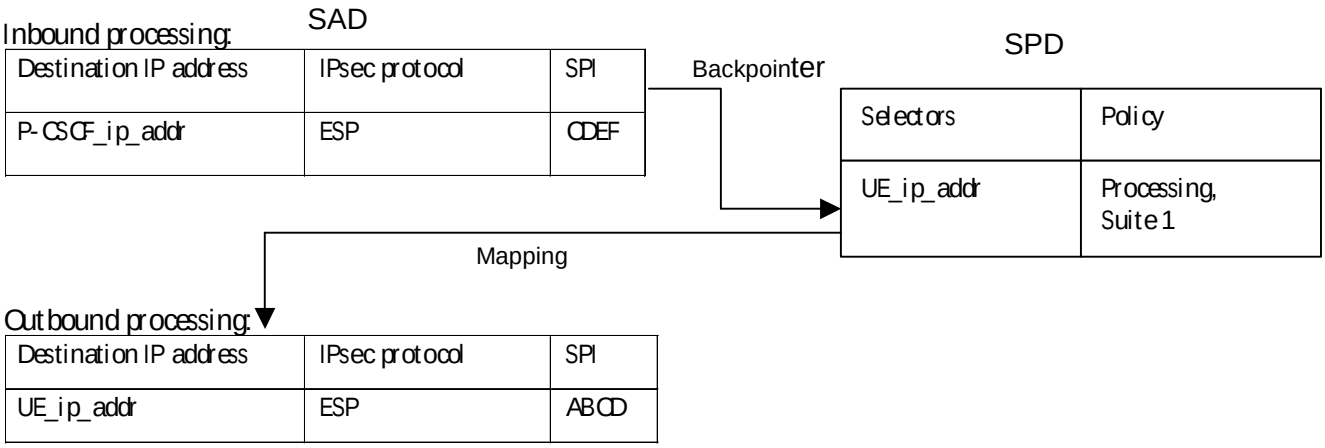
Security-Mechanism: to-uri, from-uri, mech_list_Proxy)

(Author's notes: the error message is skipped when the UE does not contain the Security-Mechanism header.)

Explanation:

- Mech_list_Proxy is the mechanism list offered by Proxy. In detail format, IPsec mechanism is elaborated as mech=ipsec-man;pref=1; SA_ID_P=CDEF;Suite=1. If other mechanism is defined, it may be extended, e.g. mech=smime;pre=2;Suite=x
- Pre=1 means that mechanism IPsec without IKE is first preference in this P-CSCF.
- SA_ID_P is the P-CSCF's SA_ID.

At this stage, P-CSCF establishes the two SAs in local SAD, and their policy in SPD (according to [RFC2401] as below:



Particularly P-CSCF shall contain a table which associates UE's IP address, port number with all permitted IMPUs, to verify the client's ID against the SA used.

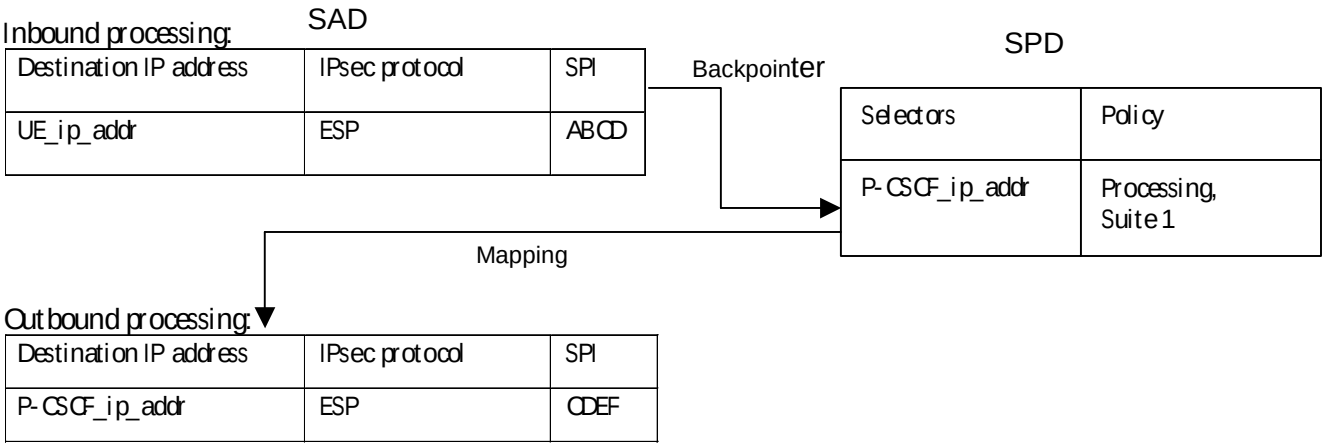
Source IP address	Source port number	IMPUs
UE_ip_addr	UE_port	IMPU1, IMPU2

Step 3: The UE receives the challenge and the P-CSCF supported list. It shall then switch on the IPsec integrity protection for subsequent SIP messages by setting up security associations according to the mechanisms and parameters negotiated in SM1 and SM6. It shall also respond to the Digest AKA challenge and furthermore, the UE must repeat the P-CSCF's list to reflect any potential manipulation:

SM7:
REGISTER(
Authorization: IMPI, digest-response
Security-Mechanism: to-uri, from-uri, mech_list_Proxy)

The UE shall establishes the two SAs as well according to [RFC2401]:

UE shall apply SA ABCD to SM7. The SM7 itself is sent from UE_ip_addr and source port number; it is sent to P-CSCF's IP address and port number as destination.



The last step 4: P-CSCF sends SM12 to the UE. SM12 does not contain information specific to the security agreement, but sending SM12 as 200 OK, the P-CSCF confirms that the registration and authentication have been successful. The 200Ok is sent from P-CSCF's source IP address and source port number; it is sent to UE's IP address and port number as destination. The outbound IPsec SPI index is CDEF.

4 Proposal

The author proposes the meeting to endorse the sprite of the proposal on Security negotiation procedure for IPsec. It is suggested that the section 2 and 3 may be added to TS33.203 clause 7.1 (Annex D.1) and 7.2 respectively. Annex F maybe deleted as well.

5 Reference

[Digest-AKA] Aki Niemi, HTTP Digest Authentication Using AKA. March 2002.

[RFC2401] S. Kent, Security Architecture for the Internet Protocol. November 1998.

[RFC2403] C. Madson, The use of HMAC-MD5 within ESP and AH. Nov. 1998.

[RFC2404] C. Madson, The use of HMAC-SHA1 within ESP and AH. Nov. 1998.

[RFC2406] S. Kent, IP Encapsulating Security Payload. Nov. 1998.

[RFC2407] D. Piper, The Internet IP Security Domain of Interpretation for ISAKMP. Nov. 1998.

[RFC2408] Maughan, D., Schertler, M., Schneider, M., and J. Turner, Internet Security Association and Key Management Protocol (ISAKMP). November 1998.

[RFC2409] D. Harkins, et al., IKE. November 1998.

[Sec-agree] Jari Arkko et al, Security Mechanism Agreement for SIP Sessions, version 01. Internet draft.

[SIP-IETF] J. Rosenberg et al., SIP (RFC2543-bis9). February, 2002.